Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

21.069

Message concernant la modification de la loi fédérale sur les systèmes d'information de l'armée

du 24 novembre 2021

Messieurs les Présidents,
Mesdames, Messieurs,

Par le présent message, nous vous soumettons le projet de modification de la loi fédérale sur les systèmes d'information de l'armée en vous proposant de l'adopter.

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames, Messieurs, l'assurance de notre haute considération.

24 novembre 2021

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Guy Parmelin
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) utilise plusieurs systèmes d'information, en particulier de l'armée, dans lesquels des données personnelles sont traitées. Cette modification de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA) crée les bases légales voulues par la législation sur la protection des données afin que les données personnelles nécessaires à l'accomplissement des tâches soient disponibles à l'avenir également.

Contexte

Les besoins du DDPS liés au traitement des données personnelles avec ses systèmes d'information en vue de l'accomplissement optimal de ses tâches ont évolué, notamment en raison du développement de l'armée (DEVA). Afin de pouvoir traiter les données personnelles répondant à ces nouveaux besoins en toute légalité, une base légale suffisante au sens du droit de la protection des données est requise. Actuellement, la LSIA ne la fournit pas encore. Il est donc nécessaire de modifier ses dispositions relatives aux systèmes d'information et d'en créer de nouvelles pour les systèmes d'information récents.

Contenu du projet

Le projet prévoit de modifier non seulement les dispositions générales de la LSIA mais encore celles qui portent sur les systèmes d'information déjà réglementés par la LSIA et de les compléter par de nouvelles pour les systèmes d'information récents. Ces modifications concernent notamment:

- *le traitement de nouvelles données personnelles,*
- *le traitement de données personnelles pour atteindre de nouveaux buts,*
- *la collecte de données personnelles auprès d'autres services, personnes ou systèmes d'information,*
- *la communication de données personnelles à d'autres services, personnes ou systèmes d'information,*
- *le regroupement de systèmes d'information,*
- *la nouvelle réglementation des organes responsables des systèmes d'information,*
- *le changement des noms de certains systèmes d'information,*
- *la simplification de la transmission des données par des accès en ligne, par des interfaces et par des portails électroniques,*
- *la nouvelle réglementation de la durée de conservation des données.*

Table des matières

Message

1 Contexte

1.1 Nécessité d'agir et objectifs visés

Le Groupement Défense et les unités administratives qui lui sont subordonnées utilisent plusieurs systèmes d'information de l'armée. Le traitement de données personnelles que ces systèmes renferment est régi par la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA)[1]. Celle-ci comporte des dispositions concernant divers autres systèmes d'information contenant des données personnelles exploités par des unités du Département fédéral de la défense, de la protection de la population et des sports (DDPS) autres que le Groupement Défense.

Le processus global de *développement de l'armée* (DEVA) a nécessité une modification fondamentale des structures, de l'organisation et des processus au sein de l'armée et du Groupement Défense. Pour pouvoir continuer de remplir correctement les tâches, il faudra pouvoir traiter de nouvelles données personnelles (notamment des données sensibles) dans les systèmes d'information du Groupement Défense ou traiter les données existantes d'une autre manière. Il en va de même pour les systèmes d'information du DDPS utilisés en dehors du Groupement Défense.

Les bases légales qu'exige la protection des données (cf. art. 17 de la loi fédérale du 19 juin 1992 sur la protection des données [aLPD][2] et l'art. 34 de la loi fédérale du 25 septembre 2020 sur la protection des données [nLPD][3], laquelle remplacera l'aLPD) font encore défaut et doivent donc être créées.

1.2 Solution retenue

Pour permettre au DDPS de répondre aux exigences légales en matière de protection des données, les dispositions de la LSIA relatives aux systèmes d'information existants doivent être modifiées selon les besoins et des dispositions pour les nouveaux systèmes d'information créées.

1.3 Relation avec le programme de la législature, avec le plan financier et avec les stratégies du Conseil fédéral

Le projet n'est pas mentionné dans le message du 29 janvier 2020 sur le programme de la législature 2019 à 2023[4] ni dans l'arrêté fédéral du 21 septembre 2020 sur le

1 RS **510.91**
2 RS **235.1**
3 FF **2020** 7397
4 FF **2020** 1709

programme de la législature 2019 à 2023[5]. La modification des bases légales pour les systèmes d'information de l'armée et du DDPS est toutefois une condition à l'accomplissement optimal des tâches légales incombant au DDPS – ainsi qu'au Groupement Défense et à l'armée en particulier. Elle aide à réaliser divers objectifs et à concrétiser des mesures que ce programme mentionne (tel l'objectif 15: «La Suisse connaît les menaces qui pèsent sur sa sécurité et dispose des instruments nécessaires pour y parer efficacement»[6]). Elle contribue aussi à atteindre l'objectif fixé par le Conseil fédéral pour 2021 visant à fournir des prestations étatiques efficaces, autant que possible sous forme numérique[7]. Aucune conséquence sur la planification financière n'est à prévoir.

1.4 Questions sur la mise en œuvre

Le Conseil fédéral vise le 1er février 2023 comme date d'entrée en vigueur de la LSIA modifiée.

La modification doit trouver sa concrétisation dans les dispositions d'exécution à l'échelon réglementaire. Le Conseil fédéral et le DDPS élaboreront ces dispositions de telle sorte qu'elles entrent en vigueur en même temps que la modification.

1.5 Classement d'interventions parlementaires

Aucun mandat de motions ou de postulats n'est rempli.

2 Procédure préliminaire, consultation comprise

2.1 Procédure préliminaire et résultats de la consultation

Avant la consultation, aucun effet majeur du projet n'a été constaté, que ce soit sur l'environnement, la société, l'économie nationale, la santé, les régions ou l'étranger, d'où aucune analyse d'impact détaillée de la réglementation effectuée et aucune commission d'experts mise sur pied.

La consultation a duré du 20 mai au 11 septembre 2020[8]. Les parties consultées qui ont rendu un avis se sont toutes prononcées en faveur du projet, sans réserve ou en demandant quelques modifications.

5 FF **2020** 8087
6 FF **2020** 8087, 8093
7 FF **2020** 8087, 8088 (objectif 2); Objectifs du Conseil fédéral 2021, volume I, objectif 2, p. 10 ss; disponible sous www.chf.admin.ch > Documentation > Aide à la conduite stratégique > Les Objectifs.
8 Les résultats de la consultation sont disponibles sous www.admin.ch > Droit fédéral > Consultations > Procédures de consultation terminées > 2020 > DDPS.

Ci-après les sujets des demandes récurrentes formulées par un grand nombre d'entre elles.

- Prendre en compte les besoins des cantons en vue d'une gestion efficace et sûre des données personnelles.
- Ne pas masquer ou effacer les données dont les cantons ont besoin dans l'accomplissement de leurs tâches.
- Étendre le Système d'information sur le personnel de l'armée et de la protection civile (SIPA) au service civil et à ses membres pour permettre aux organes responsables de ce service de gérer les jours accomplis dans le SIPA. Ces données seraient ainsi disponibles dans le système de gestion de la taxe d'exemption de servir (qui est connecté au SIPA) et il serait possible de percevoir ladite taxe ou de la rembourser une fois les obligations de servir remplies (une des parties a proposé comme alternative une interface de E-CIVI avec les systèmes de gestion de la taxe d'exemption).
- Prolonger la durée de conservation, qui parfois ne suffit pas, de certaines données du SIPA visées à l'art. 17, al. 5 (de cinq ans au plus après la libération de l'obligation de servir dans l'armée ou dans la protection civile à dix ans au plus).
- Prendre en compte les règles de la loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (LPPCi)[9], entrée en vigueur le 1er janvier 2021.
- Prendre en compte les règles de la nLPD.

Pour le reste, il s'agit exclusivement de demandes particulières émanant de l'une ou l'autre des parties.

Les détails de ces demandes sont repris dans le rapport correspondant.

2.2 Appréciation des résultats

2.2.1 Demandes examinées et autres modifications

Sur la base des demandes formulées lors de la consultation, les modifications majeures ci-après, d'ordre généralement matériel, ont été apportées au projet.

- Adaptation à la nLPD par la modification de l'art. 1, al. 1, et de l'art. 2, al. 6, et par l'introduction à l'art. 2*b* d'une base permettant de traiter les données par le profilage et le profilage à risque élevé.
- Modification des renvois à la nouvelle LPPCi aux art. 15, al. 2, let. a, et 17, al. 1, let. e.
- Mention explicite de l'armée en plus du DDPS dans la phrase introductive de l'art. 1, al. 1, afin de délimiter clairement les champs de compétences (par analogie à la limite fixée à l'al. 1 entre l'armée et l'administration militaire).

9 RS **520.1**

– Diminution de la durée de conservation des données du Système d'information sur la protection préventive de l'armée (SIPPA) prévue à l'art. 167*l*.

En outre, les compléments ci-après ont été apportés dans les commentaires relatifs aux dispositions suite à des demandes.

– Renvois à la nLPD et à la LPPCi.
– Explication complémentaire pour justifier la prolongation de la durée de conservation prévue à l'art. 125, al. 2.
– Précision sur le fait que les données collectées sur la base de l'art. 167*j* peuvent être communiquées quelle que soit la manière dont elles ont été acquises.
– Précision du terme *partenaires potentiels* avancé dans l'art. 179*p*, let. a.
– Explications complémentaires sur l'art. 186, al. 3, avec remarque sur la collaboration internationale au sens de l'art. 6 comme cas d'application où le Conseil fédéral peut conclure un accord sur le traitement transfrontalier de certaines données personnelles.

En outre, les modifications ci-après, qui n'ont pas été demandées lors de la consultation, ont été apportées au projet et au rapport explicatif.

– L'art. 1, al. 2, et les explications correspondantes ont été légèrement reformulés pour préciser que la LSIA ne s'applique pas au traitement des données par le Service de renseignement de la Confédération (SRC) ou par le Service de renseignement de l'armée (SRA).
– Le traitement de certaines données du SIPA et du Système d'information pour l'administration des prestations (MIL Office) ne permettra plus seulement d'empêcher tout abus dans le cadre des allocations pour perte de gain, mais aussi d'exécuter le régime de ces allocations (cf. modifications correspondantes aux art. 13, let. f, 16, al. 1, let. h, 85, al. 2, et 88, let. d, et dans les commentaires les concernant).
– L'ajout de *au plus* à l'art. 17, al. 4^{quater}, indique que les données ne doivent pas être conservées obligatoirement pendant cinq ans.
– La modification l'art. 140, let. c et d, précise que le Système d'information sur la circulation routière et la navigation de l'armée (SI OCRNA) ne doit contenir que les résultats du dernier examen de contrôle et la date de l'examen suivant, à l'exclusion des données d'examens plus anciens.
– À l'art. 143*c*, let. l, les données à traiter dans le Système d'information pour l'instruction et le perfectionnement aéronautiques (SPHAIR-Expert) ont été complétées.
– Le but du Système d'information sur le contrôle de sécurité relatif aux personnes (SICSP) a été précisé à l'art. 145.
– À l'art. 147, al. 2, let. c, le système de traitement des données relatives à la protection de l'État, qui n'existe plus, est remplacé par le système d'indexation des données du SRC (INDEX SRC). Les commentaires ont été complétés en ce sens.

– La communication de données du SIPPA à l'Office fédéral de la police sera aussi possible (cf. art. 167*k*, al. 2, let. h).

– Le Système d'information de l'administration des fédérations et des sociétés de tir (AFS) a été remplacé par le Système d'information du tir hors du service (SaD) (art. 179*g* à 179*l* et titre précédant l'art. 179*g*).

– À cela s'ajoutent des modifications linguistiques ou techniques mineures sans effets matériels (p. ex. la modification du titre précédant l'art. 168 ou le renvoi à la LSIA dans l'art. 146 de la loi du 3 février 1995 sur l'armée [LAAM][10]).

2.2.2 Demandes non retenues

Certaines demandes n'ont pas été retenues pour les raisons énumérées ci-après.

– Certaines parties réclamaient globalement le respect des principes généraux de la législation sur la protection des données et notamment des dispositions de l'aLPD. L'art. 1, al. 3, LSIA renvoie à l'aLPD. Sauf dispositions contraires dans la LSIA, ces principes valent dès lors d'emblée pour tous les systèmes visés. Il est donc inutile de modifier la loi pour les concrétiser davantage. La loi contient en outre pour chaque système des dispositions qui règlent en détail la collecte des données (quelles données, à quelles fins, auprès de qui) et leur traitement (comment, pendant combien de temps, communication à qui). Ces principes se concrétisent de surcroît dans les règlements de traitement (cf. art. 36, al. 4, aLPD, en relation avec l'art. 21 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données [OLPD][11]) ou plus précisément dans les registres des activités de traitement (cf. art. 12 nLPD) qui existent pour chaque système. De cette manière, le respect des principes généraux de la protection des données est garanti – notamment le traitement de données licite, proportionné et dans un but donné (art. 4, al. 1 à 3, aLPD et art. 6, al. 1 à 3, nLPD).

– Les dispositions ne précisent pas, comme certaines parties le demandaient, si les données peuvent être communiquées d'office ou sur demande des personnes intéressées. Si une communication des données est prévue sans autre précision, cela signifie qu'elle est et doit être possible d'office et sur demande, dans la mesure où elle est nécessaire pour atteindre le but visé et pour accomplir au mieux les tâches qui en dépendent.

– La demande de modification du titre de l'acte *loi fédérale sur les systèmes d'information de l'armée et du DDPS* en *loi fédérale sur les systèmes d'information de l'armée et sur les systèmes d'information du DDPS* n'a pas été retenue. Les systèmes de l'armée réglés par la LSIA sont utilisés par le Groupement Défense et les unités administratives ou les offices qui lui sont subordonnés – c'est-à-dire l'administration militaire – et mis en particulier à la disposition de l'armée. L'administration militaire faisant partie du DDPS,

10 RS **510.10**
11 RS **235.11**

ses systèmes d'information sont donc ceux qu'utilise ce département. Aucune subordination de l'armée au DDPS ne ressort du nouveau titre.

– Les règles concernant la durée d'archivage des données ou leur effacement des archives n'ont pas été reprises à l'art. 8. L'archivage n'est pas réglé par la LSIA, mais par la loi fédérale du 26 juin 1998 sur l'archivage (LAr)[12]. Un renvoi purement déclaratif à la LAr dans l'art. 8 est inutile.

– Il n'a pas été jugé nécessaire de préciser dans le commentaire relatif à l'art. 8 qu'il fallait absolument prendre en considération les besoins des cantons avant de détruire certaines données, dont ils ont absolument besoin. L'art. 8 est une disposition générale, qui s'applique à l'ensemble des systèmes réglés par la LSIA. Il découle du principe de la proportionnalité (cf. art. 4, al. 2, aLPD et art. 6, al. 2 et 4, nLPD) et indique globalement qu'il faut détruire les données qui n'ont plus d'utilité. Le but et la durée de la mise à disposition des données d'un système d'information spécifique pour les cantons, tant qu'ils en ont besoin dans un but particulier, ne font pas l'objet de l'art. 8. Ces points sont réglés dans des dispositions particulières pour chaque système (cf. notamment les dispositions concernant le but du traitement, la communication et la conservation des données).

– Il n'est pas prévu d'étendre le SIPA au service civil. La préparation, la réalisation et l'administration des engagements de ses membres sont gérées dans le système d'information E-CIVI (cf. art. 80 de la loi fédérale du 6 octobre 1995 sur le service civil [LSC][13], en relation avec l'ordonnance du 20 août 2014 sur le système d'information du service civil[14]). La gestion des données prévue par la loi a du sens car les besoins du service civil diffèrent de ceux de l'armée et de la protection civile dans les domaines de la préparation, de l'administration et du décompte des jours effectués. Le développement et la gestion d'E-CIVI incombent à l'Office fédéral du service civil (CIVI), rattaché au Département fédéral de l'économie, de la formation et de la recherche. En ce qui concerne les problèmes soulevés par les cantons en rapport avec la perception de la taxe d'exemption auprès des personnes astreintes au service civil et son remboursement après l'accomplissement de leur obligation de servir, renvoi est fait à la possibilité de raccordement en ligne au système d'information prévue par l'art. 80, al. 2, let. e, LSC. Concrètement, cela passe par l'entité compétente qui est le CIVI. Ce point n'est pas abordé dans ce projet car il ne tombe pas dans le domaine réglementé par la LSIA, qui se limite au traitement des données dans les systèmes d'information du DDPS (cf. art. 1, al. 1, P-LSIA).

– Le fait que les dispositions d'exécution édictées en vertu de art. 186, al. 1, let. a, LSIA désignent le commandement de l'Instruction comme maître du fichier SIPA et organe fédéral responsable d'assurer la protection des données qu'il contient (cf. art. 2*a*, en relation avec l'annexe 1 de l'ordonnance du

12 RS **152.1**
13 RS **824.0**
14 RS **824.095**

16 décembre 2009 sur les systèmes d'information de l'armée [OSIAr][15]) n'a rien d'incohérent et n'exige donc pas de modifier le projet. L'art. 13 LSIA prévoit en effet que le SIPA, qui contient aussi des données sur les membres de la protection civile, est géré par le Groupement Défense et non par un service ou une autorité responsable de la protection civile. La responsabilité générale du SIPA et de la protection des données qui y sont traitées incombe donc au Groupement Défense. C'est ensuite le Conseil fédéral qui désigne plus précisément l'unité administrative compétente pour la protection des données (en l'occurrence le commandement de l'Instruction), comme il le fait pour tous les systèmes d'information gérés par le Groupement Défense en vertu de la LSIA. Le Groupement Défense assumant la responsabilité (globale) de la protection des données du SIPA et les services et autorités de la protection civile étant chargés d'y contrôler les membres de la protection civile (cf. art. 47, al. 1, LPPCi) et d'y saisir les données requises, il faut donc que le Groupement Défense leur donne un accès en ligne à ces données (cf. art. 16, al. 1, let. f, LSIA).

– Il n'a pas été jugé nécessaire d'ajouter les personnes tenues de s'annoncer dans la phrase introductive de l'art. 14, al. 1. Cet alinéa règle uniquement les données contenues dans le SIPA concernant les personnes qui appartiennent à un groupe en lien avec l'armée, celles sur les personnes astreintes à la protection civile ou au service civil étant réglées aux al. 2 et 3. Pour l'armée, les personnes tenues de s'annoncer sont les conscrits et les personnes astreintes au service militaire (cf. art. 27, al. 1, LAAM). Ceux-ci étant déjà cités à l'al. 1, aucune précision supplémentaire n'est nécessaire.

– Le terme *personne astreinte au service civil*, qui est très courant, n'a pas été remplacé, dans la phrase introductive de l'art. 14, al. 2, par *personne astreinte au service militaire accomplissant volontairement un service de remplacement*. Dans toute la LSC, il est question de service civil, *d'astreinte au service civil* et de *personne astreinte au service civil*. Le terme service de remplacement apparaît uniquement dans le titre de l'acte et à l'art. 1, dans lequel service civil est introduit entre parenthèses comme raccourci pour le *service civil de remplacement*. Pour des raisons de cohérence, il faut donc respecter cette terminologie à l'art. 14, al. 2.

– La durée de conservation des données de cinq ans au plus, prévue par l'art. 17, al. 5, n'a pas été prolongée à dix ans. Le début de la durée maximale de conservation de cinq ans n'a pas non plus été lié au versement complet de la taxe d'exemption de l'obligation de servir, lequel intervient parfois après la libération des obligations militaires ou de l'obligation de servir dans la protection civile. De plus, la possibilité de conserver les données dans certains cas jusqu'à l'année où la personne concernée atteint l'âge de 40 ans n'a pas été ajoutée à l'al. 3. Le but du SIPA est en priorité de contrôler les militaires et les membres de la protection civile et non de percevoir et de contrôler la taxe d'exemption (cf. art. 13). Les problèmes liés à cette taxe ne justifient donc pas de prolonger la durée de conservation des données. Une telle prolongation

15 RS **510.911**

serait contraire au principe de la proportionnalité inscrit dans la législation sur la protection des données, qui prévoit que les données ne peuvent être traitées que pour la durée nécessaire à atteindre le but visé lors de leur collecte. Elle impliquerait en outre d'ajouter cinq classes d'âge supplémentaires au traitement et à la mise à jour automatisés des données tirées des registres communaux et fournies conformément à l'obligation d'annoncer, ce qui représenterait près de 71 500 militaires et 35 000 membres de la protection civile. Vu que le système actuel fonctionne déjà à la limite de ses capacités, il faudrait le développer pour éviter qu'il s'écroule complètement. Les coûts supplémentaires que cela engendrerait ne sont pas connus, mais ils seraient de toute façon disproportionnés par rapport à l'utilité attendue. Enfin, relier le début de la durée de conservation maximale des données au versement complet de la taxe d'exemption de l'obligation de servir n'est pas réalisable car cette date ne figure pas dans le SIPA et n'est donc pas connue du Groupement Défense.

– Une des parties consultées pense que l'abrogation de l'art. 47, al. 1, risque d'affaiblir la protection des données. Cette crainte est infondée. Le Système d'information de médecine aéronautique (MEDIS FA) est un système autonome, séparé des autres systèmes. Il gère ses propres données et les droits d'accès y sont réglés spécifiquement. Les données du MEDIS FA ne sont pas conservées au-delà du délai légal prévu à l'art. 47. Elles sont archivées par les Archives fédérales et non par le Groupement Défense (ou l'Institut de médecine aéronautique). Une fois les données proposées aux Archives fédérales, celles qui n'ont pas de valeur archivistique sont détruites par le Groupement Défense (cf. art. 8).

– L'art. 56 ne précisera pas ce qu'on entend par *documents personnels nécessaires à l'évaluation des prestations de conseil et de prise en charge*. Le Service social de l'armée adopte une approche globale pour ses prestations de conseil et de prise en charge, qui peuvent prendre des formes très variées. Ainsi, leur appréciation peut requérir toutes sortes de documents. Il faut donc rester vague dans la définition des *documents personnels* visés à l'art. 56. Une définition plus précise des documents pouvant être traités dans le système reviendrait à restreindre l'étendue des mesures sociales pouvant être proposées. Ces mesures pourraient éventuellement ne plus bénéficier d'une appréciation suffisante et donc ne plus être accordées si les documents nécessaires font défaut. Au final, les personnes désireuses d'obtenir un soutien social en pâtiraient. Il faut aussi ne pas perdre de vue que le recours au conseil et à la prise en charge ainsi que la soumission de documents personnels sont des démarches volontaires de la part de la personne concernée. Celle-ci reste libre de ne pas présenter de documents ou de ne pas prétendre à des mesures sociales.

– Une réduction des durées de conservation des données, prévues notamment aux art. 125, al. 2, 131, 143, al. 1 et 2, 173 et 179*r*, al. 2, n'a pas pu être prise en considération. Les commentaires relatifs aux dispositions concernées indiquent en partie que les données doivent être conservées la durée prévue afin d'accomplir correctement des tâches administratives et les contrôles.

– La garantie de la sécurité des données dans les systèmes d'information (p. ex. le JORASYS) n'a pas été précisée davantage. Cette question ne doit pas être réglée spécifiquement pour chaque système dans la LSIA. Un renvoi aux dispositions générales de l'aLPD, qui s'appliquent en principe aussi à ces systèmes (art. 1, al. 3, LSIA), est plus approprié. Le maître du fichier et propriétaire des données est garant de la sécurité des données (cf. art. 16, al. 1, aLPD en relation avec l'art. 7 aLPD et les art. 20 ss OLPD; art. 10*a*, al. 2, aLPD, en relation avec l'art. 22 OLPD, en particulier pour ce qui est du traitement des données par des fournisseurs externes de prestations mandatés conformément à l'art. 7, al. 2, P-LSIA; dans la nLPD, les dispositions pertinentes se trouvent à l'art. 7, en relation avec l'art. 5, let. j, à l'art. 8, en relation avec les art. 20 ss OLPD et à l'art. 9, al. 2, en relation avec l'art. 22 OLPD). Le maître du fichier doit prendre des mesures techniques et organisationnelles adaptées pour protéger les données personnelles contre toute utilisation abusive (art. 7, al. 1, aLPD et art. 8, al. 1 et 2, nLPD). Un règlement doit aussi être tenu pour les activités de traitement; il doit décrire globalement les mesures techniques et organisationnelles destinées à garantir la sécurité des données (cf. art. 21, al. 2, OLPD; et art. 12, al. 2, let. f, nLPD, qui fait de ce point un élément dont il faudra tenir compte dans les futurs registres des activités). Les mesures particulières à prendre doivent être évaluées et fixées pour chaque cas de traitement de données en tenant compte des risques spécifiques.

– Quelques demandes de modification relatives au SIPPA n'ont pas été retenues. Une partie consultée réclamait d'abroger purement et simplement les dispositions sur le SIPPA, ce qui n'est pas envisageable car ce système, dont le Service de protection préventive de l'armée (SPPA) a besoin pour remplir ses tâches, nécessite une base légale pouvant légitimer le traitement des données personnelles requises. Il n'y a pas non plus lieu de craindre que certaines données détenues par des services de renseignement étrangers soient utilisées par le domaine Personnel de l'armée sans la moindre vérification, par exemple dans l'évaluation des carrières des cadres militaires (de telles évaluations et l'examen des bases décisionnelles se déroulent selon des processus contraignants). Le traitement des orientations politiques et idéologiques visé à l'art. 167*i*, let. e, mérite d'être maintenu car il peut fournir des renseignements sur des connexions avec le terrorisme, l'extrémisme violent (émanant p. ex. de groupements radicaux ou d'extrémistes religieux) ou l'espionnage, lesquelles peuvent représenter une menace pour l'armée. Les rapports et la collaboration entre le SPPA et le SRC n'ont pas à être clarifiés dans les dispositions de la LSIA et les explications correspondantes, dont ils ne font pas partie du champ d'application. Il suffit de renvoyer aux dispositions pertinentes de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens; notamment art. 11, 19, 20 et 60)[16] et à l'art. 100, al. 1, let. a, et 4, let. b, LAAM, ainsi qu'aux dispositions d'exécution correspondantes du Conseil fédéral (cf. art. 1 et 4 et annexe 3, ch. 10.3, de l'ordonnance du 16 août 2017 sur le renseignement [ORens][17] et art. 3 de l'ordonnance du 21 novembre 2018

16 RS **121**
17 RS **121.1**

sur la sécurité militaire [OSM][18]). La collaboration entre le SPPA et d'autres partenaires, tels des services de renseignement nationaux et étrangers, est soumise chaque année à l'approbation préalable du Conseil fédéral dans le cadre de la politique commune à l'égard des services partenaires du SRA et du SRC (art. 7 et 8 ORens).

3 Présentation du projet

Le projet prévoit de modifier les dispositions de la LSIA relatives à plusieurs systèmes d'information et d'en établir pour les nouveaux. Ces modifications consistent à:

- étendre l'objet et le champ d'application de la LSIA aux systèmes d'information du DDPS, y compris la modification du titre de l'acte et d'autres modifications rendues ainsi nécessaires dans d'autres dispositions;
- créer une base légale pour l'utilisation et le traitement du numéro AVS dans les systèmes d'information du DDPS ne relevant pas de l'armée;
- intégrer dans le réseau des systèmes d'information ceux réglés par les dispositions d'exécution de la LSIA;
- communiquer les données personnelles aux fournisseurs externes de prestations informatiques chargés des tâches de maintenance, d'entretien et de programmation;
- intégrer le Système d'information sur le recrutement (SIR) et la banque de données cliniques du Service psycho-pédagogique de l'armée (banque de données SPP) dans le Système d'information sur le personnel de l'armée et de la protection civile (SIPA);
- créer une base légale pour le traitement de données personnelles supplémentaires dans divers systèmes d'information (SIPA, Système d'information sur l'évaluation du détachement de reconnaissance de l'armée [EDRA], Système d'information sur les autorisations de conduire militaires [SIAC]);
- préciser la base légale pour le traitement des données personnelles dans le Système d'information du Centre de dommages du DDPS (SCHAMIS);
- créer une base légale permettant d'acquérir des données personnelles traitées dans les systèmes d'information ou lors de l'engagement de moyens de surveillance auprès d'autres services, personnes ou systèmes d'information, de les communiquer à ces derniers, voire de les traiter à de nouvelles fins;
- désigner le Groupement Défense comme exploitant de divers systèmes d'information (SIPA, Systèmes d'information sur les patients [SIPAT], MEDIS FA, Système d'information du domaine social [SISOC], Système d'information et de conduite du Service sanitaire coordonné [SIC SSC]), ce qui permet

18 RS **513.61**

de définir les unités administratives subordonnées – maîtres du fichier et organes fédéraux responsables de la protection des données – dans les dispositions d'exécution à l'échelon réglementaire;

– renommer certains systèmes d'information (EDRA, SISOC, SIAC, Système de journal et de rapport de la Sécurité militaire [JORASYS], SCHAMIS, Système d'information stratégique de la logistique [SISLOG], AFS);
– créer une base légale permettant l'utilisation de certaines données du MIL Office afin d'exécuter le régime des allocations pour perte de gain, ainsi que leur communication à la centrale de compensation;
– régler l'utilisation d'un portail électronique pour la transmission volontaire aux commandements militaires compétents des données personnelles traitées dans MIL Office (p. ex. des demandes de congé documentées);
– prolonger la durée de conservation des données personnelles (Systèmes d'information pour les simulateurs [SISIM], Système d'information pour la gestion de l'instruction [Learning Management System, LMS DDPS], SIAC) ou la réglementer pour MEDIS FA, JORASYS;
– permettre l'accès à des données en ligne ou automatiquement par une interface (SICSP, JORASYS);
– établir une réglementation pour le Système d'information sur la protection préventive de l'armée (SIPPA; sert au SPPA pour l'accomplissement de ses tâches et pour la tenue d'un journal et la gestion de ses engagements) et pour le Système d'information *Master Data Management* (MDM; vise l'administration et la préparation de données de base communes et formelles de partenaires commerciaux pour divers processus d'affaires concernant le DDPS);
– apporter des modifications formelles, d'ordre linguistique ou en rapport avec la technique législative (dispositions générales, SIPA, Système d'information médicale de l'armée [MEDISA], MEDIS FA, EDRA, SISOC, Système d'information sur le personnel du Groupement Défense [SIP DEF], SIC SSC, MIL Office, Système d'information pour la gestion des compétences [SIGC], Système d'information et de conduite des Forces terrestres [SIC FT], Système d'information et de conduite du soldat [SICS], SIAC, SICSP, JORASYS, SCHAMIS, SISLOG, Système d'information pour la gestion intégrée des ressources [PSN]).

4 Commentaire des dispositions

4.1 Loi fédérale sur les systèmes d'information de l'armée (LSIA)

Titre

La LSIA règle déjà le traitement des données personnelles dans divers systèmes d'information qu'utilisent d'autres unités administratives du DDPS que celles du Groupement Défense. Le titre de l'acte, qui se limite jusqu'ici aux systèmes d'information de

l'armée, doit donc être élargi à l'ensemble du département, tout en maintenant le sigle actuel.

Préambule

Les dispositions mentionnées dans le préambule (art. 40, al. 2, et art. 60, al. 1, Cst.[19]) constituent la base légale de la réglementation des systèmes d'information de l'armée. Le projet visant à étendre cette base aux systèmes d'information du DDPS régis par la LSIA qui n'ont pas de caractère militaire, il faut y ajouter, faute d'une délégation de compétence explicite à la Confédération et conformément à la pratique, l'art. 173, al. 2, Cst.

Remplacement d'une expression

Dans tout l'acte *numéro d'assuré AVS* est remplacé par *numéro AVS*, qui est plus court et plus usité. Il s'agit également de la forme qui s'est imposée dans le reste de la législation.

Art. 1, al. 1, phrase introductive et let. b à d, 2 et 3

Le champ d'application est trop restreint. Il faut ajouter à la liste des systèmes d'information de l'armée déjà régis par la LSIA ceux du DDPS qui n'ont pas de caractère militaire (art. 1, al. 1, phrase introductive). Comme les données personnelles contenues dans ces derniers ne sont pas seulement traitées en vue de l'accomplissement de tâches en lien avec les affaires militaires, mais aussi d'autres tâches du DDPS, il est nécessaire de compléter l'art. 1, al. 1, let. d. De plus, des données personnelles en rapport avec la protection civile sont traitées dans divers systèmes d'information régis par la LSIA. C'est pourquoi il est prévu de mentionner aussi dans l'art. 1, al. 1, let. b et c, les membres de la protection civile et dans la let. d les personnes remplissant des tâches relevant de celle-ci.

Pour des raisons de clarté, il convient de préciser dans la phrase introductive de l'al. 1 que le traitement des données personnelles relevant du champ d'application de la LSIA concerne aussi bien des personnes physiques que morales. Cette précision est compatible avec la nLPD. En effet, la nLPD ne concernera plus que le traitement des données personnelles de personnes physiques (art. 2, al. 1, nLPD) et la définition des données personnelles à l'art. 5, let. a, nLPD ne s'appliquera par conséquent plus qu'à ces personnes. En revanche, les dispositions de la LSIA prévoient parfois le traitement des données personnelles de personnes morales. La définition des *données personnelles* sera ainsi plus large que dans la nLPD. Cela étant précisé dans l'al. 1, on évite d'emblée que la définition plus étroite de la nLPD s'applique aussi au domaine de la LSIA en vertu de l'al. 3. La LSIA réglant des particularités, elle prime la nLPD.

Les *profils de la personnalité* peuvent être supprimés de la phrase introductive. Ils sont en effet couverts par le terme *données personnelles* et ont aussi disparu de la nLPD. Une réglementation est en revanche prévue à l'art. 2*b* pour le *profilage*, qui est également réglé dans la nLPD. La phrase introductive précisera aussi que la LSIA a

19 RS **101**

pour objet le traitement de toutes les *données personnelles*, et pas uniquement celui des données personnelles sensibles.

Pour ne pas devoir revenir sur les modifications faites dans la phrase introductive après l'entrée en vigueur de la nLPD – qui prévoyait d'autres formulations –, une disposition de coordination est prévue dans la LSIA modifiée (cf. ch. 5.1).

L'art. 1, al. 2, précise que le traitement de données par le SRC et le SRA (réglé dans d'autres actes) est exclu du champ d'application, mais pas le traitement de données concernant ces services et leur personnel.

Le sigle de l'*aLPD* est introduit à l'art. 1, al. 3, et réutilisé dans le reste de l'acte aux art. 6, let. b, et 186, al. 3. Pour que ce sigle reste valable après l'entrée en vigueur de la nLPD, il faut prévoir une disposition de coordination dans la LSIA modifiée (cf. ch. 5.1).

Art. 2, al. 1, phrase introductive et let. a

En raison de l'extension du champ d'application de la LSIA (cf. commentaire relatif à l'art. 1, al. 1, phrase introductive), les dispositions générales, en particulier l'art. 2, s'appliquent aussi aux systèmes d'information du DDPS qui n'ont pas de caractère militaire. C'est ce que souligne la phrase introductive de l'art. 2, al. 1. Cette extension crée notamment la base légale nécessaire à l'utilisation du numéro AVS dans les systèmes d'information autres que militaires du DDPS conformément à l'art. 50*e*, al. 1, de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[20]. Dans le cadre de l'accomplissement des tâches légales, de nombreux points de contact existent entre les différentes unités administratives du DDPS n'appartenant pas au Groupement Défense, d'une part, et entre l'armée et l'administration militaire d'autre part, d'où l'exploitation de divers systèmes d'information dans l'ensemble du DDPS (p. ex. LMS DDPS, système de gestion des identités [ICAM]). Le recours aux numéros AVS pour identifier les personnes s'impose donc aussi dans les domaines autres que militaires afin de garantir que les activités administratives et l'accomplissement des tâches soient efficaces.

L'art. 2, al. 1, let. a, sera abrogé car les art. 17 et 19, al. 3, aLPD (art. 34 nLPD), applicables en vertu de l'art. 1, al. 3, LSIA, disposent qu'une base légale est nécessaire pour le traitement de données personnelles et précisent que celle-ci doit être prévue expressément dans une loi au sens formel. Le traitement des données non sensibles ne requiert en principe pas de base légale inscrite dans une loi au sens formel, si tant est qu'il ne permet pas d'établir des profils de la personnalité. Une disposition dans une ordonnance du Conseil fédéral est suffisante (cf. art. 17 et 19, al. 3, aLPD ou art. 34, al. 1 et 2, nLPD, et 186, al. 1, let. b, LSIA).

Art. 2b Profilage

La possibilité de traiter des données à certaines fins par un profilage, y compris un profilage à risque élevé, est prévue par l'art. 2*b*. Ces deux types de traitement sont

20 RS **831.10**

aussi réglés dans la nLPD[21]. On entend par profilage *toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* (art. 5, let. f, nLPD). Et par profilage à risque élevé *tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique* (art. 5, let. g, nLPD). La nouvelle réglementation prévue à l'art. 2*b* établira la base légale dans une loi au sens formel comme l'exige l'art. 34, al 2, let. b, nLPD pour le profilage et le profilage à risque élevé. Elle prévoit d'autoriser le traitement de certains aspects personnels relatifs à une personne physique par le profilage, y compris par le profilage à risque élevé selon les modalités suivantes.

Évaluation de données pour analyser ou prédire les **aspects personnels** suivants	Aux **fins de traitement** prévus par la LSIA					
	Art. 13 (SIPA)	**Art. 127** (LMS DDPS)	**Art. 143*b*** (SPHAIR-Expert)	**Art. 143*b*** (SIIC)	**Art. 145** (SICSP)	**Autres**
Aptitude et capacité à accomplir du service militaire et du service de protection civile, y compris les conditions déterminantes correspondantes	**x** (let. b à d)					
Aptitude à exercer des fonctions, à effectuer des activités et à réaliser des travaux, y compris les conditions déterminantes correspondantes	**x** (let. b à d)		**x** (let. d et e)			
Profil de prestations et performances, notamment dans les domaines de la santé, de l'aptitude physique, de l'intelligence, de la personnalité, du psychisme, du comportement social et de l'attitude au volant	**x** (let. b à d)		**x** (let. d et e)			
Connaissances, compétences, capacités et prestations fournies	**x** (let. b à d)	**x** (let. d et e)	**x** (let. d et e)	**x**		
Comportement d'apprentissage et progression		**x** (let. a à c)				

21 FF **2020** 7397

Évaluation de données pour analyser ou prédire les **aspects personnels** suivants	Aux **fins de traitement** prévus par la LSIA					
	Art. 13 (SIPA)	**Art. 127** (LMS DDPS)	**Art. 143*b*** (SPHAIR-Expert)	**Art. 143*h*** (SIIC)	**Art. 145** (SICSP)	**Autres**
Potentiel de cadre et possibilités de développement	**x** (let. b à d et m)					
Intérêt personnel porté au service militaire et au service de protection civile, à l'embauche, à la formation (instruction) et au perfectionnement	**x** (let. b à d et m)	**x** (let. b)	**x** (let. a, d et e)			
Risque pour la sécurité ainsi que potentiel d'abus et de dangerosité en ce qui concerne l'arme personnelle	**x** (let. l)				**x**	
Aspects personnels supplémentaires						**x** (avec le consentement de la personne concernée)

L'art. 2*b* n'autorise pas d'autre traitement de données que celui déjà appliqué par les organes responsables (p. ex. lors du recrutement), à l'exception du traitement des données que le système d'information SPHAIR-Expert prévoit conformément à la let. g (cf. commentaire relatif à l'art. 143*c*, let. l). Sur ce point, l'art. 2*b* constitue uniquement une adaptation des bases légales aux exigences relatives au niveau normatif posées par la nLPD.

Art. 3

L'extension du champ d'application de la LSIA (cf. commentaire relatif à l'art. 1, al. 1, phrase introductive) permet d'envisager d'autres prestataires que la Base d'aide au commandement pour les systèmes d'information du DDPS qui n'ont pas de caractère militaire en particulier. L'art. 3 (Exploitation des systèmes d'information) sera donc abrogé. Les exploitants techniques d'un système d'information donné pourront, par exemple, être désignés dans le règlement de traitement (art. 36, al. 4, aLPD, en relation avec l'art. 21 OLPD), puis dans le registre des activités de traitement (art. 12 nLPD).

Art. 4, al. 1

En raison de l'extension du champ d'application de la LSIA (cf. commentaire relatif à l'art. 1, al. 1, phrase introductive), la modification de l'art. 4, al. 1, prévoit que les systèmes d'information du DDPS qui n'ont pas de caractère militaire puissent être intégrés au réseau des systèmes d'information réglé par l'art. 4. Par ailleurs, les dispositions d'exécution de la LSIA prévoient également l'intégration des systèmes d'information visés uniquement dans l'ordonnance au réseau mentionné à l'art. 4 LSIA (cf. art. 2, al. 2, OSIAr). Par souci d'exhaustivité, il est prévu d'inscrire cette règle au niveau de la loi.

Art. 6 Traitement des données dans le cadre de la coopération internationale

Actuellement, l'art. 6 définit les exigences en matière de niveau de réglementation (loi formelle ou traité international sujet au référendum) pour les bases légales relatives au traitement des données personnelles sensibles et des profils de la personnalité dans le cadre de la coopération internationale (champ d'application selon l'actuel art. 1, al. 1). Pour que ces exigences ne soient pas applicables aux données personnelles non sensibles, qui entreront dans le champ d'application étendu de la LSIA modifiée (cf. commentaire relatif à l'art. 1, al. 1, phrase introductive), il faut modifier l'art. 6. Pour le traitement des données personnelles non sensibles dans le cadre de la coopération internationale visée à l'art. 6, les dispositions d'exécution de la LSIA édictées par le Conseil fédéral ou un accord international conclu par ce dernier suffiront. Étant donné que les art. 17, al. 2, et 19, al. 3, aLPD, ne requièrent une réglementation inscrite dans une loi au sens formel que pour le traitement de données personnelles sensibles et de profils de la personnalité, le niveau de réglementation demandé semble adéquat. La nLPD n'exigera pas non plus de loi au sens formel pour traiter les données personnelles non sensibles (art. 34, al. 2, nLPD).

Art. 7, al. 2, 1re phrase

Les fournisseurs de prestations informatiques internes à la Confédération sont amenés, pour des raisons de coûts et d'efficacité, à travailler avec des prestataires externes à leur unité administrative ou à l'administration fédérale. Il peut ainsi arriver que, pour pouvoir maintenir en fonction les systèmes d'information ou limiter les périodes d'interruption lors de l'exécution de tâches de maintenance, de gestion et de programmation, ils doivent leur permettre d'accéder à des données personnelles qui ne sont pas généralement accessibles. Par souci de clarté, il est donc nécessaire de préciser dans la première phrase de l'art. 7, al. 2, que ces prestataires externes comptent aussi parmi les personnes autorisées à traiter des données dans le respect des conditions prévues.

Art. 8 Conservation, archivage et destruction des données

Il est prévu de simplifier l'art. 8 et de l'adapter au déroulement chronologique de la conservation et de l'archivage des données. On mentionnera d'abord la proposition d'archivage, et ensuite seulement la destruction des données. Il sera uniquement question que de destruction des données (avec impossibilité de les récupérer) et plus d'effacement.

Art. 11

Le but et les modalités de traitement des données personnelles de même que leur durée de conservation sont réglés dans les dispositions particulières relatives à chaque système d'information. L'art. 11 (Données dont le traitement est restreint) peut donc être abrogé.

Afin que l'abrogation de cet article ne soit pas annulée par l'entrée en vigueur de la nLPD, laquelle prévoyait de l'adapter, une disposition de coordination est prévue dans la LSIA modifiée (cf. ch. 5.1).

Art. 13, let. f et n à p, art. 14, al. 1, let. a^{bis}, c^{bis} et n, 2, phrase introductive, et 4, art. 15, al. 1, phrase introductive, 2, let. a, et 4, art. 16, al. 1, phrase introductive et let. b^{bis}, h et i, et 1ter, et art. 17, al. 1, let. e, 4ter, 4^{quater} et 5 (SIPA)

La réglementation en vigueur du SIPA sera adaptée aux réalités et besoins actuels, voire étoffée.

Les changements principaux concernent l'intégration dans le SIPA de deux systèmes d'information, le SIR (art. 18 ss) et la banque de données SPP (art. 36 ss).

Pour l'intégration du SIR, les dispositions du SIPA seront adaptées comme suit.

- L'art. 14, al. 1, let. a^{bis}, reprend sans le modifier le catalogue des données visé à l'actuel art. 20, al. 2, LSIA.
- L'art. 16, al. 1, phrase introductive et let. b^{bis}, reprend l'art. 22, al. 1, et permettra aux médecins chargés du recrutement de continuer à accéder aux données dont ils ont besoin, notamment à celles visées à l'art. 14, al. 1, let. a^{bis}.
- L'art 17, al. 4ter, reprend le délai d'une semaine prévu dans l'actuel art. 23 pour transférer les données sanitaires collectées lors du recrutement (art. 26, al. 2) vers le MEDISA et les effacer du SIPA.
- Les autres dispositions du SIR sont déjà couvertes par celles du SIPA.

Pour l'intégration de la banque de données SPP, les dispositions du SIPA seront adaptées comme suit.

- L'art. 13, let. o, correspond à l'actuel art. 37, let. a.
- L'art. 14, al. 4 correspond à l'actuel art. 38.
- L'art. 15, al. 4, correspond à l'actuel art. 39.
- L'art. 16, al. 1ter, correspond à l'actuel art. 40, al. 1. Les données à communiquer selon l'actuel art. 40, al. 2, seront régies par l'art. 14, al. 1, et pourront continuer à être collectées selon l'art. 15, al. 1, let. d, auprès du SPP puis communiquées aux autorités et commandements militaires en vertu l'art. 16, al. 1, let. a et b.
- L'art. 17, al. 4^{quater}, correspond à l'actuel art. 41, où l'ajout de la locution *au plus* indique que les données ne doivent pas être conservées obligatoirement pendant cinq ans.

En outre, le complément prévu à la fin de la phrase introductive de l'art. 16, al. 1, tiendra compte du principe de la proportionnalité dans le traitement des données

(art. 4, al. 2, aLPD et art. 6, al. 2, nLPD). En effet, avec l'intégration du SIR et de la banque de données SPP et donc de données sanitaires dans le SIPA, il faut limiter l'accès en ligne aux données nécessaires à l'accomplissement des tâches légales et contractuelles et éviter que n'importe qui puisse consulter l'ensemble des données (telles les données sanitaires collectées lors du recrutement visées à l'art. 14, al. 1, let. a^{bis}).

La modification des art. 13, let. f, et 16, al. 1, let. h, a pour but non seulement d'empêcher les abus dans le cadre du traitement des allocations pour perte de gain (APG) au moyen des données du SIPA, mais aussi de permettre l'exécution du régime des APG et de rendre les données requises accessibles à la centrale de compensation. Les formulaires d'annonce pour les prestations de ce régime étant encore établis sous forme papier, il est prévu de mettre en place un système de numérisation pour l'enregistrement et le traitement des cas. Les processus pourront ainsi être automatisés, le paiement des allocations accéléré et les charges relatives au traitement des cas allégées. Mais un tel traitement numérisé n'est possible que si les données nécessaires du SIPA peuvent être disponibles à cette fin.

Les modifications apportées aux art. 13, let. n, et 14, al. 1, let. n, permettront de traiter les données du SIPA en rapport avec l'examen et le contrôle des indemnités de formation. Les données du SIPA pourront être utilisées, selon l'art. 13, let. p, pour donner des réponses anonymisées aux questions sur les chiffres du DDPS. De plus, il est prévu de verser dans le SIPA les données sur les instructions suivies et les autorisations obtenues pour l'utilisation de systèmes militaires (cf. art. 14, al. 1, let. c^{bis}) afin d'assurer notamment une répartition, une planification et une administration optimales des effectifs du personnel de l'armée. La modification apportée à l'art. 17, al. 5, et l'ajout de la précision *au plus* indiquent que la destruction des autres données du SIPA que celles visées aux alinéas précédents de l'art. 17 est aussi possible avant l'échéance de cinq ans (p. ex. destruction par classe d'âge) et qu'un délai de conservation de cinq ans n'est pas obligatoire.

La modification apportée à l'art. 14, al. 2, sont purement rédactionnelles. Comme aux al. 3 et 4, *SIPA* est remplacé par *il*.

La modification de l'art. 15, al. 1, phrase introductive, ne concerne que le texte allemand. Les art. 15, al. 2, let. a, et 17, al. 1, let. e, renvoient à la LPPCi. En outre, le sigle *LRens* est introduit dans l'art. 16, al. 1, let. i, car il est repris dans le reste de l'acte aux art. 147, al. 2, let. c, et 167*k*, al. 2, let. g.

Art. 18 à 23 (système d'information SIR)

L'intégration du SIR dans le SIPA et le traitement de ses données dans celui-ci (cf. art. 14, al. 1, let. a^{bis}), permet d'abroger les dispositions relatives au SIR.

Art. 24, 27, phrase introductive, 28, al. 1, phrase introductive et let. c, et al. 3, phrase introductive (MEDISA)

Comme pour les autres systèmes d'information du Groupement Défense réglementés par la LSIA, seul le Groupement Défense (au sens d'une unité administrative supérieure selon l'annexe 1 de l'ordonnance du 25 novembre 1998 sur l'organisation du

gouvernement et de l'administration, OLOGA[22]) est mentionné comme exploitant du MEDISA (art. 24 et phrases introductives des art. 27 et 28, al. 1 et 3). L'unité administrative subordonnée, maître du fichier et organe fédéral responsable de sa protection, doit être précisée dans des dispositions d'exécution à l'échelon réglementaire (art. 2*a* et annexe 1 OSIAr).

La modification apportée à l'art. 28, al. 1, let. c, est d'ordre rédactionnel (utilisation de l'abréviation SPP introduite dans l'art. 14, al. 4).

Art. 30 et 33, phrase introductive (SIPAT)

Comme pour les autres systèmes d'information du Groupement Défense réglementés par la LSIA, seul le Groupement Défense (au sens d'une unité administrative supérieure selon l'annexe 1 OLOGA) est mentionné comme exploitant du SIPAT. L'unité administrative subordonnée, maître du fichier et organe fédéral responsable de sa protection, doit être précisée dans des dispositions d'exécution à l'échelon réglementaire (art. 2*a* et annexe 1 OSIAr).

Art. 36 à 41 (banque de données SPP)

L'intégration de la banque de données SPP et le traitement de son contenu dans le SIPA (art. 14, al. 4) permettent d'abroger les dispositions relatives à la banque données SPP.

Art. 42, 45, phrase introductive, 46, al. 1, phrase introductive, et 2, et 47, al. 1 et 3 (MEDIS FA)

Comme pour les autres systèmes d'information du Groupement Défense réglementés par la LSIA, seul le Groupement Défense (au sens d'une unité administrative supérieure selon l'annexe 1 OLOGA) est mentionné comme exploitant du MEDIS FA. L'unité administrative subordonnée, maître du fichier et organe fédéral responsable de sa protection, doit être précisée dans des dispositions d'exécution à l'échelon réglementaire (art. 2*a* et annexe 1 OSIAr).

L'art. 47, al. 1, sera abrogé puisque, selon l'art. 8 LSIA et la LAr, les Archives fédérales archivent les documents qui ne sont plus systématiquement utilisés. L'art. 2, al. 3, autorise encore le traitement non électronique des données du MEDIS FA. Le nouvel art. 47, al. 3, garantit aussi que les données des personnes traitées ou prises en charge par l'Institut de médecine aéronautique après la fin de la durée de conservation visée à l'art. 47, al. 2, pourront être consultées et seront conservées dix ans après le traitement ou la prise en charge (même au-delà de l'âge de 80 ans).

22 RS **172.010.1**

Titre précédant l'art. 48, art. 48, 50, 51, phrase introductive, 52, al. 1, et 53, al. 2 (Système d'information sur le personnel d'intervention du commandement des Forces spéciales [SIPI CFS])

Il est prévu de traiter dans le système non seulement les données des membres du détachement de reconnaissance de l'armée subordonné au commandement des Forces spéciales (CFS) et des personnes du CFS qui doivent appuyer les engagements (conduite, logistique, aide au commandement), mais aussi celles des candidats à évaluer et des membres du détachement spécial de la police militaire (qui fait aussi partie du CFS). Le nom donné au système d'information, son abréviation et certaines dispositions citant les cercles de personnes concernées (art. 49, let. a et b, et 53, al. 2) seront donc modifiés de manière à inclure toutes les personnes susmentionnées. La modification de l'art. 49, let. c, est de nature purement rédactionnelle et ne concerne que le texte français. L'art. 50 en langue allemande est modifié afin de correspondre aux textes en langues française et italienne, dans lesquels *au cours d'un engagement* s'applique tant au risque de défaillance qu'à l'endurance.

Titre précédant l'art. 54, art. 54 à 58 (SISOC)

Comme pour les autres systèmes d'information du Groupement Défense réglementés par la LSIA, seul le Groupement Défense (au sens d'une unité administrative supérieure selon l'annexe 1 OLOGA) est mentionné comme exploitant du SISOC. L'unité administrative subordonnée, maître du fichier et organe fédéral responsable de sa protection, doit être précisée dans des dispositions d'exécution à l'échelon réglementaire (art. 2*a* et annexe 1 OSIAr).

Le nouveau nom du système d'information (*Système d'information pour l'assistance sociale* remplaçant *Système d'information du domaine social*) doit être repris dans l'art. 54 tout comme dans le titre qui précède cet article.

Il est nécessaire d'élargir cercle de personnes visées à l'art. 55 aux membres de la protection civile, au personnel du Service de la Croix-Rouge, aux personnes engagées dans le service de promotion de la paix, aux membres de la justice militaire ainsi qu'aux parents des personnes citées à l'art. 55, car ces personnes aussi bénéficient du soutien du Service social de l'armée, conformément à l'ordonnance du 30 novembre 2018 sur le Fonds social pour la défense et la protection de la population[23].

Pour fonder ses décisions de soutien financier, le Service social de l'armée a besoin, en plus des données visées à l'actuel art. 56, de celles relatives à la gestion des cas, des notes sur les entretiens et des documents personnels nécessaires à l'évaluation de prestations de conseil et de prise en charge (notamment soutien financier). Une modification en conséquence de l'art. 56 s'impose. Le SIPA sera aussi mentionné dans l'art. 57 comme source de données. La collecte de données à partir du SIPA dans le but de planifier des entretiens se limite à l'identité et au numéro AVS. En outre, dans l'optique du versement de montants à partir du Fonds social pour la défense et la protection de la population, il faut pouvoir vérifier dans le SIPA si le bénéficiaire y a droit (encore astreint au service militaire) ou non (déjà libéré des obligations militaires).

23 RS **611.021**

Les militaires incorporés à l'état-major spécialisé du Service social de l'armée, qui contribuent également à atteindre le but de l'art. 55 LSIA et à accomplir les tâches de ce service et qui, pour ce faire, ont besoin d'accéder aux données du SISOC, doivent aussi être mentionnés explicitement à l'art. 58, let. b, car ils ne font pas partie du personnel du service, mais des éléments de milice de l'armée. Par ailleurs, il est prévu que le service spécialisé Diversité dans l'Armée suisse et l'Aumônerie de l'armée introduits à l'art. 58, let. c et d, qui proposent aussi un appui social aux militaires, pourront accéder aux seules données du SISOC concernant leurs bénéficiaires.

Art. 63, al. 2, et 65, al. 2 (système d'information SIP DEF)

Le Système d'information sur le personnel de la Confédération (BV PLUS) a été remplacé par le Système d'information pour la gestion des données du personnel (IGDP), régi par les art. 30 à 38 de l'ordonnance du 22 novembre 2017 concernant la protection de données personnelles du personnel de la Confédération (OPDC)[24]. De ce fait, dans l'art. 63, al. 2, l'IGDP remplace le BV PLUS comme source de données. Dans l'art. 65, al. 2, la notion d'effacement est remplacée par celle de destruction, conformément au commentaire relatif à l'art. 8.

Art. 72, 73, phrase introductive, 75, phrase introductive (SIC SSC)

Comme pour les autres systèmes d'information du Groupement Défense réglementés par la LSIA, seul le Groupement Défense (au sens d'une unité administrative supérieure selon l'annexe 1 OLOGA) est mentionné comme exploitant du SIC SSC. L'unité administrative subordonnée, maître du fichier et organe fédéral responsable de sa protection, doit être précisée dans des dispositions d'exécution à l'échelon réglementaire (art. 2*a* et annexe 1 OSIAr). Après adaptation, l'art. 72 ne mentionnera plus le SSC. Celui-ci doit donc être explicité dans la phrase introductive de l'art. 73. Les autres modifications des art. 73 et 75 ne concernent que le texte allemand.

Art. 85, al. 2, 86, let. a, a^{bis} et h, 87, let. a, et 88 (système d'information MIL Office)

Afin d'exécuter le régime des APG, la modification des art. 85, al. 2, et 88 (nouvelle let. d) crée une base légale permettant de communiquer à la Centrale de compensation les données du MIL Office sur la comptabilisation des soldes et des frais ainsi que sur les absences et les services commandés en même temps que d'autres données (identité, adresse, coordonnées, incorporation, grade, fonction et instruction).

La modification de l'art. 87, let. a, crée une base légale permettant à la personne concernée d'utiliser un portail électronique pour transmettre volontairement des données personnelles (telles des demandes de congé assorties d'annexes) au commandement militaire compétent. Cette possibilité raccourcit et simplifie les processus en lien avec l'administration et l'organisation des écoles et des cours (conformément au but du MIL Office visé à l'art. 85 LSIA).

Par souci de clarté et d'exhaustivité, la modification de l'art. 86 (nouvelle teneur de la let. a et ajout de la let. h; l'actuelle let. a devient la let. a^{bis}) intègre dans la loi les

24 RS **172.220.111.4**

données personnelles (non sensibles) pouvant être traitées dans le MIL Office qui figurent déjà dans les dispositions d'exécution (cf. annexe 16, ch. 1, 5 et 12, OSIAr).

Les modifications apportées à l'art. 88, let. a à c, sont d'ordre linguistique et rédactionnel. Elles ne concernent que le texte français.

Art. 94 (système d'information SIGC)

Par souci d'uniformité avec de nombreuses autres dispositions de la LSIA réglant la communication de données propres à un système d'information, l'art. 94 précise que la communication jusqu'ici réservée à des *personnes* sera accordée à des *services et personnes*. Par souci d'harmonisation terminologique avec les art. 93 et 95, *collaborateurs concernés* est remplacé par *personne concernée* et *responsables hiérarchiques* par *supérieur*s.

Art. 103, phrase introductive et let. a et c (SIC FT)

Le SIC FT ne sera plus engagé pour conduire des actions, mais pour suivre la situation, et servir au commandement des Opérations et à la Base d'aide au commandement dans l'exécution de leurs tâches. D'où la nécessité d'apporter ces précisions à l'art. 103, let. a et c. La modification apportée à la phrase introductive est purement linguistique.

Art. 109, let. a, 110, let. a (système d'information et de conduite des Forces aériennes [SIC FA])

Le SIC FA ne sera plus engagé pour conduire des actions, mais pour suivre la situation. D'où la nécessité d'apporter cette précision à l'art. 109, let. a.

Les données sur la confession n'étant pas traitées dans le SIC FA, cette précision peut par ailleurs être biffée à l'art. 110, let. a.

Art. 119 (Système d'information et de conduite du soldat [SICS])

Effacement est remplacé par *destruction* (cf. commentaire relatif à l'art. 8).

Art. 121, 123, phrase introductive et let. c, 124, al. 2, let. c, et 125, al. 2 (Systèmes d'information pour les simulateurs [SISIM])

Il faut que les données des personnes s'entraînant régulièrement sur simulateurs soient (si possible) disponibles et conservées pendant tout le temps passé à l'armée, période qui dépasse généralement cinq ans. Les résultats obtenus lors de l'instruction et les compétences acquises sont ainsi mieux documentés, contribuant de ce fait à un meilleur accomplissement des tâches. L'art. 125, al. 2, est modifié de sorte que la durée de conservation des données est prolongée de cinq à dix ans. Il est aussi prévu, dans les diverses dispositions (art. 121, 123, let. c, 124, al. 2, let. c, et 125, al. 2), que les données des civils ou des tiers (tels les membres d'organisation d'intervention d'urgence) s'entraînant sur simulateurs puissent être traitées et qu'elles puissent être collectées auprès de leurs supérieurs civils ou leur être communiquées.

Art. 131 (LMS DDPS)

L'expérience montre que souvent, les militaires continuent à participer à des activités hors du service ou les employés du DDPS à travailler dans l'administration fédérale une dizaine d'années après la libération des obligations militaires ou la fin de leurs rapports de travail. Ces personnes ont acquis des compétences inscrites dans le LMS DDPS, qui sont nécessaires pour les activités hors du service ou un emploi à la Confédération (p. ex. conducteurs de véhicules à moteur engagés en dehors du service dans les domaines du transport de marchandises dangereuses ou de l'arrimage de la cargaison, ou encore officiers fédéraux de tir dans le domaine des prescriptions générales de sécurité). Pour permettre un contrôle l'instruction (art. 127, let. d, LSIA) et assurer la gestion des compétences (art. 127, let. g, LSIA), il faut connaître ces informations. Il est donc prévu de conserver ces données dans le LMS DDPS dix ans après la libération des obligations militaires ou la fin des rapports de travail. Les personnes concernées ne seront ainsi pas obligées de suivre une nouvelle fois les formations ou de présenter les certificats de capacité.

Titre précédant l'art. 138, art. 138, 139, phrase introductive et let. a, c, e et f, 140, phrase introductive et let. b à d, 141, phrase introductive et let. b à e, 142, al. 1, et 143 (SI OCRNA)

L'Office de la circulation routière et de la navigation de l'armée (OCRNA) est notamment chargé de l'établissement, de l'administration et du retrait:

- des autorisations de conduire militaires pour les conducteurs de véhicules (art. 32 et 38 de l'ordonnance du 11 février 2004 sur la circulation militaire, OCM[25]), et des permis de conduire militaires pour conducteur de bateaux (art. 4 et 14 de l'ordonnance du 1er mars 2006 concernant la navigation militaire, ONM[26]);
- des permis des experts de la circulation militaires (ou des experts militaires aux examens) qui organisent les examens pour les conducteurs de véhicules et de bateaux (cf. art. 29 OCM et art. 4 ONM);
- des permis de conduire fédéraux (art. 3 et 11 de l'ordonnance du 1er mars 2006 concernant la navigation civile de l'administration fédérale[27]).

Il est prévu de traiter toutes les données personnelles nécessaires à l'accomplissement de ces tâches dans le système d'information géré par l'OCRNA. Aussi, l'appellation trop limitative de *système d'information sur les autorisations de conduire militaires* (SIAC) doit être comprise dans un sens plus général et modifiée en *système d'information sur la circulation routière et la navigation de l'armée* (abrégé SI OCRNA). Il est prévu de compléter les art. 139, let. a et c (But) et 140, let. b (Données) pour y faire figurer, si ce n'est déjà le cas, les groupes de personnes, les autorisations de conduire et les permis préalablement cités. De plus, l'IGDP (art. 30 à 38 OPDC) sera cité dans l'art. 141, let. d, comme nouvelle source de données, notamment pour ce qui concerne les données sur les permis de conduire fédéraux.

25 RS **510.710**
26 RS **510.755**
27 RS **747.201.2**

L'art. 139, let. f, sera abrogé car plus aucune donnée ne sera traitée dans le cadre fixé par cette lettre (gérer les certificats de formation conformément à l'Accord européen du 30 septembre 1957 relatif au transport international des marchandises dangereuses par route[28]).

Les registres signalés comme sources de données à l'art. 141, let. b (registre des autorisations de conduire), et comme destinataires de données à l'art. 142, al. 1, let. b (registre des mesures administratives), seront remplacés par le Système d'information sur l'admission à la circulation (SIAC) de l'Office fédéral des routes (cf. ordonnance du 30 novembre 2018 sur le système d'information relatif à la circulation[29]).

L'art. 143, al. 1, prévoit d'étendre la possibilité de conserver des données du SI OCRNA, y compris celles qui portent sur les mesures administratives (type de mesure, motif, durée et service l'ayant prononcée ou saisie), au-delà de la libération de l'obligation de servir, jusqu'à 80 ans après leur saisie. Cette mesure est nécessaire dès lors que les autorisations de conduire militaires conservent leur validité dans le cadre des activités militaires hors du service, même lorsque leurs détenteurs ont quitté l'armée (art. 33 OCM). Elle l'est aussi du fait que de nombreux experts de la circulation militaire ne sont plus forcément astreints au service militaire. C'est pourquoi l'OCRNA doit aussi pouvoir exercer ses tâches d'administration et de contrôle après la libération des obligations militaires de la personne concernée et disposer des données personnelles nécessaires à ces fins. Cela se justifie aussi par le fait que le SIP DEF est indiqué à l'art. 141, let. c, comme autre source de données permettant notamment d'accéder – autrement que par le SIPA – aux dernières données relatives aux permis des experts de la circulation militaire qui ne sont plus astreints au service militaire. À la différence de ce que prévoit l'art. 143, al. 1, l'al. 2 précise que les données du SI OCRNA portant sur les mesures administratives civiles ne seront conservées qu'aussi longtemps qu'elles le sont dans le SIAC. Concernant les examens de contrôle visés à l'al. 3, l'OCRNA a besoin de connaître uniquement la date, le résultat et la durée de validité du dernier contrôle (afin de savoir quand les prochains examens de contrôle devront être effectués). Il n'est pas nécessaire de conserver les données des examens de contrôle précédents. La modification apportée à l'art. 140, let. c et d, le précise.

D'autres modifications rédactionnelles concernant les art. 139, let. e, et 140, phrase introductive, ne concernent que l'allemand. Par souci d'uniformité avec de nombreuses autres dispositions de la LSIA, *personnes et services* est remplacé par *services et personnes* dans les art. 141, let. e, et 142, al. 1, let. a.

Art. 143c, let. l (SPHAIR-Expert)

En vue du profilage prévu à l'art. 2*b*, let. g, il est prévu d'ajouter une nouvelle let. l à l'art. 143*c*, pour permettre de traiter également l'intérêt personnel porté à l'embauche, à la formation (instruction), au perfectionnement, ainsi qu'au choix du métier et de la fonction.

28 RS **0.741.621**
29 RS **741.58**

Art. 143g à 143l (Système d'information pour l'instruction de conduite [SIIC])

Afin de créer la base légale formelle requise par l'art. 34, al. 2, let. b, nLPD pour traiter des données par profilage et profilage à risque élevé, il faudra, en plus de la nouvelle réglementation prévue à l'art. 2*b*, inscrire dans la LSIA les dispositions régissant le SIIC, qui ne figurent actuellement qu'à l'échelon réglementaire. Ces nouveaux articles de la LSIA permettront de continuer à exploiter le SIIC comme il l'a été jusqu'à maintenant sur la base des art. 62 ss et de l'annexe 29 OSIAr.

Art. 145, 147, al. 2, phrase introductive et let. c et d, 148, al. 1, phrase introductive et let. c, ch. 2bis, et d (SICSP)

La modification de l'art. 145 permet de tenir compte des différentes mentions et des différents buts visés par les évaluations et les contrôles inscrits à l'échelon législatif. En font notamment partie, les contrôles de sécurité relatifs aux personnes visés aux art. 19 à 21 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[30], aux art. 23 et 103 LAAM et à l'art. 20*a* de la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl)[31], ainsi que les évaluations du potentiel d'abus ou de dangerosité en ce qui concerne l'arme personnelle visées à l'art. 113 LAAM et les contrôles de fiabilité visés à l'art. 24 de la loi du 21 mars 2003 sur l'énergie nucléaire[32].

Pour des raisons de cohérence terminologique, l'expression *dans les limites prévues [par les dispositions correspondantes]* est remplacée, dans la phrase introductive de l'art. 147, al. 2, par *dans le cadre prévu [par les dispositions correspondantes]* (cf. art. 183, al. 2).

Dans l'art. 147, al. 2, let. c, le *système d'information* INDEX SRC remplace le *système de traitement des données relatives à la protection de* l'État, qui n'existe plus.

Les bases légales permettant d'accéder en ligne aux données des diverses banques de données de l'Office central des armes visées à l'art. 32*a*, al. 1, de la loi du 20 juin 1997 sur les armes (LArm)[33] (plate-forme d'information sur les armes ARMADA) existent déjà. Elles se trouvent dans l'art. 32*c*, al. 8, LArm en relation avec l'art. 61, al. 2, let. e, et dans l'art. 61, al. 6, en relation avec l'annexe 3 de l'ordonnance du 2 juillet 2008 sur les armes (OArm)[34]. La possibilité d'un accès en ligne sera aussi intégrée dans l'art. 147, al. 2, let. d, LSIA. Les diverses bases de données accessibles de l'Office central des armes n'y seront pas énumérées car la phrase introductive lie l'accès en ligne au cadre prévu par les dispositions correspondantes, de sorte qu'une modification des droits d'accès à l'échelon de l'OArm s'appliquerait automatiquement au SICSP, sans avoir à modifier la LSIA.

La Société nationale du réseau de transport sera par ailleurs mentionnée à l'art. 148, al. 1, let. c, ch. 2bis, car l'art. 20*a* LApEl, entré en vigueur début 2018, dispose que les personnes chargées de certaines tâches au sein de cette société sont soumises à un

30 RS **120**
31 RS **734.7**
32 RS **732.1**
33 RS **514.54**
34 RS **514.541**

contrôle de sécurité relatif aux personnes. L'accès en ligne au SICSP de cette société vise à faciliter la communication des résultats des contrôles prévue à l'art. 20*a*, al. 3, LApEl. La société aura un accès direct aux seules données du SICSP nécessaires à l'accomplissement de ses tâches, conformément au principe de la proportionnalité découlant de l'art. 1, al. 3, LSIA, en relation avec l'art. 4, al. 2, aLPD (art. 6, al. 2, nLPD).

La précision apportée à l'art. 148, al. 1, let. d, garantit que seuls les services fédéraux qui ont besoin des données du SICSP – et donc des données concernant les contrôles de sécurité relatifs aux personnes – dans le cadre de leurs tâches de sécurité y auront un accès en ligne. De plus, l'accès sera limité aux données qui ne sont pas préjudiciables à la personne concernée.

Les dispositions relatives au SICSP ne seront modifiées que jusqu'à l'éventuelle entrée en vigueur de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[35], dont les dispositions abrogent, entre autres, celles de la LSIA sur le Système d'information sur le contrôle de la sécurité industrielle (SICSI, art. 150 à 155) et sur le SICSP (art. 144 à 149). En effet, la LSI fixe une réglementation sur les systèmes d'information et la protection des données. Il faut donc prévoir la disposition de coordination requise dans la LSIA (cf. ch. 5.2); celle-ci répétera, pour des raisons de clarté, la règle contenue dans la LSI et abrogera les art. 144 à 155.

Titre précédant l'art. 167a, art. 167a, 167b, let. a et b, 167d, 167e, al. 1, 2, let. b (ne concerne que le texte allemand) et c, et 167f (système d'information JORASYS)

Le Système de journal et de rapport de la Sécurité militaire devient le Système de journal et de rapport de la *Police militaire*, adaptant ainsi son nom complet aux structures créées dans le cadre du DEVA, tout en conservant son nom abrégé JORASYS.

Le nouvel art. 167*d*, let. e, reprend les dispositions de l'actuel art. 167*d*, al. 2, LSIA où la nouvelle abréviation SI OCRNA remplace le SIAC (cf. commentaires relatifs aux art. 138 ss). De plus, il doit ressortir clairement de la phrase introductive de l'art. 167*d*, let. e, que les données issues des systèmes d'information, visés notamment aux ch. 2 à 7 et 9, peuvent être collectées par une interrogation manuelle des systèmes (généralement au moyen d'une interface réseau fournie par les opérateurs du système ou d'un logiciel spécifique) ou par une transmission automatique des données au moyen d'une interface (à prévoir). Ainsi, les données personnelles nécessaires à l'accomplissement de tâches quotidiennes (p. ex. établissement de rapports pour les autorités judiciaires, préparation d'interventions, contrôles de la police militaire de la circulation) et qui doivent toujours être actuelles pourront être collectées plus rapidement et plus simplement. Dans le détail, les systèmes d'information ajoutés à l'art. 167*d*, let. e, donnent accès aux données suivantes.

35 FF **2020** 9665

(Ajouté) Système d'information	permet d'accéder à
RIPOL (art. 167*d*, let. e, ch. 2)	Données sur les infractions non élucidées (p. ex. les objets déclarés volés) (art. 3, let. h, 6, al. 1, let. o, 7, al. 1, et annexe 1, ch. 2, de l'ordonnance RIPOL du 26 octobre 2016[36])
SIAC (art. 167*d*, let. e, ch. 3)	Données sur les véhicules et leur admission à la circulation, sur les conducteurs et leur autorisation de conduire, sur les détenteurs et les assureurs (art. 89*e*, let. a, de la loi fédérale du 19 décembre 1958 sur la circulation routière[37])
Banques de données visées à l'art. 32*a* LArm (art. 167*d*, let. e, ch. 4)	Accès en ligne aux banques de données de l'Office central des armes visées à l'art. 32*a* LArm pour voir si une personne a l'interdiction d'acquérir une arme ou si une arme lui a été retirée (art. 32*a* à 32*c* LArm)
Consultation en ligne des registres d'armes cantonaux (art. 167*d*, let. e, ch. 5)	Accès en ligne aux registres cantonaux sur les détenteurs d'une arme à feu (données sur l'acquisition et la possession d'armes à feu) (art. 32*a*, al. 2 et 3, et 32*b*, al. 6, LArm)
SIPA (art. 167*d*, let. e, ch. 6)	Données militaires comme l'incorporation, le grade, la fonction et les services accomplis dans l'armée (art. 167*c*, al. 1, let. d)
SIP DEF (art. 167*d*, let. e, ch. 7)	Données comme la fonction, l'instruction, l'engagement dans l'armée, le statut militaire, la carrière professionnelle, les connaissances linguistiques (art. 62, let. b à e et g, LSIA)
SI IDD (art. 167*d*, let. e, ch. 9)	Données comme l'incorporation, le grade, la fonction, l'instruction, la qualification et l'équipement dans l'armée ou la protection civile (art. 176, let. a, LSIA)

Par souci de simplification et de clarté, la périphrase *personnes chargées d'évaluer la situation militaire sur le plan de la sécurité et d'assurer l'autoprotection de l'armée* (art. 100, al. 1, let. a et e, LAAM, et art. 11 OSM) est remplacée par *personnel du SPPA* dans l'art. 167*e*, al. 1, let. c. La modification de l'art. 167*e*, al. 2, let. b, ne concerne que le texte allemand. Il est prévu de reformuler l'art. 167*e*, al. 2, let. c, afin que le destinataire des données ne soit plus un organe spécifique responsable de la sécurité des informations et des objets (p. ex. le domaine Sécurité des informations et des objets, qui dépend administrativement du Secrétariat général du DDPS [SG-DDPS]),

36 RS **361.0**
37 RS **741.01**

mais plus généralement les *services chargés de la sécurité des informations et des objets* (en particulier au sein du Groupement Défense). De plus, comme une durée uniforme de conservation des données de dix ans à compter de la fin des activités de la Police militaire relatives à un cas donné est jugée nécessaire et suffisante, l'art. 167*f* est modifié en conséquence.

Les modifications apportées aux art. 167*b*, let. a et b, et 167*e*, al. 1, phrase introductive et let a, sont de nature purement formelle et ne concernent que le texte français.

Art. 167g à 167l (SIPPA)

Les nouveaux art. 167*g* à 167*l* visent à créer une base légale pour le SIPPA permettant au SPPA d'accomplir ses tâches, de tenir son journal et de conduire ses engagements. Ce service doit notamment apprécier la situation en matière de sécurité et prendre des mesures préventives pour assurer la sécurité de l'armée contre l'espionnage, le sabotage et d'autres activités illicites (art. 100, al. 1, let. a et e, LAAM, et 11 OSM). Pour ce faire, il est nécessaire de saisir les données concernant les personnes liées à une menace potentielle de l'armée (art. 167*i*, phrase introductive) et les détails sur cette menace potentielle (art. 167*i*, let. m).

Les données personnelles traitées dans le SIPA sont parfois des données sensibles. Il s'agit notamment:

– de données sur l'appartenance ethnique et la confession (art. 167*i*, let. c; pour évaluer d'éventuels motifs dans le domaine de l'extrémisme violent, du terrorisme et de l'espionnage contre l'armée),
– de données sur l'orientation politique et idéologique (art. 167*i*, let. e; pour évaluer d'éventuels motifs dans le domaine de l'extrémisme violent, du terrorisme et de l'espionnage contre l'armée),
– de données médicales et biométriques (art. 167*i*, let. h; pour identifier clairement les personnes ou détecter des maladies psychiques qui pourraient menacer la sécurité de l'armée),
– d'autres données personnelles, y compris sensibles (art. 167*i*, let. n; voir aussi art. 100, al. 3, LAAM).

Pour pouvoir traiter ces données sensibles dans le SIPPA, l'art. 17, al. 2, aLPD (art. 34, al. 2, nLPD) exige l'établissement d'une base légale dans une loi au sens formel.

Les personnes de référence visées à l'art. 167*i*, let. j, ne constituent pas une menace pour l'armée mais ont un rapport direct avec une personne pouvant en constituer une. Elles peuvent permettre d'identifier, de trouver ou d'approcher une personne qui représente une menace potentielle et ainsi de réduire ou de neutraliser la menace.

Aux sources d'information indiquées à l'art. 167*j*, let. a à f, s'ajoutent – par un accès en ligne permanent – les systèmes d'information visés à l'art. 167*j*, let. g, afin que le SPPA dispose rapidement et aisément des données qui lui sont nécessaires. L'art. 167*j* étant formulé de manière très générale, les données qu'il permet de collecter englobent toutes les données qui peuvent être traitées dans le SIPPA aux fins prévues à l'art. 167*h*, peu importe la manière dont le service qui les met à disposition se les est

procurées. L'acquisition de données auprès des services de renseignement en vertu de l'art. 167*j*, al. 1, let. c, ne tient aucunement compte des mesures et des méthodes employées par lesdits services pour les obtenir, ni du fait que ces mesures et méthodes aient été soumises à autorisation ou non.

Titre précédant l'art. 168, art. 168, 169, phrase introductive et let. d et e, 170, phrase introductive et let. a et a^{bis}, 171, phrase introductive et let. i, 172 et 173 (SCHAMIS)

La modification du titre précédant l'art. 168 est purement formelle. Elle ne concerne que les textes français et italien.

Le SG-DDPS travaille avec l'application du Système d'information du Centre de dommages du DDPS qui a succédé au Système d'information du service des sinistres du DDPS (SI SIN), utilisé depuis fin 2003. La désignation technique de la nouvelle application est SCHAMIS. Elle vient de l'allemand *SCHAdenManagement- und InformationsSystem*. Le *SI SIN* sera donc remplacé par le *SCHAMIS* dans tout l'acte.

L'art. 169, let. d et e, mentionne deux nouveaux buts visés par le SCHAMIS.

– Le Centre de dommages du DDPS (CEDO DDPS) règle les accidents et les sinistres impliquant des véhicules de la Confédération, conformément à l'art. 21 de l'ordonnance du 23 février 2005 concernant les véhicules automobiles de la Confédération et leurs conducteurs[38]. Pour cette activité semblable à celle d'un assureur, l'art. 5, al. 1, let. b, de l'ordonnance du 20 novembre 1959 sur l'assurance des véhicules[39], lui confère le droit d'établir des attestations d'assurance à l'intention des services cantonaux chargés de l'immatriculation des véhicules (services des automobiles). Désormais, cette procédure pourra être traitée dans le SCHAMIS et ainsi s'ajouter aux buts indiqués (art. 169, let. d).
– Le règlement des sinistres concerne aussi les véhicules à moteur des députés, conformément à l'art. 4, al. 2, de l'ordonnance de l'Assemblée fédérale du 18 mars 1988 relative à la loi sur les moyens alloués aux parlementaires[40]. Il s'effectue dans le SCHAMIS, il faut donc l'indiquer dans les buts (art. 169, let. e).

La base légale requise par la législation sur la protection des données permettait déjà de traiter des données concernant des sinistres. Pour répondre aux impératifs actuels de la protection des données, il est nécessaire de préciser ces données dans l'art. 170, let. a, et de citer expressément dans la loi le traitement des données personnelles sensibles relatives aux lésés et aux auteurs du dommage – comme celles concernant la situation financière ainsi que les procédures pénales, civiles, disciplinaires et administratives. L'art. 170, let. a^{bis}, prévoit en outre le traitement de données de tiers, réduit au minimum nécessaire pour atteindre le but visé.

38 RS **514.31**
39 RS **741.31**
40 RS **171.211**

Lors du règlement des sinistres, les assurances privées échangent entre elles les données les plus diverses, par exemple pour clarifier la question de la responsabilité au regard des dossiers ou pour établir le montant des créances récursoires. Le CEDO DDPS, agissant en qualité d'assureur, était déjà autorisé implicitement par la loi à collecter des données auprès des assurances, dans la mesure où il leur demandait des données sur les personnes concernées ou leurs personnes de référence. Les assurances seront désormais mentionnées explicitement à l'art. 171, let. i.

Le règlement des sinistres exige, dans bien des cas, que certaines données soient communiquées à des tiers. Ceux-ci n'agissent pas toujours formellement sur mandat du SG-DDPS ou du CEDO DDPS, d'où la suppression de cette restriction inutile (art. 172, al. 2).

Titre précédant l'art. 174, art. 174, 175, phrase introductive, 176, phrase introductive et let. c, 177, phrase introductive, 178 et 179 (Système d'information concernant l'interface des données de la défense [SI IDD])

La désignation et l'abréviation du système d'information seront adaptées selon sa nouvelle structure et le but principal qu'il vise en tant qu'interface de données. Le *Système d'information stratégique de la logistique* (SISLOG) devient donc le *Système d'information concernant l'interface des données de la défense* (SI IDD). Le SI IDD n'est pas seulement utilisé par la Base logistique de l'armée, mais par d'autres services du Groupement Défense.

Les données personnelles sensibles font aussi partie des données visées à l'art. 176, let. c, qui peuvent être échangées entre les systèmes d'information de l'armée par l'intermédiaire du SI IDD, conformément à l'art. 175, let. c (voir la définition de *données* à l'art. 1, al. 1).

L'art. 178 précisera les services et personnes auxquelles les données personnelles traitées par le SI IDD peuvent être communiquées. Ainsi, ces données susceptibles d'être échangées avec d'autres systèmes d'information de l'armée devront être communiquées uniquement aux services ou personnes compétents. Il est prévu de communiquer seulement les données personnelles visées à l'art. 176, let. a et b, aux commandements militaires et aux unités administratives de la Confédération et des cantons.

Art. 179b, let. d, 179c, al. 4, 179d, let. e, et 179e, al. 2, let. e (PSN)

L'art. 179*c*, al. 4, ne renverra plus aux deux articles de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[41], abrogés le 1er janvier 2018, mais d'une manière générale à la LPers et à ses dispositions d'exécution (cf. art. 8 ss, dossier de candidature, et 19 ss OPDC, dossier personnel).

Le BV PLUS étant remplacé par l'IGPD, que règlent les art. 30 à 38 OPDC, il en va de même pour son appellation dans les art. 179*d*, let. e, et 179*e*, al. 2, let. e.

La modification de l'art. 179*b*, let. d, ne concerne que le texte allemand.

41 RS **172.220.1**

Titre précédant l'art. 179g, art. 179g, 179h, phrase introductive, 179i, phrase introductive, 179j, phrase introductive, 179k, al. 1, phrase introductive, et al. 2, et 179l, al. 1 (SaD)

En raison de l'adaptation au futur système, le nom et l'abréviation de l'AFS sont changés en Système d'information sur le tir hors du service (SaD).

Art. 179m à 179r (MDM)

Les nouveaux art. 179*m* à 179*r* visent à donner une base légale au MDM qui sera exploité par le SG-DDPS. Le MDM permettra d'administrer et d'établir, pour l'ensemble du DDPS, des données claires et homogènes concernant les partenaires actuels ou potentiels (art. 179*o*) impliqués dans les processus d'affaires du DDPS relatifs aux domaines finances, acquisitions, logistique, immobilier et personnel (art. 179*n*) – ces données sont appelées *données de base* ou *master data*. Parmi ces données, on trouve le *numéro d'assurance sociale* (art. 179*o*, let. k), qui peut être un numéro AVS ou le numéro d'une assurance sociale étrangère à laquelle est affilié un partenaire. Les partenaires peuvent être des entreprises ou des particuliers. Par *partenaires potentiels*, on entend des personnes (physiques ou morales) qui, suite à une prise de contact ou la manifestation d'un intérêt, seront *très probablement* impliquées dans un des processus d'affaires visés à l'art. 179*n*. Si la probabilité élevée n'est pas donnée, les données des personnes ne seront pas collectées dans le MDM. Les données de base prédéfinies seront gérées de façon centralisée, uniquement dans le MDM, afin d'obtenir une source de données actuelle d'excellente qualité. En raison des exigences accrues de sécurité et de protection de l'information au sein du DDPS, il est prévu que l'accès au MDM se fera par un système d'information propre au DDPS et non par celui que la Confédération exploite en dehors du DDPS et qui dépend du Département fédéral des finances. Les données principalement collectées à partir de ce système au profit du MDM seront toutefois transmises au moyen d'une interface spéciale (art. 179*p*, let. c). Les autres communications de données du MDM au sein du DDPS se feront par une procédure d'accès en ligne. La durée de conservation des données prévue pour les données de base logistiques, comme celles sur le matériel ou sur la structure des systèmes, en lien avec un partenaire est de 50 ans après la fin des rapports d'affaires avec le partenaire concerné (art. 179*r*, al. 1, let. b), compte tenu du cycle de vie du matériel par exemple, et pas uniquement de 10 ans comme le prévoit, pour les autres données, la loi du 7 octobre 2005 sur les finances[42] et ses dispositions d'exécution. Pour les personnes enregistrées au titre de partenaires potentiels, mais qui ne deviennent pas des partenaires, la durée de conservation des données est de deux ans à compter de la date de leur exclusion des rapports d'affaires, et ce pour assurer la traçabilité administrative et celle des décisions prises (art. 179*r*, al. 2).

Art. 181, al. 1, let. a, et 2, phrase introductive (moyens de surveillance)

L'extension du but visé à l'art. 181, al. 1, let. a, permettra d'engager des moyens pour surveiller des objets de l'armée, de l'administration militaire ou de tiers utilisés à des fins militaires – tels des biens immobiliers civils de la Base logistique de l'armée dans

42 RS **611.0**

lesquels du matériel de l'armée est entreposé –, et de collecter et traiter les données personnelles nécessaires à cet effet.

La modification de la phrase introductive de l'art. 181, al. 2, précise que l'armée ne met jamais ses moyens de surveillance avec appui aérien et leur personnel *à la disposition* des autorités qui en font la demande, mais qu'elle leur fournit seulement des prestations en engageant ces moyens et ce personnel.

Art. 186, al. 3

Il est prévu, par cette disposition, de donner au Conseil fédéral la compétence de conclure des accords internationaux permettant le traitement transfrontalier de données personnelles dont le traitement ne requiert pas une base dans une loi au sens formel conformément à l'aLPD. Cette compétence permettra aussi au Conseil fédéral de conclure des accords internationaux dans le cadre de la coopération visée au nouvel art. 6, let. b (cf. commentaire relatif à l'art. 6).

4.2 Loi sur l'armée (LAAM)

Art. 146 Systèmes d'information de l'armée

La LSIA ayant changé de titre (cf. commentaire relatif au titre de la LSIA), il faut modifier le renvoi inscrit à l'art. 146 LAAM.

Ce renvoi fera alors référence au traitement de toutes les données personnelles, même de celles qui ne sont pas sensibles (cf. commentaire relatif à l'art. 1, al. 1), car la LSIA contient des dispositions permettant le traitement de ces dernières. Pour que cette modification ne soit pas annulée par l'entrée en vigueur de la nLPD – qui prévoit une reformulation moins générale de l'art. 146 LAAM –, une disposition de coordination est prévue dans la LSIA modifiée (cf. ch. 5.1).

4.3 Loi sur la sécurité de l'information (LSI)

Art. 45, al. 3bis et 6, let. d

L'entrée en vigueur de la LSI entraînera l'abrogation des dispositions de la LSIA régissant le SICSP (art. 144 à 149). Dès lors les dispositions nécessaires en matière de systèmes d'information et de protection des données seront réglées directement dans la LSI.

La réglementation définie aux art. 2*b*, let. h, et 147, al. 2, let d, LSIA (cf. commentaires relatifs aux dispositions correspondantes) ne figure pas encore dans la LSI. Celle-ci doit donc être complétée par l'ajout de l'art. 45, al. 3bis (correspondant aux règles prévues à l'art. 2*b*, let. h, LSIA) et de l'art. 45, al. 6, let. d (correspondant aux règles prévues à l'art. 147, al. 2, let. d, LSIA).

De plus, le nouvel art. 145 LSIA précisant le but du traitement des données et cette précision ne figurant pas encore dans la LSI, il faudra l'ajouter à l'art. 45, al. 1. Aux buts figurant par ailleurs déjà dans le nouvel art. 145 LSIA viennent s'ajouter, dans

l'art. 45, al. 1, LSI, les contrôles de loyauté, que la LSI prévoit d'introduire en ajoutant ou en modifiant les dispositions de l'art. 29*a* de la loi du 26 juin 1998 sur l'asile[43], de l'art. 20*b* LPers, de l'art. 14 LAAM et de l'art. 20*a* LApEl.

5 Coordination avec autres actes

Les dispositions nécessaires pour la coordination avec la nLPD et la LSI sont prévues comme suit:

5.1 Coordination avec la nLPD

Coordination avec la loi fédérale du 25 septembre 2020 sur la protection des données[44]

1. Quel que soit l'ordre dans lequel la présente modification ou la loi fédérale du 25 septembre 2020 sur la protection des données[45] *entrent en vigueur, à l'entrée en vigueur de la deuxième de ces lois ou à leur entrée en vigueur simultanée, l'art. 1, al. 1, phrase introductive, et 3, et l'art. 11 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée*[46] *ont la teneur suivante:*

Art. 1, al. 1, phrase introductive, et 3

1 La présente loi règle le traitement de données personnelles concernant des personnes physiques et morales (données), données sensibles comprises, dans les systèmes d'information et lors de l'engagement de moyens de surveillance de l'armée et du Département fédéral de la défense, de la protection de la population et des sports (DDPS) par:

3 Dans la mesure où la présente loi ne contient pas de dispositions spécifiques, la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[47] est applicable.

Art. 11

Abrogé

2. Quel que soit l'ordre dans lequel la présente modification ou la loi fédérale du 25 septembre 2020 sur la protection des données[48] *entrent en vigueur, à l'entrée en vigueur de la deuxième de ces lois ou à leur entrée en vigueur simultanée, l'art. 146 de la loi du 3 février 1995 sur l'armée*[49] *a la teneur suivante:*

43 RS **142.31**
44 FF **2020** 7397
45 FF **2020** 7397
46 RS **510.91**
47 RS **235.1**
48 FF **2020** 7397
49 RS **510.10**

Art. 146 Systèmes d'information de l'armée

Le traitement des données personnelles dans les systèmes d'information et lors de l'engagement de moyens de surveillance de l'armée et de l'administration militaire est réglé par la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS[50].

5.2 Coordination avec la LSI

Coordination avec la loi du 18 décembre 2020 sur la sécurité de l'information[51]

Quel que soit l'ordre dans lequel la présente modification ou la loi du 18 décembre 2020 sur la sécurité de l'information[52] *entrent en vigueur, à l'entrée en vigueur de la deuxième de ces lois ou à leur entrée en vigueur simultanée, l'art. 2b, let. h, et le chap. 5, sections 1 et 2 (art. 144 à 155), de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée*[53] *ont la teneur suivante:*

Art. 2b, let. h

Les organes responsables désignés par la présente loi peuvent effectuer un profilage, y compris un profilage à risque élevé, pour analyser, évaluer, apprécier ou prédire les aspects personnels ci-après relatifs à une personne physique:

h. risque pour la sécurité, ainsi que potentiel d'abus et de dangerosité en ce qui concerne l'arme personnelle: traitement des données comme indiqué à l'art. 13, let. l;

Chap. 5, sections 1 et 2 (art. 144 à 155)

Abrogées

6 Conséquences

6.1 Conséquences pour la Confédération

Le projet n'a pas de conséquences financières, de conséquences sur l'état du personnel ou d'autres conséquences pour la Confédération. Son but est uniquement de créer les bases légales requises en matière de protection des données pour que les données personnelles nécessaires à l'accomplissement des tâches publiques puissent effectivement être traitées. Les travaux informatiques nécessaires se déroulent, le cas échéant, dans le cadre de la modification et du développement courants des systèmes.

50 RS **510.91**
51 FF **2020** 9665
52 FF **2020** 9665
53 RS **510.91**

6.2 Autres conséquences

Le projet n'a pas de conséquences spécifiques pour les cantons, les communes, les centres urbains, les agglomérations et les régions de montagne, ni pour l'économie, la société et l'environnement.

7 Aspects juridiques

7.1 Constitutionnalité

Concernant les systèmes d'information de l'armée déjà réglés par la LSIA, la compétence de légiférer de la Confédération repose sur l'art. 60, al. 1, Cst., qui dispose que la législation militaire ainsi que l'organisation, l'instruction et l'équipement de l'armée relèvent de sa compétence. Pour ce qui est du traitement des données personnelles des Suisses et des Suissesses de l'étranger, cette compétence se fonde sur l'art. 40, al. 2, Cst. La compétence pour les systèmes d'information non militaires du DDPS nouvellement introduits dans la LSIA doit se fonder sur l'art. 173, al. 2, Cst. faute de norme de compétence explicite à ce sujet. De fait, ces systèmes, qui ne relèvent pas de l'armée (et les données personnelles qui y sont traitées), servent à assurer des tâches de la Confédération définies dans d'autres actes et qui incombent au DDPS. Leur réglementation dépend en fin de compte de l'organisation des unités administratives du DDPS, laquelle relève de leur compétence ou de celle de la Confédération.

7.2 Compatibilité avec les obligations internationales de la Suisse

Le projet est compatible avec les engagements de la Suisse relevant du droit international public. Il n'induit aucun nouvel engagement envers un État ou une organisation internationale.

7.3 Forme de l'acte à adopter

Le projet propose des dispositions importantes fixant des règles de droit, au sens de l'art. 164 Cst., qui doivent être édictées sous la forme d'une loi. Et le traitement de données personnelles sensibles au sens de l'art. 17, al. 2, aLPD (art. 34, al. 2, let. a, nLPD) prévu dans les dispositions nécessite une base légale inscrite dans une loi au sens formel.

7.4 Frein aux dépenses

Le projet ne contient pas de dispositions relatives aux subventions et ne prévoit ni crédits d'engagement ni plafonds de dépenses. Il n'est donc pas soumis au frein aux dépenses (art. 159, al. 3, let. b, Cst.).

7.5 Conformité aux principes de subsidiarité et d'équivalence fiscale

Le projet n'a aucun effet sur les principes de subsidiarité et de l'équivalence fiscale.

7.6 Conformité à la loi sur les subventions

Le projet ne prévoit pas d'aides financières et d'indemnités au sens de la loi du 5 octobre 1990 sur les subventions[54].

7.7 Délégation de compétences législatives

Une loi fédérale peut prévoir une délégation de la compétence d'édicter des règles de droit, à moins que la Constitution ne l'exclue (art. 164, al. 2, Cst.). Le projet prévoit, à l'art. 186, al. 3, LSIA, d'autoriser le Conseil fédéral à conclure des accords internationaux sur le traitement transfrontalier de données personnelles non sensibles. L'actuel art. 186, al. 1, LSIA, lui donne par ailleurs déjà la compétence d'arrêter les dispositions d'exécution nécessaires pour les systèmes d'information qui sont ajoutés à la loi.

7.8 Protection des données

Le projet concerne notamment le traitement de données personnelles sensibles. En vertu de l'art. 17, al. 2, aLPD (art. 34, al. 2, let. a, nLPD), les organes de la Confédération ne peuvent en principe traiter ce type de données que si une loi au sens formel le prévoit. Afin d'assurer le traitement et l'échange de données personnelles nécessaire à l'accomplissement de tâches, les modifications prévues dans le projet sont nécessaires du point de vue de la protection des données.

54 RS **616.1**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Projet

Loi fédérale sur les systèmes d'information de l'armée (LSIA)

Modification du ...

L'Assemblée fédérale de la Confédération suisse,
vu le message du Conseil fédéral du 24 novembre 2021[1],
arrête:

I

La loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[2] est modifiée comme suit:

Titre

Loi fédérale sur les systèmes d'information de l'armée et du DDPS (LSIA)

Préambule

vu les art. 40, al. 2, 60, al. 1, et 173, al. 2, de la Constitution[3],

Remplacement d'une expression

Dans tout l'acte «numéro d'assuré AVS» *est remplacé par* «numéro AVS».

Art. 1, al. 1, phrase introductive et let. b à d, al. 2 et 3

[1] La présente loi règle le traitement de données personnelles concernant des personnes physiques et morales (données), données sensibles comprises, dans les systèmes d'information et lors de l'engagement de moyens de surveillance de l'armée et du Département fédéral de la défense, de la protection de la population et des sports (DDPS) par:

b. les commandants et les organes de commandement de l'armée (commandements militaires) et les commandants de la protection civile;

1 FF **2021** 3046
2 RS **510.91**
3 RS **101**

c. d'autres militaires et membres de la protection civile;

d. les tiers accomplissant des tâches liées à l'armée ou à la protection civile ou pour le DDPS.

2 Elle ne s'applique pas au traitement des données par les services de renseignement.

3 Dans la mesure où la présente loi ne contient pas de dispositions spécifiques, la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[4] est applicable.

Art. 2, al. 1, phrase introductive et let. a

1 Lors de l'exploitation de systèmes d'information ou de l'engagement de moyens de surveillance de l'armée et du DDPS, les services et personnes visés à l'art. 1, al. 1, peuvent, pour accomplir leurs tâches légales ou contractuelles:

a. *abrogée*

Art. 2b Profilage

Les organes responsables désignés par la présente loi peuvent effectuer un profilage, y compris un profilage à risque élevé, pour analyser, évaluer, apprécier ou prédire les aspects personnels ci-après relatifs à une personne physique:

a. aptitude et capacité à accomplir du service militaire et du service de protection civile, y compris les conditions déterminantes correspondantes: traitement des données comme indiqué à l'art. 13, let. b à d;

b. aptitude à exercer des fonctions, à effectuer des activités et à réaliser des travaux, y compris les conditions déterminantes correspondantes: traitement des données comme indiqué aux art. 13, let. b à d, et 143*b*, let. d et e;

c. profil de prestations et performances, notamment dans les domaines de la santé, de l'aptitude physique, de l'intelligence, de la personnalité, du psychisme, du comportement social et de l'attitude au volant: traitement des données comme indiqué aux art 13, let. b à d, et 143*b*, let. d et e;

d. connaissances, compétences, capacités et prestations fournies: traitement des données comme indiqué aux art. 13, let. b à d, 127, let. d et e, 143*b*, let. d. et e, et 143*h*;

e. comportement d'apprentissage et progression: traitement des données comme indiqué à l'art. 127, let. a à c;

f. potentiel de cadre et possibilités de développement: traitement des données comme indiqué à l'art. 13, let. b à d et m;

g. intérêt personnel porté au service militaire et au service de protection civile, à l'embauche, à la formation (instruction) et au perfectionnement: traitement des données comme indiqué aux art. 13, let. b à d et m, 127, let. b, et 143*b*, let. a, d et e;

4 RS **235.1**

h. risque pour la sécurité, ainsi que potentiel d'abus et de dangerosité en ce qui concerne l'arme personnelle: traitement des données comme indiqué aux art. 13, let. l, et 145;

i. aspects personnels supplémentaires permettant de parvenir à d'autres fins de traitement des données, si la personne concernée y consent.

Art. 3

Abrogé

Art. 4, al. 1

1 Les systèmes d'information réglés par la présente loi et ses dispositions d'exécution sont exploités en réseau conjointement par le DDPS et ses unités administratives.

Art. 6 Traitement des données dans le cadre de la coopération internationale

Les autorités compétentes et les commandements militaires peuvent, dans le cadre de la coopération avec les autorités et commandements militaires d'autres pays et avec des organisations internationales, traiter des données et notamment les rendre accessibles en ligne:

a. lorsqu'une loi au sens formel ou un traité international sujet au référendum le prévoit;

b. lorsque des dispositions d'exécution édictées par le Conseil fédéral pour la présente loi ou un accord international conclu par le Conseil fédéral le prévoient et que la LPD[5] ne soumet pas le traitement de ces données à l'existence d'une base dans une loi au sens formel.

Art. 7, al. 2, 1re phrase

2 Les personnes, y compris les fournisseurs externes de prestations, chargées de la maintenance, de la gestion et de la programmation ne peuvent traiter des données que si elles sont absolument nécessaires à l'accomplissement de leurs tâches et que la sécurité des données est garantie. ...

Art. 8 Conservation, archivage et destruction des données

1 Les données sont conservées tant qu'elles sont nécessaires.

2 Les données qui ne sont plus nécessaires sont proposées aux Archives fédérales avant d'être détruites.

Art. 11

Abrogé

5 RS **235.1**

Art. 13, let. f et n à p

Le SIPA sert à l'accomplissement des tâches suivantes:

f. exécuter le régime des allocations pour perte de gain à l'armée et à la protection civile;

n. examiner et contrôler les indemnités de formation;

o. gérer les cas relevant du suivi psychologique des militaires pendant leur service;

p. répondre aux questions sur les chiffres du DDPS au moyen de données anonymisées.

Art. 14, al. 1, let. a^{bis}, c^{bis} et n, 2, phrase introductive, et 4

1 Le SIPA contient les données ci-après sur les conscrits, les personnes astreintes au service militaire, le personnel pour la promotion de la paix et les civils qui sont pris en charge par la troupe ou qui participent à un engagement de l'armée de durée déterminée:

a^{bis}. les données collectées lors des examens, tests et questionnaires du recrutement et fondant les décisions visées à la let. a concernant:

1. l'état de santé: anamnèse, électrocardiogramme, fonction pulmonaire, ouïe, vue, test d'intelligence, test de compréhension d'un texte, questionnaire en vue du dépistage de troubles psychiques et, sur une base volontaire, analyses de laboratoire et radiographies,
2. l'aptitude physique: condition physique, à savoir endurance, force, rapidité et coordination,
3. l'intelligence et la personnalité: intelligence générale, capacité à résoudre des problèmes, capacité de concentration et attention, souplesse, rigueur, assurance et sens de l'initiative,
4. le psychisme: courage, assurance, résistance au stress, stabilité émotionnelle et sociabilité,
5. les compétences sociales: adaptabilité et comportement au sein de la société, de la communauté et du groupe,
6. l'aptitude à exercer certaines fonctions: examens spécifiques permettant de révéler des aptitudes qui ne ressortent pas du profil de prestations visé aux ch. 1 à 5,
7. le potentiel de cadre: aptitude à exercer la fonction de sous-officier, sous-officier supérieur ou officier,
8. l'intérêt de la personne concernée à accomplir ses obligations militaires,
9. le risque d'utiliser abusivement l'arme personnelle;

c^{bis}. les données sur les instructions suivies et les autorisations obtenues pour l'utilisation de systèmes militaires;

n. les données pour les examens et les contrôles des demandes de versement d'indemnités de formation.

2 Il contient les données ci-après sur les personnes astreintes au service civil:

4 Il contient les données ci-après sur les personnes prises en charge par le Service psychopédagogique de l'armée (SPP):

a. l'incorporation, le grade, la fonction et l'instruction suivie dans l'armée;

b. les données psychologiques suivantes:
   1. l'état psychique,
   2. l'anamnèse biographique sur les caractéristiques psychiques,
   3. les résultats des tests psychologiques,
   4. les certificats de spécialistes civils en psychologie;

c. les données sanitaires de nature psychologique ou psychiatrique nécessaires à l'accomplissement des tâches visées à l'art. 13;

d. la correspondance échangée avec les personnes prises en charge, ainsi qu'avec les services concernés;

e. les données fournies volontairement par les personnes prises en charge.

Art. 15, al. 1, phrase introductive, 2, let. a, et 4

1 *Ne concerne que le texte allemand.*

2 Le SIPA peut être mis en réseau avec les systèmes d'information fédéraux et cantonaux ci-après, de manière que les services et personnes compétents puissent transférer d'un système à un autre les données dont l'enregistrement est autorisé dans les deux systèmes:

a. les systèmes de gestion des cours (art. 93, al. 2, de la loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile, LPPCi[6]);

4 Le SPP collecte les données visées à l'art. 14, al. 4, auprès des services et personnes suivants:

a. la personne prise en charge;

b. ses supérieurs militaires;

c. le Service médico-militaire;

d. des tiers, pour autant que la personne prise en charge y ait consenti.

Art. 16, al. 1, phrase introductive et let. b^bis, h et i, et 1^ter

1 Le Groupement Défense donne accès en ligne aux données du SIPA, à l'exception des données visées à l'art. 14, al. 4, aux services et personnes ci-après, lorsque ces données sont nécessaires à l'accomplissement de leurs tâches légales ou contractuelles:

b^bis. les services et personnes chargés du recrutement;

6 RS **520.1**

h. la Centrale de compensation pour l'exécution du régime des allocations pour perte de gain;

i. le Service de renseignement de la Confédération, en vue d'identifier les personnes qui, sur la base de renseignements sur les menaces pour la sûreté intérieure ou extérieure au sens de l'art. 6, al. 1, let. a, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[7] pourraient représenter une menace pour la sécurité de l'armée;

1ter Le SPP donne accès en ligne aux données visées à l'art. 14, al. 4, aux services et personnes suivants:

a. les collaborateurs du SPP responsables de la prise en charge psychologique des militaires;

b. les services et médecins chargés du recrutement;

c. les services responsables du Service médico-militaire de l'armée.

Art. 17, al. 1, let. e, 4ter, 4quater, et 5

1 Les données du SIPA relatives à des infractions, des décisions ou des mesures pénales peuvent être conservées si elles ont fondé:

e. une décision d'exclusion de la protection civile prise en vertu de la LPPCi[8].

4ter Les données visées à l'art. 14, al. 1, let. abis, qui sont également des données sanitaires visées à l'art. 26, al. 2, sont conservées jusqu'à leur communication au Système d'information médicale de l'armée (MEDISA), mais une semaine au plus à compter de la fin du recrutement.

4quater Les données visées à l'art. 14, al. 4, sont conservées cinq ans au plus à compter de la fin de la prise en charge.

5 Les autres données du SIPA sont conservées cinq ans au plus à compter de la libération de l'obligation de servir dans l'armée ou dans la protection civile.

Chap. 2, section 2 (art. 18 à 23)

Abrogée

Art. 24 Organe responsable

Le Groupement Défense exploite le MEDISA.

Art. 27, phrase introductive

Le Groupement Défense collecte les données destinées à être versées au MEDISA auprès des services et personnes suivants:

7 RS **121**
8 RS **520.1**

Art. 28, al. 1, phrase introductive et let. c, et 3, phrase introductive

1 Le Groupement Défense donne accès en ligne aux données du MEDISA aux services et personnes suivants:

c. les spécialistes du SPP responsables de la prise en charge psychologique des militaires;

3 Le Groupement Défense communique aux services et autorités ci-après les décisions concernant l'aptitude au service militaire ou au service de protection civile:

Art. 30 Organe responsable

Le Groupement Défense exploite de manière décentralisée, sur chaque place d'armes et dans chaque hôpital militaire, un système d'information sur les patients (SIPAT).

Art. 33, phrase introductive

Le Groupement Défense collecte les données destinées à être versées aux SIPAT auprès des personnes suivantes:

Chap. 2, section 5 (art. 36 à 41)

Abrogée

Art. 42 Organe responsable

Le Groupement Défense exploite le Système d'information de médecine aéronautique (MEDIS FA).

Art. 45, phrase introductive

Le Groupement Défense collecte les données destinées à être versées au MEDIS FA auprès des services et personnes suivants:

Art. 46, al. 1, phrase introductive, et 2

1 Le Groupement Défense donne accès en ligne aux données du MEDIS FA aux personnes ci-après, lorsque ces données sont nécessaires à l'accomplissement de leurs tâches légales:

2 Il autorise les médecins traitants ou experts ainsi que les médecins de l'assurance militaire à consulter les données du MEDIS FA en présence de médecins ou de psychologues de l'Institut de médecine aéronautique.

Art. 47, al. 1 et 3

1 *Abrogé*

3 Si une personne est encore traitée ou prise en charge par l'Institut de médecine aéronautique après la durée de conservation visée à l'al. 2, ses données sont conservées dix ans après le traitement ou la prise en charge.

Titre précédant l'art. 48

Section 7
Système d'information sur le personnel d'intervention du commandement des Forces spéciales

Art. 48 Organe responsable

Le Groupement Défense exploite le Système d'information sur le personnel d'intervention du commandement des Forces spéciales (SIPI CFS).

Art. 49 But

Le SIPI CFS sert à l'accomplissement des tâches suivantes:

a. évaluer, sur les plans psychologique, psychiatrique et médical, les candidats au détachement de reconnaissance de l'armée ou au détachement spécial de la police militaire;

b. évaluer l'aptitude à l'engagement des militaires du détachement de reconnaissance de l'armée et du détachement spécial de la police militaire;

c. évaluer l'aptitude à l'engagement des personnes du commandement des Forces spéciales qui doivent appuyer les engagements.

Art. 50 Données

Le SIPI CFS contient les données nécessaires à l'évaluation et à l'appréciation de l'aptitude à l'engagement qui ont été collectées au moyen d'examens, de tests et de questionnaires en vue de l'appréciation, sous l'angle biostatistique, de l'endurance et du risque de défaillance au cours d'un engagement.

Art. 51, phrase introductive

Le Groupement Défense collecte les données destinées à être versées au SIPI CFS auprès des personnes suivantes:

Art. 52, al. 1

[1] Le Groupement Défense donne accès en ligne aux données du SIPI CFS aux psychologues chargés de l'évaluation et au médecin des opérations spéciales.

Art. 53, al. 2

[2] Les données des militaires du détachement de reconnaissance de l'armée et du détachement spécial de la police militaire ainsi que des personnes du commandement des Forces spéciales qui appuient les engagements sont conservées jusqu'à ce qu'ils quittent leur détachement ou leur commandement.

Titre précédant l'art. 54

Section 8 Système d'information pour l'assistance sociale

Art. 54 Organe responsable

Le Groupement Défense exploite le Système d'information pour l'assistance sociale (SISOC).

Art. 55 But

Le SISOC sert à la gestion administrative des activités de conseil et de prise en charge sociales des militaires, des membres de la protection civile, du personnel du Service de la Croix-Rouge, des personnes engagées dans le service de promotion de la paix, des membres de la justice militaire, des patients militaires ainsi que de leurs parents et survivants.

Art. 56 Données

Le SISOC contient des données relatives au soutien financier apporté et à la gestion des cas, des notes sur les entretiens et des documents personnels nécessaires à l'évaluation des prestations de conseil et de prise en charge.

Art. 57 Collecte des données

Le Groupement Défense collecte les données destinées à être versées au SISOC auprès des services et personnes suivants:

a. la personne concernée ou ses représentants légaux;
b. les commandements militaires;
c. les unités administratives compétentes de la Confédération et des cantons;
d. les personnes de référence désignées par la personne concernée;
e. le SIPA.

Art. 58 Communication des données

Le Groupement Défense donne accès en ligne aux données du SISOC aux services et personnes suivants:

a. le personnel du Service social de l'armée;
b. les militaires incorporés à l'état-major spécialisé du Service social de l'armée;
c. le service spécialisé Diversité dans l'Armée suisse, pour les données concernant ses bénéficiaires;
d. l'Aumônerie de l'armée, pour les données concernant ses bénéficiaires.

Art. 63, al. 2

2 Les données visées à l'art. 62 qui sont contenues dans le Système d'information pour la gestion des données du personnel (IGDP) peuvent être consultées en ligne par l'intermédiaire du SIP DEF.

Art. 65, al. 2

2 Les données des candidats qui n'ont pas été engagés sont détruites après six mois au plus.

Art. 72 Organe responsable

Le Groupement Défense exploite le Système d'information et de conduite pour le service sanitaire coordonné (SIC SSC).

Art. 73, phrase introductive

Le SIC SSC sert au mandataire du Conseil fédéral pour le service sanitaire coordonné (SSC), ainsi qu'aux services civils et militaires chargés de planifier, de préparer et de prendre les mesures sanitaires nécessaires (partenaires du SSC), à accomplir les tâches ci-après afin de maîtriser les événements sanitaires:

Art. 75, phrase introductive

Ne concerne que le texte allemand.

Art. 85, al. 2

2 Il sert aussi à l'exécution du régime des allocations pour perte de gain.

Art. 86, let. a, a^{bis} et h

Le MIL Office contient les données suivantes:

a. l'identité, l'adresse et les coordonnées;

a^{bis}. l'incorporation, le grade, la fonction et l'instruction;

h. les données pour l'administration et l'attribution de matériel de l'armée.

Art. 87, let. a

Les commandements militaires collectent les données destinées à être versées au MIL Office auprès des services et personnes suivants:

a. la personne concernée, qui peut aussi transmettre les données par un portail électronique du Groupement Défense;

Art. 88 Communication des données

Les commandements militaires communiquent les données du MIL Office aux services et personnes suivants:

a. les responsables de la planification des carrières;

b. les responsables de l'engagement;

c. les responsables des contrôles militaires;

d. la Centrale de compensation, pour l'exécution du régime des allocations pour perte de gain: les données visées à l'art. 86, let. a, a^{bis}, c et g.

Art. 94 Communication des données

Le Secrétariat général du DDPS donne accès en ligne aux données du SIGC aux services et personnes du DDPS chargés de la planification et du développement des cadres et de la gestion des compétences, ainsi qu'à la personne concernée et à ses supérieurs.

Art. 103, phrase introductive et let. a et c

Le SIC FT sert au Groupement Défense et à aux commandements militaires à:

a. assurer la planification de l'action et le suivi de la situation des états-majors et formations du commandement des Opérations, et de la Base d'aide au commandement;

c. mettre en réseau les moyens d'exploration, de conduite et d'engagement du commandement des Opérations et de la Base d'aide au commandement.

Art. 109, let. a

Le SIC FA sert aux Forces aériennes et à leurs commandements militaires à:

a. assurer la planification de l'action et le suivi de la situation des états-majors et des formations des Forces aériennes;

Art. 110, let. a

Le SIC FA contient les données ci-après sur les militaires:

a. le sexe;

Art. 119 Conservation des données

Les données du SICS sont détruites une fois l'engagement terminé.

Art. 121 But

Les SISIM servent à gérer l'instruction et la qualification:

a. des militaires;

b. des civils qui participent à un engagement de l'armée de durée déterminée;

c. des tiers qui s'entraînent sur les simulateurs.

Art. 123, phrase introductive (ne concerne que le texte allemand) et let. c

Les services et personnes compétents collectent les données destinées à être versées aux SISIM auprès des services et personnes suivants:

c. les supérieurs militaires ou civils de la personne concernée.

Art. 124, al. 2, let. c

2 Ils communiquent les données aux services et personnes suivants:

c. les civils instruits sur les simulateurs et les tiers qui s'y exercent ainsi que les services et personnes qui leur sont supérieurs.

Art. 125, al. 2

2 Si des militaires, des civils ou des tiers s'exercent régulièrement sur les mêmes simulateurs, les données de leurs entraînements peuvent être conservées dix ans.

Art. 131 Conservation des données

Les données du LMS DDPS sont conservées dix ans au plus:

a. après la libération de l'obligation de servir dans l'armée, pour les militaires;

b. après la fin des rapports de travail, pour les employés du DDPS.

Titre précédant l'art. 138

Section 4
Système d'information sur la circulation routière et la navigation de l'armée

Art. 138 Organe responsable

Le Groupement Défense exploite le Système d'information sur la circulation routière et la navigation de l'armée (SI OCRNA).

Art. 139, phrase introductive et let. a, c, e et f

Le SI OCRNA sert à:

a. établir et administrer les autorisations de conduire militaires pour les conducteurs de véhicules et de bateaux, les permis de conduire fédéraux pour les conducteurs de bateaux et les permis d'expert militaire de la circulation;

c. exécuter les mesures administratives visant les personnes détentrices d'un document mentionné à la let. a;

e. contrôler l'instruction des élèves conducteurs, des moniteurs de conduite de l'armée et des experts militaires de la circulation;

f. *abrogée*

Art. 140, phrase introductive et let. b à d

Le SI OCRNA contient les données ci-après sur les élèves conducteurs et les personnes autorisées à conduire, les moniteurs de conduite de l'armée et les experts militaires de la circulation:

b. l'instruction suivie, les autorisations de conduire militaires et les permis;

c. les mesures administratives;

d. les résultats du dernier examen de contrôle et la date du prochain examen.

Art. 141, phrase introductive et let. b à e

Le Groupement Défense collecte les données destinées à être versées au SI OCRNA auprès des services et personnes suivants:

b. le Système d'information sur l'admission à la circulation (SIAC) de l'Office fédéral des routes;

c. le SIP DEF;

d. l'IGDP;

e. les services et personnes chargés des tâches visées à l'art. 139.

Art. 142, al. 1

1 Le Groupement Défense communique les données du SI OCRNA aux services et personnes suivants:

a. les services et personnes chargés des tâches visées à l'art. 139;

b. le SIPA et le SIAC.

Art. 143 Conservation des données

1 Les données du SI OCRNA sont conservées 80 ans au plus après leur enregistrement, notamment celles qui portent sur les mesures administratives prononcées par l'Office de la circulation routière et de la navigation de l'armée.

2 Les données sur les mesures administratives civiles sont conservées au plus aussi longtemps qu'elles le sont dans le SIAC.

3 Les données relatives à un examen de contrôle ne sont conservées que jusqu'à l'examen suivant.

Art. 143c, let. l

Le SPHAIR-Expert contient les données suivantes des personnes intéressées, du personnel et des candidats visés à l'art. 143*b*:

l. l'intérêt personnel porté à l'embauche, à la formation (instruction), au perfectionnement, ainsi qu'au choix du métier et de la fonction.

Insérer la section 6 (art. 143g à 143l) avant le titre du chap. 5

Section 6 Système d'information pour l'instruction de conduite

Art. 143g Organe responsable

Le Groupement Défense exploite le Système d'information pour l'instruction de conduite (SIIC).

Art. 143h But

Le SIIC sert à contrôler l'instruction, à analyser ses résultats et à organiser les examens.

Art. 143i Données

Le SIIC contient les données suivantes:

a. l'identité, le domicile, le lieu d'origine, le canton d'origine et les adresses;
b. l'incorporation, le grade, la fonction et les services accomplis dans l'armée;
c. le numéro AVS;
d. le sexe;
e. la date de naissance;
f. la formation et les examens, le numéro de candidat, la langue d'examen et les indications relatives à l'examen (date, heure, lieu, nom de l'expert);
g. les prestations personnelles (date de présentation, résultats);
h. la participation aux examens et les résultats obtenus.

Art. 143j Collecte des données

Le Groupement Défense collecte les données destinées à être versées au SIIC auprès des services et personnes suivants:

a. la personne concernée;
b. les supérieurs militaires de la personne concernée;
c. les unités administratives compétentes du Groupement Défense;
d. le SIPA.

Art. 143k Communication des données

1 Le Groupement Défense donne accès en ligne aux données du SIIC aux services et personnes responsables:

a. de la saisie des données dans le SIIC;

b. de la coordination des examens pour les divers modules.

2 Il communique les données du SIIC:

a. à l'organe civil responsable de l'établissement du certificat attestant la réussite d'un module donné;

b. aux personnes enregistrées dans le SIIC, à titre de preuve de l'instruction suivie.

Art. 143l Conservation des données

Les données du SIIC sont conservées dix ans au plus après leur saisie.

Art. 145 But

Le SICSP sert à l'exécution:

a. des contrôles de sécurité relatifs aux personnes;

b. des évaluations du potentiel d'abus ou de dangerosité en ce qui concerne l'arme personnelle;

c. des contrôles de fiabilité.

Art. 147, al. 2, phrase introductive et let. c et d

2 Elles ont accès en ligne aux registres et banques de données ci-après, dans le cadre prévu par les dispositions correspondantes:

c. le système d'information INDEX SRC visé à l'art. 51 LRens[9], sous réserve de l'art. 20, al. 2, de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[10];

d. les banques de données de l'Office central des armes visées à l'art. 32*a*, al. 1, LArm[11].

Art. 148, al. 1, phrase introductive (ne concerne que le texte allemand) et let. c, ch. 2bis, et d

1 Le CSP DDPS donne accès en ligne aux données du SICSP aux autorités et services suivants:

c. les services responsables de l'exécution des contrôles de sécurité relatifs aux personnes:

2bis. à la Société nationale du réseau de transport,

9 RS **121**
10 RS **120**
11 RS **514.54**

d. les services fédéraux responsables des tâches relatives à la sécurité, si les activités de ces services dépendent des données concernant les contrôles de sécurité relatifs aux personnes et si les données ne sont pas préjudiciables à la personne concernée.

Titre précédant l'art. 167a

Section 5 Système de journal et de rapport de la Police militaire

Art. 167a Organe responsable

Le Groupement Défense exploite le Système de journal et de rapport de la Police militaire (JORASYS).

Art. 167b, let. a et b

Le JORASYS sert à l'accomplissement des tâches visées à l'art. 100, al. 1, LAAM[12], notamment:

a. tenir le journal des centrales d'engagement du commandement de la Police militaire;

b. établir les rapports sur les tâches de police judiciaire et de police de sûreté des formations professionnelles du commandement de la Police militaire;

Art. 167d Collecte des données

Le commandement de la Police militaire collecte les données destinées à être versées au JORASYS à partir des systèmes et auprès des services et personnes suivants:

a. la personne concernée;

b. les commandements militaires;

c. les unités administratives compétentes de la Confédération, des cantons et des communes;

d. les autorités pénales civiles et militaires, les autorités d'exécution des peines et les autorités chargées du contentieux administratif;

e. par accès en ligne ou automatiquement par une interface:
   1. l'index national de police,
   2. le système de recherches informatisées de police RIPOL de l'Office fédéral de la police,
   3. le SIAC,
   4. les banques de données visées à l'art 32*a*, al. 1, LArm[13],
   5. la consultation en ligne des registres d'armes cantonaux,
   6. le SIPA,

12 RS **510.10**
13 RS **514.54**

7. le SIP DEF,
8. le SI OCRNA,
9. le Système d'information concernant l'interface des données de la défense (SI IDD),
10. le PSN.

Art. 167e, al. 1, et 2, let. b et c

1 Le commandement de la Police militaire donne accès en ligne aux données du JORASYS aux personnes suivantes:

a. le personnel des centrales d'engagement du commandement de la Police militaire;

b. le personnel du commandement de la Police militaire pour l'accomplissement des tâches visées à l'art. 100 LAAM[14];

c. le personnel du Service de protection préventive de l'armée (SPPA) pour l'accomplissement des tâches visées à l'art. 100 LAAM.

2 Il communique des extraits de données du JORASYS, sous forme écrite, aux services et personnes suivants:

b. *ne concerne que le texte allemand;*

c. les services chargés de la sécurité des informations et des objets.

Art. 167f Conservation des données

Les données du JORASYS sont conservées dix ans après la fin des activités de la Police militaire relatives à un incident.

Insérer la section 6 (art. 167g à 167l) avant le titre du chap. 6

Section 6
Système d'information sur la protection préventive de l'armée

Art. 167g Organe responsable

Le Groupement Défense exploite le Système d'information sur la protection préventive de l'armée (SIPPA).

Art. 167h But

Le SIPPA sert au SPPA à accomplir les tâches visées à l'art. 100, al. 1, LAAM[15], notamment:

14 RS **510.10**
15 RS **510.10**

a. apprécier la situation militaire en matière de sécurité;

b. prendre des mesures préventives de protection contre l'espionnage, le sabotage et d'autres activités illicites;

c. tenir son journal et diriger son engagement.

Art. 167i Données

Le SIPPA contient les données ci-après sur les personnes liées à une menace potentielle de l'armée:

a. l'identité;

b. l'état civil, le lieu de naissance, le lieu d'origine, la profession et la formation;

c. la nationalité, l'appartenance ethnique, la confession, le statut de résident;

d. les preuves de l'identité, avec les caractéristiques physiques;

e. l'orientation politique et idéologique;

f. les résultats du recrutement, l'incorporation, le grade, la fonction, l'instruction suivie, les qualifications, les états de service, les engagements et l'équipement à l'armée ou à la protection civile;

g. les revenus et la fortune;

h. les données médicales et biométriques;

i. les images et les enregistrements vidéo et audio;

j. les personnes de référence et leur identité;

k. le lieu de séjour de la personne avec les profils de déplacement;

l. les moyens de locomotion et de communication, y compris leur utilisation, leur positionnement et les profils de déplacement;

m. les détails sur la menace potentielle de l'armée émanant de la personne;

n. d'autres informations et données dont le SPPA a besoin pour accomplir les tâches visées à l'art. 100, al. 1, LAAM[16].

Art. 167j Collecte des données

Le SPPA collecte les données destinées à être versées au SIPPA:

a. auprès de la personne concernée;

b. auprès des commandements militaires;

c. auprès des services de renseignement suisses et étrangers;

d. auprès des unités administratives de la Confédération, des cantons et des communes;

16 RS **510.10**

e. auprès des autorités pénales civiles et militaires et des autorités chargées du contentieux administratif;

f. en consultant des sources publiques;

g. en accédant en ligne aux systèmes d'information suivants:
   1. le SIPA,
   2. le SI OCRNA,
   3. le JORASYS,
   4. le SI IDD,
   5. le PSN.

Art. 167k Communication des données

1 Le SPPA donne à son personnel un accès en ligne aux données du SIPPA pour l'accomplissement des tâches visées à l'art. 100 LAAM[17].

2 Il communique des extraits de données du SIPPA, sous forme écrite, aux services et personnes ci-après, lorsque ces données sont nécessaires à l'accomplissement de leurs tâches légales:

a. les services chargés de la sécurité des informations et des objets;

b. les services chargés de la cyberdéfense;

c. le service spécialisé Extrémisme dans l'armée;

d. le commandement de la Police militaire;

e. le Personnel de l'armée;

f. les commandants de troupe pour leur domaine de compétence;

g. le Service de renseignement de la Confédération, sous réserve de l'art. 5, al. 5, LRens[18];

h. l'Office fédéral de la police.

Art. 167l Conservation des données

Les données du SIPPA sont conservées cinq ans au plus à compter du moment où la personne concernée n'est plus liée à une menace potentielle de l'armée.

17 RS **510.10**
18 RS **121**

Titre précédant l'art. 168

Chapitre 6 Autres systèmes d'information

Section 1 Système d'information du Centre de dommages du DDPS

Art. 168 Organe responsable

Le Secrétariat général du DDPS exploite le Système d'information du Centre de dommages du DDPS (SCHAMIS).

Art. 169, phrase introductive et let. d et e

Le SCHAMIS sert à:

d. établir des attestations d'assurance électroniques pour les véhicules de la Confédération;

e. régler les sinistres impliquant les véhicules à moteur des députés, conformément à l'art. 4, al. 2, de l'ordonnance de l'Assemblée fédérale du 18 mars 1988 relative à la loi sur les moyens alloués aux parlementaires[19].

*Art. 170, phrase introductive et let. a et a^bis^*

Le SCHAMIS contient:

a. les données suivantes relatives aux lésés et aux auteurs du dommage:
   1. l'identité, l'adresse, les coordonnées et la langue de correspondance,
   2. le numéro d'assurance sociale,
   3. la situation financière et professionnelle,
   4. les assurances,
   5. les données médicales et sanitaires,
   6. les procédures pénales, civiles, disciplinaires et administratives,
   7. la gestion militaire,
   8. les détenteurs de véhicules;

a^bis^. les données suivantes relatives à des tiers, nécessaires pour atteindre le but visé:
   1. l'identité, l'adresse, les coordonnées et la langue de correspondance,
   2. la profession;

Art. 171, phrase introductive et let. i

Le Secrétariat général du DDPS collecte les données destinées à être versées au SCHAMIS auprès des services et personnes suivants:

i. les assurances.

19 RS **171.211**

Art. 172 Communication des données

[1] Le Secrétariat général du DDPS donne accès en ligne aux données du SCHAMIS au personnel chargé des tâches visées à l'art. 169.

[2] Il communique aux tiers collaborant à la procédure les données nécessaires pour régler les sinistres et les actions en responsabilité civile.

Art. 173 Conservation des données

Les données du SCHAMIS sont conservées dix ans à compter de la décision qui clôt la procédure.

Titre précédant l'art. 174

Section 2
Système d'information concernant l'interface des données de la défense

Art. 174 Organe responsable

Le Groupement Défense exploite le Système d'information concernant l'interface des données de la défense (SI IDD).

Art. 175, phrase introductive

Le SI IDD sert à l'accomplissement des tâches suivantes:

Art. 176, phrase introductive et let. c

Le SI IDD contient les données suivantes:

c. les données nécessaires à l'échange de données selon l'art. 175, let. c.

Art. 177, phrase introductive

Le Groupement Défense collecte les données destinées à être versées au SI IDD auprès des services et personnes suivants:

Art. 178 Communication des données

Le Groupement Défense donne accès en ligne aux données du SI IDD aux services et personnes suivants:

a. les commandements militaires et les unités administratives compétentes de la Confédération et des cantons, pour les données visées à l'art. 176, let. a et b;

b. les services et personnes responsables des systèmes d'information de l'armée, pour les données visées à l'art. 176, let. c.

Art. 179 Conservation des données

Les données du SI IDD sont conservées cinq ans au plus.

Art. 179b, let. d

Ne concerne que le texte allemand.

Art. 179c, al. 4

4 Il contient les données sur les candidats et sur les employés qui figurent respectivement dans le dossier de candidature et dans le dossier du personnel gérés selon la LPers[20] et ses dispositions d'exécution.

Art. 179d, let. e

Les unités administratives du Groupement Défense collectent les données destinées à être versées au PSN auprès des services et personnes suivants:

e. les unités administratives compétentes de la Confédération et des cantons, à partir des systèmes d'information de l'armée, de l'IGDP et de la banque de données visée à l'art. 32*a*, al. 1, let. c, LArm[21].

Art. 179e, al. 2, let. e

2 Elles communiquent les données du PSN aux services et personnes ci-après pour l'accomplissement de leurs tâches légales ou contractuelles:

e. les unités administratives de la Confédération, par une interface avec l'IGDP;

Titre précédant l'art. 179g

Section 4 Système d'information du tir hors du service

Art. 179g Organe responsable

Le Groupement Défense exploite le Système d'information du tir hors du service (SaD).

Art. 179h, phrase introductive

Le SaD sert à l'administration et à l'exploitation des affaires relatives au tir hors du service dans les domaines suivants:

Art. 179i, phrase introductive

Le SaD contient les données ci-après sur les militaires astreints au tir, les commissaires du tir hors du service, les sociétés de tir reconnues, leurs membres et les tireurs pour assurer le contrôle des tirs obligatoires et des autres tirs au profit de la défense nationale:

20 RS **172.220.1**
21 RS **514.54**

Art. 179j, phrase introductive

Le Groupement Défense collecte les données destinées à être versées au SaD auprès des services et personnes suivants:

Art. 179k, al. 1, phrase introductive, et 2

1 Le Groupement Défense donne accès en ligne aux données du SaD aux services et personnes ci-après pour l'accomplissement de leurs tâches:

2 Il communique à l'assurance-vieillesse et survivants, aux administrations fiscales et au service chargé des opérations de paiement les données du SaD qui sont nécessaires au décompte et à l'imputation visés à l'art. 179*h*.

Art. 179l, al. 1

1 Les données du SaD sont conservées cinq ans à compter de la dernière inscription sur la personne concernée.

Insérer la section 5 (art. 179m à 179r) avant le titre du chap. 7

Section 5 Système d'information *Master Data Management*

Art. 179m Organe responsable

Le Secrétariat général du DDPS exploite le Système d'information *Master Data Management* (MDM).

Art. 179n But

Le MDM sert à administrer et à établir des données concernant les partenaires actuels ou potentiels impliqués dans les processus d'affaires du DDPS relatifs aux domaines finances, acquisition, logistique, immobilier et personnel.

Art. 179o Données

Le MDM contient les données ci-après concernant les partenaires actuels ou potentiels:

a. le nom et les données sur l'entreprise;
b. l'adresse;
c. les coordonnées bancaires;
d. les coordonnées;
e. le sexe;
f. la nationalité;
g. la langue de correspondance;
h. la catégorie d'étranger;

i. la profession;

j. la date de naissance;

k. le numéro d'assurance sociale;

l. la forme juridique;

m. le numéro d'identification de l'entreprise (IDE), le numéro fiscal et d'autres numéros et codes d'enregistrement spécifiques aux entreprises;

n. les données concernant une faillite;

o. le statut du partenariat;

p. les données de base logistiques, comme les données de base sur le matériel et les données sur la structure des systèmes, en lien avec le partenaire.

Art. 179p Collecte des données

Le Secrétariat général du DDPS collecte les données destinées à être versées au MDM:

a. auprès des partenaires actuels ou potentiels;

b. auprès des unités administratives de la Confédération, des cantons et des communes;

c. à partir du système d'information de la Confédération exploité en dehors du DDPS au profit du *Master Data Management*, par une interface;

d. auprès des fournisseurs et des fabricants de matériel suisses et étrangers.

Art. 179q Communication des données

Le Secrétariat général du DDPS donne accès en ligne aux données du MDM aux services et personnes chargés des processus d'affaires du DDPS relatifs aux domaines finances, acquisition, logistique, immobilier et personnel.

Art. 179r Conservation des données

1 Les données du MDM sont conservées après la fin des rapports d'affaires avec un partenaire pendant:

a. 10 ans, pour les données visées à l'art. 179*o*, let. a à o;

b. 50 ans, pour les données visées à l'art. 179*o*, let. p.

2 S'il est établi qu'une personne n'est pas un partenaire, ses données sont conservées deux ans.

Art. 181, al. 1, let. a, et 2, phrase introductive

1 Les moyens de surveillance contribuent à l'exécution des tâches suivantes:

a. garantir la sécurité des militaires ainsi que des installations et du matériel de l'armée dans le domaine:

1. de la troupe,
2. des objets de l'armée, de l'administration militaire ou de tiers utilisés à des fins militaires;

2 L'armée peut fournir aux autorités civiles qui en font la demande des prestations de surveillance avec appui aérien en engageant ses moyens de surveillance et le personnel nécessaire dans les cas suivants:

Art. 186, al. 3

3 Il peut, dans le cadre des affaires étrangères et de la politique de sécurité, conclure des accords internationaux sur le traitement transfrontalier de données personnelles dont le traitement ne requiert pas une base dans une loi au sens formel conformément à la LPD[22].

II

Les actes mentionnés ci-après sont modifiés comme suit:

1. Loi du 3 février 1995 sur l'armée[23]

Art. 146 Systèmes d'information de l'armée

Le traitement des données personnelles dans les systèmes d'information et lors de l'engagement de moyens de surveillance de l'armée et de l'administration militaire est réglé par la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS[24].

2. Loi du 18 décembre 2020 sur la sécurité de l'information[25]

Art. 45, al. 1, 3bis et 6, let. d

1 Les services spécialisés CSP exploitent un système d'information. Celui-ci sert à l'exécution:

a. des contrôles de sécurité relatifs aux personnes;

b. des évaluations du potentiel d'abus ou de dangerosité en ce qui concerne l'arme personnelle;

c. des contrôles de fiabilité;

d. des contrôles de loyauté.

22 RS **235.1**
23 RS **510.10**
24 RS **510.91**
25 RS ...; FF **2020** 9665

3bis Un profilage au sens de la LPD, y compris un profilage à risque élevé, peut être effectué à l'aide des données contenues dans le système d'information pour analyser, évaluer, apprécier ou prédire les aspects personnels ci-après relatifs à une personne physique dans les buts visés à l'al. 1:

a. risque pour la sécurité;

b. potentiel d'abus et de dangerosité en ce qui concerne l'arme personnelle.

6 Les données visées à l'al. 4 peuvent être collectées automatiquement et systématiquement en ligne dans les systèmes d'information suivants:

d. banques de données de l'Office central des armes visées à l'art. 32*a*, al. 1, de la loi du 20 juin 1997 sur les armes[26].

III

1 La présente loi est sujette au référendum.

2 Le Conseil fédéral fixe la date d'entrée en vigueur sous réserve des al. 3 et 4.

3 L'art. 2*b* n'entre pas en vigueur avant la loi fédérale du 25 septembre 2020 sur la protection des données[27].

4 L'art. 45, al. 3bis, de la loi du 18 décembre 2020 sur la sécurité de l'information[28], n'entre pas en vigueur avant la loi fédérale du 25 septembre 2020 sur la protection des données[29].

26 RS **514.54**
27 RS **...**; FF **2020** 7397
28 RS **...**; FF **2020** 9665
29 RS **...**; FF **2020** 7397