Ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée

(ordonnance sur la sécurité de l'information, OSI)

du … Avant-projet du 24 août 2022

Le Conseil fédéral suisse,

vu les art. 2, al. 3 et 4, 12, al. 3, 83, al. 3, 84, al. 1, 85, al. 1 et 2, et 86, al. 4, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],

arrête:

Section 1 Dispositions générales

Art. 1 Objet

(art. 1 LSI)

La présente ordonnance régit les tâches, les responsabilités, les compétences et les procédures qui permettent de garantir la sécurité de l'information au sein de l'administration fédérale et de l'armée.

Art. 2 Champ d'application

(art. 2, 3 et 84, al. 3, LSI)

[1] La présente ordonnance s'applique:

a. au Conseil fédéral;

b. aux unités de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[2];

c. à l'armée.

[2] La LSI et la présente ordonnance s'appliquent aux unités de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA[3] de la manière suivante:

RS **128.1**

1 RS **128**
2 RS **172.010.1**
3 RS **172.010**

a. aux unités administratives qui ont accès aux moyens informatiques des fournisseurs internes de prestations informatiques visés à l'art. 9 de l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI)[4] relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28: la LSI et la présente ordonnance;

b. aux unités administratives qui utilisent les moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28: la LSI et la présente ordonnance;

c. aux unités administratives qui ne sont pas concernées par les let. a et b, mais qui traitent des informations classifiées de la Confédération: les art. 9 à 15 et 27 à 73 LSI et les dispositions de la section 4 de la présente ordonnance.

3 La Chancellerie fédérale ou les départements peuvent demander au Conseil fédéral de soumettre à la LSI, à la présente ordonnance ou à certaines des parties de cette dernière les unités administratives de l'administration fédérale décentralisée qui ne sont pas concernées par l'al. 2.

4 L'annexe 1 porte sur:

a. les unités administratives visées à l'al. 2;

b. les unités administratives visées à l'al. 3 et les dispositions de la LSI et de la présente ordonnance qui les concernent.

5 Les organisations visées à l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[3] sont exclues du champ d'application de la LSI et de la présente ordonnance.

6 S'appliquent aux cantons sous réserve de l'art. 3, al. 2, LSI:

a. lors du traitement d'informations classifiées de la Confédération: les dispositions de la section 4;

b. lors de l'accès aux moyens informatiques de la Confédération: les art. 28 à 30 et 34.

Section 2 Principes

Art. 3 Objectifs de sécurité

(art. 7, al. 2, let. a, LSI)

1 Les organisations visées à l'art. 2 veillent ensemble à protéger leurs informations et leurs moyens informatiques en fonction des risques et à faire preuve d'une résilience appropriée envers les risques pour la sécurité de l'information.

2 En collaborant et en échangeant des informations avec les autres autorités fédérales, les cantons, les communes, l'économie, la société, les milieux scientifiques et les partenaires internationaux, elles contribuent à améliorer durablement la sécurité de l'information de la Suisse.

4 RS **172.010.58**

3 Elles s'engagent à harmoniser sur le plan national et international les prescriptions et les niveaux en matière de sécurité afin de permettre l'interaction des autorités fédérales avec d'autres autorités de la Confédération, des cantons et des communes.

Art. 4 Responsabilité

1 Les unités administratives sont responsables de la protection des informations qu'elles traitent ou dont elles délèguent le traitement et sont responsables de la sécurité de leurs moyens informatiques qu'elles exploitent elles-mêmes ou qu'elles font exploiter par des tiers.

2 Elles assument toutes les tâches qui relèvent de leur domaine de compétence que la présente ordonnance et le droit fédéral n'attribuent pas à une autre organisation ou à un autre service.

3 Les collaborateurs de l'administration fédérale et les militaires qui traitent ou utilisent des informations ou des moyens informatiques de la Confédération sont responsables du respect des prescriptions en la matière.

4 Les supérieurs hiérarchiques de tous les échelons sont responsables de la formation de leurs collaborateurs dans le domaine de la sécurité de l'information en fonction de leurs tâches et s'assurent que leurs collaborateurs respectent les directives.

Section 3 Gestion de la sécurité de l'information

Art. 5 Système de management de la sécurité de l'information
(art. 7, al. 1, LSI)

1 Les unités administratives établissent chacune un système de management de la sécurité de l'information (SMSI).

2 Elles fixent les objectifs de leur SMSI, vérifient chaque année si ces objectifs ont été atteints et relèvent les indicateurs nécessaires à cette fin.

3 Elles font contrôler leur SMSI au moins tous les trois ans par un service indépendant ou par le département et veillent à continuellement améliorer le système.

4 Elles coordonnent leur SMSI avec la gestion ordinaire des risques, la gestion de la continuité des activités et la gestion des crises.

Art. 6 Gestion des bases légales et des engagements contractuels
(art. 7, al. 1, LSI)

1 Les unités administratives, les départements et le service spécialisé de la Confédération pour la sécurité de l'information établissent la liste des bases légales déterminantes pour leur domaine de compétence et de leurs obligations contractuelles en matière de sécurité de l'information et la tiennent à jour.

2 Les unités administratives et les départements consultent le service spécialisé de la Confédération pour la sécurité de l'information en cas de directives et de projets dans le domaine de la sécurité.

Art. 7 Inventaire des objets à protéger
(art. 7, al. 1, LSI)

1 Les unités administratives dressent l'inventaire de leurs objets à protéger et le tiennent un jour.

2 Par objets à protéger, on entend:

a. les collections de toutes les données traitées dans le but d'exécuter une tâche de la Confédération;

b. les moyens informatiques visés à l'art. 5, let. a, LSI.

3 L'inventaire sert à justifier:

a. le besoin de protection des objets à protéger;

b. les responsabilités liées aux objets à protéger;

c. le cas échéant. l'utilisation partagée de l'objet à protéger;

d. la participation de tiers;

e. le résultat de l'évaluation des risques;

f. la mise en œuvre des mesures de sécurité et l'acceptation des risques résiduels;

g. les contrôles et les audits périodiques.

Art. 8 Gestion des risques
(art. 7, al. 2, let. b, et 8 LSI)

1 Les unités administratives évaluent en continu les risques pour leurs objets à protéger et assument pour ce faire notamment les tâches suivantes:

a. elles analysent régulièrement les menaces et les vulnérabilités et en évaluent les répercussions sur les objets à protéger;

b. elles mettent en œuvre les mesures nécessaires et en contrôlent les effets;

c. elles contrôlent le respect des directives;

d. elles démontrent l'acceptation des risques résiduels.

2 Le service spécialisé de la Confédération pour la sécurité de l'information, les unités administratives qui fournissent des prestations et les organes de sécurité de la Confédération informent les unités administratives et les départements des menaces et vulnérabilités actuelles et des risques qui les concernent. Ils émettent au besoin des recommandations de mesures de limitation des risques.

3 Les unités administratives rendent compte de leurs risques pour la sécurité de l'information dans le cadre du processus ordinaire de gestion des risques conformément aux directives de l'Administration fédérale des finances.

Art. 9 Autorisation et exceptions
(art. 7, al. 1, LSI)

1 Si une unité administrative n'est pas en mesure d'observer une directive concernant un objet à protéger, elle a besoin d'une autorisation du service ayant émis la directive.

2 Le service spécialisé de la Confédération pour la sécurité de l'information et les départements peuvent déléguer l'octroi d'exceptions.

3 Si une exception relevant du domaine de compétence du service spécialisé de la Confédération pour la sécurité de l'information concerne également des directives de la Chancellerie fédérale sur la transition numérique et la gouvernance de l'informatique, le service spécialisé de la Confédération pour la sécurité de l'information consulte au préalable le délégué TNI conformément à l'art. 4, al. 1, OTNI[5].

4 Les unités administratives, les départements et le service spécialisé de la Confédération pour la sécurité de l'information tiennent à jour la liste des autorisations exceptionnelles:

a. qu'ils ont eux-mêmes accordées;

b. qui ont été accordées pour leurs propres objets à protéger.

Art. 10 Collaboration avec les tiers
(art. 9 LSI)

1 Les unités administratives évaluent à la lumière les directives de l'art. 8 les risques encourus par leurs objets à protéger lors de la collaboration avec des tiers et leur dépendance envers des tiers.

2 Les services d'achat visés aux art. 9 et 10 de l'ordonnance du 24 octobre 2012 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP)[6] collaborent à l'évaluation et mettent les informations nécessaires à disposition.

3 Après avoir consulté la Conférence des achats de la Confédération visée à l'art. 24 Org-OMP, le service spécialisé de la Confédération pour la sécurité de l'information émet des recommandations quant aux dispositions relatives à la sécurité de l'information que doivent contenir tous les contrats d'acquisition et de prestation de la Confédération.

Art. 11 Formation et sensibilisation
(art. 7, al. 1 et 20, al. 1, let. c, LSI)

1 Les unités administratives forment leurs collaborateurs à leur entrée en fonction, puis périodiquement de manière à ce qu'ils puissent assumer leurs responsabilités en matière de sécurité de l'information. Elles tiennent la liste des formations et des participants.

2 La formation comprend notamment:

a. l'identification correcte du besoin de protection des informations;

5 RS **172.010.58**
6 RS **172.056.15**

b. l'utilisation sûre des informations et des moyens informatiques;

c. la réaction correcte en cas de soupçon d'incident de sécurité;

d. la connaissance de l'organisation de sécurité et des personnes de contact en cas de questions relatives à la sécurité de l'information;

e. les tâches de contrôle des supérieurs hiérarchiques;

f. la mise en œuvre de la sécurité de l'information lors de projets et de l'exploitation.

3 Les unités administratives, les départements et le service spécialisé de la Confédération pour la sécurité de l'information veillent à sensibiliser régulièrement les collaborateurs de tous les échelons aux risques pour la sécurité de l'information.

4 Le service spécialisé de la Confédération pour la sécurité de l'information assure la coordination et établit des outils de formation et de sensibilisation.

Art. 12 Gestion des incidents
(art. 7, al. 1, et 10, al. 1, LSI)

1 Les unités administratives fixent en accord avec les fournisseurs de prestations la manière dont les incidents et les failles de sécurité sont annoncées et maîtrisées. Elles règlent également la compétence décisionnelle en matière de mesures urgentes.

2 Les fournisseurs de prestations annoncent immédiatement aux unités administratives auxquelles ils fournissent leurs prestations les incidents et les failles de sécurité qui les concernent et les aident à les maîtriser.

3 Le service spécialisé de la Confédération pour la sécurité de l'information peut aider les unités administratives et les départements à maîtriser les incidents de sécurité et à traiter les failles de sécurité.

4 Les unités administratives vérifient lors de la maîtrise des incidents de sécurité s'il est nécessaire de faire une annonce au Préposé fédéral à la protection des données et à la transparence en vertu de la législation sur la protection des données.

5 Elles informent immédiatement leur département et le service spécialisé de la Confédération pour la sécurité de l'information de l'incident ou de la faille de sécurité si l'une des conditions suivantes est remplie:

a. le fonctionnement de l'administration fédérale ou de l'armée pourrait être compromis;

b. un moyen informatique relevant des catégories de sécurité «protection élevée» ou «protection très élevée» est concerné;

c. plusieurs départements pourraient être touchés;

d. la protection des informations classifiées d'un État ou d'une organisation internationale avec lequel ou laquelle le Conseil fédéral a conclu un traité international selon l'art. 87 LSI pourrait être menacée;

e. l'incident ou la faille de sécurité pourrait avoir une grande importance politique;

f. l'incident ou la faille de sécurité requiert des mesures sortant de la procédure visée à l'al. 1.

6 Le service spécialisé de la Confédération pour la sécurité de l'information évalue le risque et le soutien requis avec l'unité administrative concernée.

7 Dans les cas visés à l'al. 5, il peut, en accord avec l'unité administrative et le département concernés, diriger les opérations de maîtrise de l'incident de sécurité ou de traitement de la faille de sécurité. Il a dans ce cadre les tâches et les compétences suivantes:

a. il peut obliger les unités administratives, les fournisseurs de prestations et les tiers à lui communiquer toutes les informations nécessaires;

b. il peut ordonner des mesures urgentes;

c. il peut demander l'aide de spécialistes externes;

d. il informe la direction de l'unité administrative concernée et des départements de l'avancement des opérations.

8 Lorsque la sécurité de l'information a été rétablie à la suite d'un incident ou d'une faille de sécurité et que les travaux de suivi nécessaires et leur financement ont été arrêtés, le service spécialisé de la Confédération pour la sécurité de l'information rend la direction de la gestion à l'unité administrative concernée.

Art. 13 Planification des contrôles et des audits

(art. 7, al. 1, 81, al. 2, let. c, et 83, al. 1, let. c, LSI)

1 Les unités administratives et les départements fixent dans une planification annuelle de contrôle et d'audit la manière de contrôler en fonction du risque le respect des prescriptions de la présente ordonnance et l'efficacité des mesures permettant de garantir la sécurité de l'information dans leur domaine de compétence et auprès des tiers mandatés.

2 Les audits menés auprès de tiers disposant d'une déclaration de sécurité relative aux entreprises visée à l'art. 61 LSI doivent être coordonnés avec le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises visé à l'art. 51, al. 2, LSI.

3 Le service spécialisé de la Confédération pour la sécurité de l'information collecte le besoin de contrôle et d'audit pour garantir la sécurité de l'information de l'ensemble de l'administration fédérale et de l'armée et le communique au Contrôle fédéral des finances.

Art. 14 Compte rendu

(art. 7, al. 1, 81, al. 2, let. c, et 83, al. 1, let. h, LSI)

1 Les départements et la Chancellerie fédérale rendent compte chaque année au service spécialisé de la Confédération pour la sécurité de l'information de la situation en matière de sécurité de l'information dans leur domaine de compétence.

2 Ils collectent les informations nécessaires auprès des unités administratives et de leurs fournisseurs de prestations.

3 Le service spécialisé de la Confédération pour la sécurité de l'information rend compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

4 Il fixe les modalités des comptes rendus des fournisseurs internes de prestations visés à l'art. 9 OTNI[7].

5 Il coordonne les comptes rendus avec les autorités visées à l'art. 2, al. 1, LSI.

Art. 15 Directives de gestion de la sécurité de l'information
(art. 85 LSI)

Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences minimales auxquelles la gestion de la sécurité de l'information visée aux art. 5 à 14 doit répondre.

Section 4 Informations classifiées

Art. 16 Principes
(art. 11 LSI)

1 La communication et la mise à disposition d'informations classifiées et l'établissement des supports d'information classifiés doivent être limités autant que possible.

2 Si des informations sont regroupées dans un recueil, il faut contrôler si celui-ci doit être classifié ou recevoir un échelon de classification supérieur.

3 En cas de demande d'accès à des documents officiels, l'instance compétente examine, indépendamment de l'éventuelle mention de classification, s'il y a lieu d'autoriser, de limiter, de différer ou de refuser l'accès conformément aux dispositions de la loi du 17 décembre 2004 sur la transparence[8].

Art. 17 Auteurs de la classification
(art. 12 LSI)

1 Les personnes et les services suivants sont compétents pour classifier et déclassifier les informations:

a. le personnel de la Confédération et les militaires: les supports d'information qu'ils produisent ou font produire et les informations qu'ils communiquent oralement;

b. les collaborateurs d'entreprises disposant d'une déclaration de sécurité visée à l'art. 61 LSI: les supports d'information qu'ils produisent sur mandat de la Confédération;

7 RS **172.010.58**
9 RS **152.3**

c. la personne responsable de la tâche: les objets à protéger visés à l'art. 7, al. 2, let. a.

2 Les unités administratives, la Chancellerie fédérale et les départements fixent dans un catalogue de classification la manière de classifier les informations souvent traitées dans leur domaine de compétence.

3 Le service spécialisé de la Confédération pour la sécurité de l'information contrôle le catalogue de classification visé à l'al. 2 et émet si nécessaire une recommandation.

4 Il fixe, après avoir consulté la Conférence des préposés à la sécurité de l'information, dans un catalogue de classification la manière de classifier les informations souvent traitées dans l'administration fédérale et à l'armée.

Art. 18 Échelon de classification «interne»
(art. 13, al. 1, LSI)

Les informations susceptibles de nuire de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «interne»:

a. un important processus d'affaires du Conseil fédéral ou de l'administration fédérale ou un important processus de conduite de l'armée est nettement entravé;

b. l'exécution d'engagements des autorités de poursuite pénale, du Service de renseignement de la Confédération (SRC), de l'armée ou des autres organes de sécurité de la Confédération est nettement entravée;

c. des personnes subissent des lésions corporelles;

d. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont indirectement compromises;

e. la Suisse subit un désavantage sur les plans de la politique extérieure ou de l'économie;

f. les relations entre la Confédération et les cantons ou entre les cantons sont perturbées durant des mois.

Art. 19 Échelon de classification «confidentiel»
(art. 13, al. 2, LSI)

Les informations susceptibles de nuire considérablement de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «confidentiel»:

a. la capacité de décision ou la liberté d'action du Conseil fédéral, du Parlement, de plusieurs unités administratives ou de plusieurs corps de troupe de l'armée sont entravées durant plusieurs jours;

b. l'exécution conforme d'opérations des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération est compromise;

c. les moyens et les méthodes opérationnelles des services de renseignement et des autorités de poursuite pénale de la Confédération ou l'identité des sources et des personnes exposées sont divulgués;

d. la sécurité de la population est compromise durant plusieurs jours ou des personnes ou des groupes de personnes meurent;

e. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont compromises;

f. l'approvisionnement économique du pays ou l'exploitation d'infrastructures critiques sont entravés;

g. la Suisse subit un désavantage considérable sur les plans de la politique extérieure ou de l'économie ou les relations diplomatiques avec un État ou avec une organisation internationale sont interrompues;

h. la position de la Suisse est provisoirement considérablement affaiblie lors de négociations relatives à des affaires importantes de politique extérieure.

Art. 20 Échelon de classification «secret»
(art. 13, al. 3, LSI)

Les informations susceptibles de nuire gravement de la manière suivante aux intérêts définis à l'art. 1, al. 2, let. a à d, LSI si elles sont portées à la connaissance d'une personne non autorisée sont classifiées «secret»:

a. la capacité de décision et d'action du Conseil fédéral, du Parlement, de plusieurs unités administratives ou de plusieurs corps de troupes l'armée est annihilée durant des jours ou entravée sérieusement pendant des semaines;

b. l'exécution d'opérations d'importance stratégique des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération est compromise ou entravée durant des jours dans une mesure particulièrement importante;

c. les sources stratégiques, l'identité de personnes particulièrement exposées ou les moyens et les méthodes stratégiques des services de renseignement et des autorités de poursuite pénale de la Confédération sont divulgués.

d. la sécurité de la population est compromise dans une mesure particulièrement importante durant plusieurs semaines ou un grand nombre de personnes meurent;

e. la sécurité nucléaire ou la sûreté d'installations nucléaires ou de matières nucléaires sont compromises dans une mesure particulièrement importante;

f. l'approvisionnement économique du pays ou l'exploitation d'infrastructures critiques ne sont plus assurés durant plusieurs jours;

g. la Suisse subit durant des semaines des conséquences particulièrement lourdes sur les plans de la politique extérieure ou de l'économie telles que des mesures d'embargo ou des sanctions;

h. la position de la Suisse est affaiblie lors de négociations relatives à des affaires stratégiques de politique extérieure durant plusieurs années.

Art. 21 Directives relatives au traitement
(art. 6, al. 2, 84, al. 1, et 85 LSI)

1 Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent le traitement des informations classifiées et fixe les exigences de sécurité en matière d'organisation, de personnel et de construction, de même que sur le plan technique.

2 Il consulte au préalable les services suivants:

a. le service cryptographique de l'armée;

b. les services ayant la compétence d'acheter des biens cryptologiques visés à l'art. 10, al. 1, let. d, Org-OMP[9], et

c. les organes responsables de la sécurité des objets de l'administration fédérale et de l'armée.

3 Il tient compte des normes internationales.

4 La Chancellerie fédérale règle le traitement des affaires classifiées du Conseil fédéral.

5 Le traitement des informations classifiées provenant de l'étranger est régi par les prescriptions correspondant à l'échelon de classification étranger. Les prescriptions différentes figurant dans un traité international visé à l'art. 87 LSI sont réservées.

Art. 22 Mesures de sécurité liées à l'engagement
(art. 6, al. 2, et 85 LSI)

1 Si des informations classifiées sont traitées dans le cadre d'un engagement ou d'une opération et ne sont accessibles qu'à un cercle d'utilisateurs fermé clairement identifiable, les personnes suivantes peuvent, après avoir consulté le service spécialisé de la Confédération pour la sécurité de l'information, fixer des directives spécifiques à l'engagement ou à l'opération visant à simplifier le traitement:

a. le directeur de l'Office fédéral de la police;

b. le directeur du SRC;

c. le chef de l'Armée;

d. le chef du commandement des Opérations;

e. le directeur de l'Office fédéral de la douane de la sécurité des frontières.

2 Les personnes visées à l'al. 1 veillent à ce que l'on sache clairement si les prescriptions de traitement simplifié s'appliquent.

9 RS **172.056.15**

3 Les directives relatives au traitement visées à l'art. 21 s'appliquent en dehors du cercle d'utilisateurs et à la conservation des informations en vue de leur archivage.

Art. 23 Accréditation de sécurité des moyens informatiques
(art. 83, al. 1, let. e, LSI)

1 Les moyens informatiques doivent être accrédités avant leur mise en service sur le plan de la sécurité si l'une des conditions suivantes est remplie:

a. ils sont utilisés pour accomplir des tâches dépassant le cadre d'un office et impliquant le traitement d'informations classifiées «secret»;

b. ils sont utilisés pour accomplir des tâches dépassant le cadre d'une autorité ou d'un département et impliquant le traitement d'informations classifiées «confidentiel»;

c. l'accréditation de sécurité est nécessaire à la collaboration nationale et internationale.

2 L'accréditation de sécurité atteste que le moyen informatique remplit les exigences minimales de sécurité correspondant à l'échelon de classification concerné et que les risques résiduels sont supportables conformément à l'état des connaissances techniques.

3 Elle est répétée en cas de changements importants concernant les risques ou le moyen informatique.

4 Si l'accréditation de sécurité ne peut pas être octroyée parce que le moyen informatique ne remplit pas les exigences minimales de sécurité, le Conseil fédéral prend la décision concernant les risques résiduels.

5 Le service spécialisé de la Confédération pour la sécurité de l'information assume les tâches suivantes:

a. il octroie l'accréditation de sécurité après avoir entendu le service cryptographique de l'armée et les services visés à l'art. 10, al. 1, let. d, Org-OMP[10];

b. il peut déléguer au Groupement Défense la compétence d'accréditer uniquement les systèmes militaires.

6 Le [département compétent] fixe la procédure relative à l'accréditation de sécurité en tenant compte des normes internationales en la matière.

Art. 24 Protection en cas de menace des informations classifiées
(art. 10, al. 1, et 11, al. 1, LSI)

1 Celui qui constate que des informations classifiées ont été compromises, ont disparu ou qu'il en a été fait un usage abusif ou que des informations n'ont par erreur pas été classifiées ou qu'elles ont été classifiées de manière erronée prend les mesures de protection nécessaires.

10 RS **172.056.15**

2 Il en informe immédiatement l'auteur de la classification et les organes de sécurité concernés.

Art. 25 Contrôle du besoin de protection et personnes autorisées
(art. 11, al. 2, LSI)

Les auteurs de la classification contrôlent le besoin de protection de leurs informations classifiées et le cercle des personnes autorisées au moins tous les cinq ans et l'examine systématiquement lorsque les informations sont proposées aux Archives fédérales.

Art. 26 Archivage
(art. 12, al. 3, LSI)

1 L'archivage des informations classifiées est régi par les prescriptions de la législation fédérale sur l'archivage.

2 Les Archives fédérales veillent à ce que la sécurité de l'information visée dans la présente ordonnance soit garantie.

3 Il n'est plus nécessaire de classifier les archives une fois que le délai de protection est échu. Une prolongation du délai de protection est régie par l'art. 14 de l'ordonnance du 8 septembre 1999 sur l'archivage[11].

Section 5 Sécurité des moyens informatiques

Art. 27 Procédure de sécurité
(art. 16 LSI)

1 Les unités administratives doivent pouvoir démontrer le besoin de protection de leurs objets à protéger et leur importance pour la gestion de la continuité relative à l'exploitation.

2 Elles mettent en œuvre les consignes minimales des différentes catégories de sécurité et vérifient si des mesures de sécurité supplémentaire sont nécessaires.

3 Elles démontrent les risques qui ne peuvent pas être réduits de manière suffisante (risques résiduels).

4 Les responsables de la sécurité visés à l'art. 36 décident si les risques résiduels sont jugés acceptables. Ils peuvent déléguer cette décision à d'autres membres de la direction.

5 La procédure de sécurité est répétée en cas de changements importants concernant la menace, la technologie, les tâches et la situation de l'organisation.

6 Les unités administratives contrôlent chaque année si un changement important au sens de l'al. 5 a eu lieu.

11 RS **152.11**

Art. 28 Attribution des catégories de sécurité «protection élevée» et «protection très élevée»
(art. 17 LSI)

[1] La catégorie de sécurité «protection élevée» est attribuée à un moyen informatique lorsqu'une violation de la sécurité de l'information est susceptible de provoquer un préjudice considérable selon l'art. 19 ou un préjudice de 50 millions à 500 millions de francs.

[2] La catégorie de sécurité «protection très élevée» est attribuée à un moyen informatique lorsqu'une violation de la sécurité de l'information est susceptible de provoquer un préjudice considérable selon l'art. 20 ou un préjudice d'au moins 500 millions de francs.

Art. 29 Mesures de sécurité
(art. 6, al. 3, 18 et 85 LSI)

[1] Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences minimales auxquelles doivent répondre les catégories de sécurité visées à l'art. 17 LSI.

[2] Il tient compte des exigences concernant la sécurité des données sensibles au sens de la législation sur la protection des données et celle des autres informations que la Confédération doit protéger en vertu de ses obligations légales ou contractuelles.

[3] L'efficacité des mesures de sécurité des moyens informatiques suivants doit être contrôlée au moins tous les cinq ans avant leur mise en exploitation, en cas de changements importants durant l'exploitation:

a. les moyens informatiques de la catégorie de sécurité «protection élevée» qui sont utilisés pour accomplir des tâches dépassant le cadre d'une autorité ou d'un département;

b. les moyens informatiques de la catégorie de sécurité «protection très élevée».

[4] Les départements et la Chancellerie fédérale intègrent leurs moyens informatiques de la catégorie de sécurité «protection très élevée» dans leur gestion de la continuité.

Art. 30 Sécurité de l'exploitation
(art. 19 LSI)

[1] Les unités administratives veillent à ce que les responsabilités en matière de sécurité informatique soient définies au niveau opérationnel dans les accords de projets et les conventions de prestations conclus avec les fournisseurs internes de prestations.

[2] Les fournisseurs internes de prestations mettent à la disposition des unités administratives, de la Chancellerie fédérale, des départements et du service spécialisé de la Confédération pour la sécurité de l'information les informations dont ils ont besoin pour assurer la sécurité de l'information.

3 Ils garantissent qu'ils disposent des capacités et compétences personnelles et financières nécessaires pour déceler à temps, procéder à l'analyse technique et à la maîtrise des incidents de sécurité et au traitement des failles de sécurité qui les concernent ou, dans le cadre des conventions visées à l'al. 2, qui concernent leurs bénéficiaires de prestations.

4 Ils procèdent à une surveillance pour s'assurer que l'infrastructure informatique soit utilisée de manière sûre et recherchent régulièrement les menaces et les vulnérabilités. Ils peuvent charger des tiers d'effectuer ces recherches.

5 Le traitements des données personnelles dans le cadre de la surveillance et des recherches visées à l'al. 4 est régie par l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération[12].

Section 6 Mesures relatives aux personnes et protection physique

Art. 31 Vérification de l'identité des personnes et des machines
(art. 20 et 85 LSI)

1 Après avoir consulté le délégué TNI, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences techniques minimales auxquelles doit satisfaire la vérification, sous l'angle du risque, de l'identité des personnes et des machines qui ont besoin d'accéder à des informations, à des moyens informatiques, à des locaux et à d'autres infrastructures de la Confédération.

2 Le traitement des données personnelles effectué lors de la vérification de l'identité dans les systèmes de gestion des données d'identification visés à l'art. 24 LSI est régi par les dispositions de l'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[13].

Art. 32 Sécurité relative aux personnes
(art. 6, al. 2 et 3, 8 et 20, al. 1, let. a et c, LSI)

1 Les unités administratives garantissent que les collaborateurs faisant l'objet d'un contrôle de sécurité relatif aux personnes visé dans l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[14] soient sensibilisés chaque année à l'activité sensible déterminante et aux risques qui y sont liés.

2 Les collaborateurs visés à l'al. 1 sont tenus d'annoncer à leur employeur et les circonstances privées professionnelles les empêchant d'accomplir leur activité sensible dans le respect des prescriptions.

12 RS **172.010.442**
13 RS **172.010.59**
14 RS ...

Art. 33 Soupçons de comportement répréhensible
(art. 7, al. 2, let. c, LSI)

[1] Lorsque la violation des prescriptions en matière de sécurité de l'information paraît constituer en même temps une infraction, les départements transmettent le dossier de l'enquête et les procès-verbaux d'interrogatoire au Ministère public de la Confédération ou à l'auditeur en chef de l'Armée suisse.

[2] Ils saisissent les objets qui sont à même de servir de moyens de preuve dans une procédure.

Art. 34 Mesures physiques de protection
(art. 22 et 85 LSI)

[1] Après avoir consulté les organes responsables de la sécurité des objets de l'administration fédérale et de l'armée, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les mesures minimales requises par la protection physique des informations et des moyens informatiques.

[2] Il tient compte à cet égard:

a. du cycle de vie entier des informations et des moyens informatiques;

b. des exigences spécifiques à la place de travail, et

c. des stratégies et des concepts d'hébergement de l'administration fédérale et de l'armée.

Art. 35 Zones de sécurité
(art. 23 et 85 LSI)

[1] Les unités administratives peuvent établir les zones de sécurité suivantes:

a. zone de sécurité 1: les locaux et les espaces dans lesquels des informations classifiées «confidentiel» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection élevée» sont exploités;

b. zone de sécurité 2: les locaux et les espaces dans lesquels des informations classifiées «secret» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection très élevée» sont exploités.

[2] Les locaux et les espaces visés à l'al. 1 ne sont considérés comme des «zones de sécurité» que si l'organe responsable de la sécurité des objets de l'administration fédérale et de l'armée confirme avant leur mise en exploitation et ensuite au moins tous les cinq ans que les exigences en matière de sécurité sont remplies.

[3] Après avoir consulté les organes responsables de la sécurité des objets de l'administration fédérale et de l'armée, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à tous les services visés à l'art. 2, al. 1 à 3 qui concernent les exigences en matière de sécurité auxquelles doivent répondre les zones de protection et leurs installations.

Section 7 Organisation de sécurité

Art. 36 Responsables de la sécurité de la Chancellerie fédérale et des unités administratives

(art. 7, al. 1, LSI)

1 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités de l'administration fédérale centrale et décentralisée sont responsables de la sécurité dans leur domaine de compétence.

2 Ils peuvent déléguer la responsabilité en matière de sécurité à un membre de la direction s'il dispose des pouvoirs nécessaires pour prendre des mesures, les contrôler et les corriger.

3 Les responsables de la sécurité de la Chancellerie fédérale et des unités administratives assument notamment les tâches suivantes:

a. ils assurent la mise en place, l'exploitation, le contrôle et l'amélioration continue du SMSI dans leur domaine de compétence et émettent les directives nécessaires;

b. ils prennent toutes les décisions importantes qui concernent la sécurité de l'information dans leur domaine de compétence, notamment concernant l'organisation, les processus, l'acceptation des risques et les objectifs de sécurité;

c. ils décident des mesures nécessaires, notamment concernant les mesures de formation et de sensibilisation;

d. ils approuvent la planification annuelle de contrôle et d'audit et mettent les ressources nécessaires à disposition.

4 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités de l'administration fédérale centrale et décentralisée confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 37 et veillent à:

a. ce qu'ils disposent des compétences et des ressources appropriées, et

b. à ce qu'ils ne se voient confier aucune tâche susceptible d'entrer en conflit avec les tâches visées à l'art. 37.

Art. 37 Préposés à la sécurité de l'information des unités administratives

(art. 7, al. 1, LSI)

1 Les unités administratives désignent un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

2 Les préposés à la sécurité de l'information accomplissent notamment les tâches suivantes:

a. ils gèrent le SMSI de l'unité administrative sur mandat du responsable de la sécurité;

b. ils élaborent les bases de décision nécessaires à l'intention du responsable de la sécurité et lui demandent de prendre des mesures;

c. ils sont le point de contact central des unités administratives pour les questions de sécurité de l'information et conseillent les personnes et les services responsables et les aident à accomplir leurs tâches et devoirs dans le domaine de la sécurité de l'information;

d. ils veillent à la mise en œuvre des directives en matière de sécurité de l'information et à l'application de la procédure de sécurité visée à l'art. 27;

e. ils exercent la surveillance de la liste des bases légales, de l'inventaire des objets à protéger et de la liste des autorisations exceptionnelles;

f. ils exercent la surveillance de la planification de la formation et de la sensibilisation visées à l'art. 11 et demandent aux responsables de la sécurité de procéder à des mesures de formation et de sensibilisation supplémentaire;

g. ils demandent l'ouverture de la procédure de sécurité relative aux entreprises visée à l'art. 4 de l'ordonnance sur du … sur la procédure de sécurité relative aux entreprises[15];

h. ils coordonnent l'annonce et la maîtrise des incidents de sécurité et le traitement des failles de sécurité dans les unités administratives et auprès des tiers mandatés;

i. ils établissent la planification annuelle de contrôle et d'audit et la soumettent au responsable de la sécurité pour approbation;

j. sur mandat du responsable de la sécurité, ils peuvent contrôler ou faire contrôler l'utilisation des informations aux postes de travail ouverts, partagés ou non verrouillables et dans les moyens informatiques des unités administratives;

k. ils rendent compte chaque semestre au responsable de la sécurité de la situation en matière de sécurité de l'information.

Art. 38 Sécurité de l'information dans les services standard
(art. 7, al. 1, LSI)

1 Le délégué TNI est chargé de garantir la sécurité de l'information dans les services standard visés à l'art. 17, al. 1, let. e, OTNI[16].

2 Il désigne un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

3 Le préposé à la sécurité de l'information visé à l'al. 2 assume les tâches des services standard visées à l'art. 37, al. 2 et informe l'administration fédérale et l'armée des risques.

Art. 39 Responsabilité des départements en matière de sécurité
(art. 7, al. 1, et 81 LSI)

1 Les départements sont responsables du pilotage et de la surveillance de la sécurité de la formation dans leur domaine de compétence.

15 RS …
16 RS **172.010.58**

2 Ils accomplissent à cet égard notamment les tâches suivantes:

a. ils déterminent la politique en matière de sécurité de l'information et l'organisation de sécurité du département, y compris la conduite technique des préposés à la sécurité de l'information des unités administratives;

b. ils édictent les directives nécessaires et en surveillent la mise en œuvre;

c. ils surveillent le SMSI des unités administratives et collectent les indicateurs nécessaires;

d. ils fixent des objectifs annuels de sécurité pour les unités administratives et vérifient qu'elles les ont atteints;

e. ils veillent au contrôle de la sécurité de l'information en fonction du risque;

f. ils confient des mandats à leurs préposés à la sécurité de l'information visés à l'art. 40 et veillent à:

1. ce qu'ils disposent des compétences et des ressources appropriées,

2. ce qu'ils ne se voient confier aucune tâche susceptible d'entrer en conflit avec les tâches visées à l'art. 40.

3 Ils peuvent assumer les tâches et les compétences que la présente ordonnance attribue aux unités administratives.

4 Ils peuvent fixer pour leur domaine de compétence des exigences en matière de sécurité qui dépassent les exigences minimales du service spécialisé de la Confédération pour la sécurité de l'information ou de l'unité administrative.

5 Pour autant que les chefs de département n'en décident pas autrement, la sécurité dans le département relève de la responsabilité du secrétaire général qui leur est subordonné.

Art. 40 Préposés à la sécurité de l'information des départements
(art. 7, al. 1, et 81 LSI)

Les préposés à la sécurité de l'information des départements accomplissent les taches suivantes en plus de celles qui sont visées à l'art. 81, al. 2, LSI:

a. ils assurent la coordination interdépartementale de la sécurité de l'information;

b. ils élaborent les bases de décision nécessaires à l'intention du responsable de la sécurité et lui demandent de prendre des mesures;

c. ils coordonnent l'annonce et la maîtrise des incidents de sécurité et le traitement des failles de sécurité impliquant plusieurs unités administratives;

d. ils représentent le département au sein d'organes spécialisés;

e. ils sont consultés pour le choix des préposés à la sécurité de l'information visés à l'art. 37;

f. ils vérifient périodiquement et en cas de changement ou de départ d'un membre du Conseil fédéral ou du chancelier de la Confédération que les supports d'informations classifiés «secret» soient au complet;

g. ils autorisent l'ouverture de contrôles de sécurité relatifs aux personnes pour les tiers (art. 8, al. 2, let. b, OCSP)[17];

h. ils rendent compte chaque année au responsable de la sécurité du département de la situation en matière de sécurité de l'information dans le département.

Art. 41 Service spécialisé de la Confédération pour la sécurité de l'information
(art. 7, al. 1, et 83 LSI)

1 Le service spécialisé de la Confédération pour la sécurité de l'information accomplit les tâches suivantes pour l'administration fédérale et l'armée:

a. il élabore des stratégies concernant les thèmes dans le domaine de la sécurité;

b. il peut, en cas de projets dans le domaine de la sécurité, demander des informations, prendre position et demander des modifications;

c. il participe à la formation de l'organisation de sécurité;

d. il prépare des modèles et des aides.

2 Il peut rechercher les menaces techniques et les vulnérabilités dans l'infrastructure informatique de l'administration fédérale et de l'armée ou sur Internet afin d'évaluer et d'améliorer la situation en matière de sécurité de l'information; il peut en charger d'autres services de l'administration fédérale ou de l'armée ou des tiers.

3 Il consulte la Conférence des préposés à la sécurité de l'information lors de l'accomplissement des tâches visées à l'al. 1 et à l'art. 83, al. 1, LSI.

4 Il représente la Suisse dans les relations internationales en tant qu'autorité nationale de sécurité et assume les tâches suivantes dans ce contexte:

a. il élabore les traités internationaux visés à l'art. 87 LSI et en contrôle la mise en œuvre;

b. il garantit que les incidents de sécurité qui concernent des informations classifiées d'États partenaires soient clarifiés de manière appropriée;

c. il peut exécuter les contrôles prévus dans les traités internationaux ou les faire exécuter;

d. il représente la Suisse dans des organismes internationaux;

e. il autorise l'arrivée d'étrangers se rendant en Suisse pour participer à des projets classifiés et le détachement de personnes se rendant à l'étranger pour participer à des projets classifiés;

f. il délivre les certificats internationaux de sécurité visés à l'art. 30 OCSP[18].

5 Le service spécialisé de la Confédération pour la sécurité de l'information est rattaché au *[département compétent]*.

17 RS ...
18 RS ...

Section 8 Coûts et évaluation

Art. 42 Coûts

1 Les coûts décentralisés de la sécurité de l'information font partie des coûts de projet et d'exploitation.

2 Les unités administratives garantissent que les coûts sont suffisamment pris en compte et démontrés lors de la planification.

3 Le service spécialisé de la Confédération pour la sécurité de l'information perçoit un émolument 100 francs pour établir et envoyer les certificats internationaux de sécurité visés à art. 30 OCSP[19] des personnes qui n'accomplissent aucune activité sensible de la Confédération.

Art. 43 Évaluation

(art. 88 LSI)

Six ans après l'entrée en vigueur de la présente ordonnance et ensuite tous les dix ans, le service spécialisé de la Confédération pour la sécurité de l'information demande au Contrôle fédéral des finances d'évaluer la législation sur la sécurité de l'information à la Confédération.

Section 9 Traitement des informations et des données personnelles

Art. 44 Généralités

1 Les organisations visées à l'art. 2, al. 1 à 3, et les organes de sécurité de la Confédération peuvent traiter les informations utiles à la garantie de la sécurité de l'information, y compris les données personnelles.

2 Ils peuvent échanger les informations, y compris les données personnelles, visées à l'al. 1 entre eux et avec les organisations nationales, internationales et étrangères du droit public et privé, dans la mesure où:

a. aucune obligation de maintien du secret légale ou contractuelle n'est violée, et

b. les prescriptions de la législation fédérale en matière de protection des données sont respectées.

3 Pour autant que cela soit nécessaire pour maîtriser un incident de sécurité ou traiter une faille de sécurité, elles peuvent également traiter et échanger des données sensibles relatives à l'identité et aux actes des personnes ayant participé à l'incident ou qui sont concernées par l'incident ou qui pourraient y avoir participé ou être concernées.

19 RS **126.xxx**

Art. 45 Application SMSI

[1] Les organisations visées à l'art. 2, al. 1 à 3 peuvent exploiter un système d'information (application SMSI) pour gérer la sécurité de l'information.

[2] Elles peuvent traiter dans l'application SMSI toutes les informations liées à la gestion de la sécurité de l'information en vertu de la présente ordonnance et les données sensibles visées à l'art. 4, al. 3.

[3] Elles peuvent relier leurs applications SMSI et échanger des informations pertinentes pour la sécurité de l'information par des interfaces automatisées.

Art. 46 Services électroniques de formulaire

[1] Le service spécialisé de la Confédération pour la sécurité de l'information peut gérer les services électroniques de formulaire et les relier à leur application SMSI dans les buts suivants:

a. gérer les voyages visés à l'art. 41, al. 4, let. e;

b. établir et envoyer les certificats internationaux de sécurité visés à l'art. 30 OCSP[20];

c. établir et envoyer et les certificats internationaux de sécurité visés à l'art. 66 LSI.

[2] Les données personnelles figurant dans l'annexe 2 peuvent être traitées à l'aide des services de formulaires visés à l'al. 1. Elles peuvent être conservées pendant dix ans au plus.

[3] Les organisations visées à l'art. 2, al. 1 à 3 peuvent exploiter les services électroniques de formulaire pour annoncer des incidents et des failles de sécurité et les relier à leur application SMSI.

[4] À l'aide des services de formulaires visés à l'al. 3, elles peuvent traiter les données personnelles, y compris les données sensibles, visées à l'art. 44, al. 3, qui sont nécessaires à la maîtrise des incidents de sécurité et au traitement des failles de sécurité.

[5] Les données visées à l'al. 4 doivent être effacées du service de formulaire immédiatement après l'envoi de l'annonce. Elles peuvent provisoirement être enregistrées avant l'envoi durant 24 heures au plus.

Section 10 Dispositions finales

Art. 47 Abrogation et modification d'autres actes

[1] Sont abrogées:

a. l'ordonnance du 27 mai 2020 sur les cyberrisques[21];

20 RS **128.xxx**
21 [RO **2020** 2107, **2020** 5871, **2021** 132]

b. l'ordonnance du 4 juillet 2007 concernant la protection des informations[22].

2 La modification d'autres actes est réglée dans l'annexe 3.

Art. 48 Dispositions transitoires

1 Les directives en matière de sécurité informatique émises par le Centre national pour la cybersécurité et les exceptions qu'il a autorisées avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant six ans au plus après l'entrée en vigueur de la présente ordonnance.

2 Le service spécialisé de la Confédération pour la sécurité de l'information prend les décisions concernant les changements des consignes et des exceptions autorisées.

3 Les directives en matière de sécurité informatique émises par la Conférence des secrétaires généraux ou l'Organe de coordination pour la protection des informations au sein de la Confédération avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant cinq ans au plus après l'entrée en vigueur de la présente ordonnance.

4 Les unités administratives et la Chancellerie fédérale mettent en place leur SMSI au plus tard trois ans après l'entrée en vigueur de la présente ordonnance.

5 L'accréditation de sécurité visée à l'art. 23 n'est pas effectuée pour les moyens informatiques qui:

a. sont en service avant l'entrée en vigueur de la présente ordonnance;

b. sont en développement au moment de l'entrée en vigueur de la présente ordonnance, dans la mesure où elle entraînerait une charge de travail disproportionnée.

Art. 49 Entrée en vigueur

La présente ordonnance entre en vigueur le … 2023.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, …
Le chancelier de la Confédération, Walter Thurnherr

22 [RO **2007** 3401, **2010** 3207, **2013** 1341, **2014** 3543, **2016** 1785, **2017** 7391, **2020** 6011]

Annexe 1
(art. 2, al. 2 et 3)

Unités de l'administration fédérale décentralisée auxquelles s'applique l'ordonnance sur la sécurité de l'information ou certaines de ses parties

1. Unités administratives qui ont accès aux moyens informatiques des fournisseurs internes de prestations informatiques visés à l'art. 9 OTNI[23] relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28 (cf. art. 2, al. 2, let. a):

a. …

b. …

c. …

2. Unités administratives qui utilisent les moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée» visées à l'art. 28 (cf. art. 2, al. 2, let. b)

a. …

b. …

c. …

3. Unités administratives qui ne sont pas concernées par les let. a et b, mais qui traitent des informations classifiées de la Confédération (cf. art. 2, al. 2, let. c):

a. …

b. …

c. …

4. Autres unités administratives (cf. art. 2, al. 3):

a. …

b. …

c. …

23 RS **172.010.58**

Annexe 2
(art. 46, al. 2)

Traitement des données dans les services de formulaire visés à l'art. 46

Les données personnelles suivantes peuvent être traitées dans les services de formulaire visés à l'art. 46:

1. Service de formulaire visé à l'art. 46, al. 1, let. a, OSI
   a. Données relatives à la personne:
      1. Prénoms et noms*
      2. Numéro AVS
      3. Civilité, titre et rang*
      4. Date de naissance*
      5. Lieu d'origine et lieu de naissance*
      6. Nationalité/s*
      7. Numéro de carte d'identité et de passeport, lieu d'établissement et validité*
   b. Données concernant les fonctions professionnelles ou militaires de la personne:
      1. Fonction au sein de l'organisation ou de l'armée*
      2. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
      3. Décision positive concernant le contrôle de sécurité relatif aux personnes, degré de contrôle et durée de validité*
   c. Données relatives à l'organisation requérante:
      1. Nom, adresse et coordonnées de l'organisation*
      2. Prénoms et noms de la personne de référence
      3. Fonction de la personne de référence au sein de l'organisation ou de l'armée
      4. Adresse professionnelle, adresse e-mail, numéros de téléphone et coordonnés électroniques de la personne de référence
   d. Données concernant la visite:
      1. Nom, adresse, adresse e-mail et coordonnées de l'organisation étrangère*
      2. Motif de la visite*
      3. Catégorie de sécurité de la visite*
      4. Durée de la visite*
      5. Points du passage de la frontière*
      6. Moyens de transport*
      7. Matériel transporté, y c. armes, munitions, explosifs, véhicules et autres équipements*

Les données munies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

2. Service de formulaire visé à l'art. 46, al. 1, let. b, OSI

   a. Données relatives à la personne:
      1. Prénoms et noms
      2. Numéro AVS
      3. Civilité, titre et rang
      4. Date de naissance
      5. Lieu d'origine et lieu de naissance
      6. Nationalités
      7. Numéro de carte d'identité et de passeport, lieu d'établissement et validité
   b. Données concernant les fonctions professionnelles ou militaires de la personne:
      1. Fonction au sein de l'organisation ou de l'armée
      2. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
      3. Décision positive concernant le contrôle de sécurité relatif aux personnes, degré de contrôle et durée de validité
   c. Données relatives à l'organisation requérante:
      1. Nom, adresse, adresse e-mail et coordonnées de l'organisation
      2. Prénoms et nom de la personne de référence au sein de l'organisation ou de l'armée
      3. Fonction de la personne de référence au sein de l'organisation ou de l'armée
      4. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques, de la personne de référence
      5. Motif de l'établissement du certificat

3. Service de formulaire visé à l'art. 46, al. 1, let. c, OSI

   a. Données relatives à l'entreprise:
      1. Nom complet*
      2. Forme juridique*
      3. Numéro d'identification des entreprises
      4. Adresse, adresse e-mail et autres coordonnées, en particulier électroniques*
      5. Siège*
      6. Prénoms et noms de la personne de référence*
      7. Fonction de la personne de référence au sein de l'entreprise
      8. Adresse professionnelle, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques, de la personne de référence

b. Données concernant le certificat de sécurité:
   1. Date d'établissement et durée de validité*
   2. Champ d'application et charges*
   3. Catégorie de classification ou de sécurité la plus élevée autorisée*

Les données munies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

4. Service de formulaire visé à l'art. 46, al. 3 à 5, OSI

a. Données concernant l'auteur de l'annonce:
   1. Prénoms et noms
   2. Adresse, adresse e-mail, numéros de téléphone et autres coordonnées, en particulier électroniques
   3. Fonction au sein de l'organisation ou de l'armée
b. Données relatives au dommage et au calcul du dommage
c. Photographies, enregistrements sonores ou vidéos de l'incident ou de la faille de sécurité
d. Documents ou fichiers portant sur l'incident ou la faille de sécurité
e. Données relatives aux éventuelles personnes impliquées dans l'incident
f. Premières analyses de spécialistes, y compris premières mesures prises

Annexe 3
(art. 47, al. 2)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale[24]

Art. 2, al. 2, phrase introductive

2 Peuvent, sous réserve d'autres dispositions d'organisation contenues dans le droit fédéral, se soumettre par un accord avec le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF) à la présente ordonnance, à l'ordonnance du […] sur la sécurité de l'information[25] et à l'ordonnance GEVER du 3 avril 2019[26], y compris aux directives fondées sur celles-ci:

2. Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports[27]

Art. 3, al. 2

2 Il édicte des prescriptions en vue de garantir l'équipement de l'armée.

Art. 6, let. b

Abrogée

3. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[28]

Art. 4, let. c

Les services suivants peuvent établir formellement des relations militaires internationales dans leur domaine d'activités sans autorisation du Protocole militaire:

c. le service spécialisé de la Confédération pour la sécurité de l'information;

24 RS **172.010.58**
25 RS …
26 RS **172.010.441**
27 RS **172.214.1**
28 RS **510.215**

Art. 5, al. 1

[1] La remise d'informations classifiées à des personnes ou à des organes étrangers et l'accès à des informations militaires classifiées, à du matériel classifié ou à des installations militaires en Suisse par des personnes étrangères sont soumis aux dispositions régissant la protection de l'information, notamment:

a. le traité international applicable dans le cas concret visé à l'art. 87 de la loi du 20 décembre 2020 sur la sécurité de l'information[29];

b. l'ordonnance du … sur les contrôles de sécurité relatif aux personnes[30];

c. l'ordonnance du … sur la sécurité de l'information[31];

d. l'ordonnance du … sur la procédure de sécurité relative aux entreprises[32].

29 RS **128**
30 RS **...**
31 RS **...**
32 RS **...**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Modification du … Projet du 25 juillet 2022

Le Conseil fédéral suisse
arrête:

I

L'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération[1] est modifiée comme suit:

Préambule

vu les art. 26 et 84, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[2],
vu l'art. 27, al. 5 et 6, de la loi du 24 mars 2000 sur le personnel de la Confédération[3],
vu l'art. 186 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[4],

Art. 2 Champ d'application

La présente ordonnance s'applique aux:

a. unités de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[5];

1 RS **172.010.59**
2 RS **126**
3 RS **172.220.1**
4 RS **510.91**
5 RS **172.010.1**

b. unités de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA, dans la mesure où elles ont accès aux moyens informatiques de l'administration fédérale centrale.

Art. 3, al. 1

1 Un système IAM sert à gérer conjointement des données sur l'identité et les autorisations de personnes, de machines et de systèmes pour les mettre à la disposition des systèmes en aval et d'autres systèmes IAM.

Art. 5 Systèmes IAM

1 Les organes de la Confédération responsables des systèmes IAM sont:

a. le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF), pour tous les systèmes IAM proposés comme services standard et tous les systèmes IAM relevant explicitement du secteur TNI de la ChF;

b. la Direction des ressources du Département fédéral des affaires étrangères (DFAE), pour le système IAM exploité par l'unité Informatique DFAE;

c. le secteur TNI de la ChF, pour le système IAM des processus d'assistance, y compris le raccordement au *cloud*;

d. le Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports (DDPS), pour le système IAM exploité par la Base d'aide au commandement (BAC) du DDPS;

e. le Secrétariat général du Département fédéral de l'économie, de la formation et de la recherche (DEFR), pour le système IAM exploité par le Centre de services informatiques du DEFR (ISCeco);

f. l'Office fédéral des routes, pour son système IAM de gestion des équipements d'exploitation et de sécurité des routes nationales.

2 Les organes de la Confédération visés à l'al. 1 veillent à ce que la licéité du traitement des données personnelles figurant dans les systèmes IAM dont ils sont responsables soit vérifiée au moins tous les quatre ans par un organe externe.

3 Si la présente ordonnance s'applique aux autorités visées à l'art. 2, al. 1, let. a et c à e, LSI conformément à l'art. 84, al. 3, LSI, celles-ci déterminent elles-mêmes quels organes de la Confédération de leur domaine sont responsables.

4 Le service technique compétent demeure responsable du système en aval, et en particulier de l'accès à celui-ci.

Art. 11, al. 2 et 3

2 Aucun profilage ne peut être effectué dans ces systèmes.

3 En l'absence d'une base légale particulière en la matière, aucune donnée sensible ne peut être traitée dans ces systèmes à l'exception des données biométriques visées à l'art. 20, al. 2, LSI.

Art. 13, al. 4

4 Les données peuvent être transmises de manière automatisée à d'autres systèmes d'information internes à l'administration fédérale, dans lesquels elles sont reprises et harmonisées, à condition que le système concerné:

a. dispose d'une base légale prévoyant le traitement des données à transmettre et d'un règlement de traitement au sens de l'art. 21 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), et

Art. 14, al. 2

2 Les dispositions de l'art. 20, al. 2, LSI relatives à la destruction des données biométriques sont réservées.

Titre précédant l'art. 18

Section 6 Mesures de protection des systèmes IAM et des services d'annuaires

Art. 18, al. 1 et 2

1 Les exploitants internes et externes d'éléments d'un système IAM ou d'un service d'annuaires doivent avoir des instructions écrites sur la sécurité de l'information et la gestion des risques. En particulier, chaque organe responsable d'un système ou d'un service d'annuaires au sens de la présente ordonnance établit un règlement de traitement conformément à l'art. 21 OLPD.

2 Les systèmes IAM et les services d'annuaires qui ne sont pas gérés par des organes au sens de l'art. 2 ou sur mandat de ces derniers peuvent être raccordés à des systèmes IAM ou à des services d'annuaires internes à l'administration fédérale uniquement s'ils respectent les exigences minimales prédéfinies concernant la sécurité de l'information.

Art. 20 Système global IAM

Les systèmes IAM de l'administration fédérale peuvent être reliés entre eux et aux systèmes IAM externes visés à l'art. 21 pour former un système global.

Art. 21 Conditions pour le raccordement de systèmes IAM externes

Les systèmes IAM externes ci-après peuvent être raccordés aux systèmes IAM de la Confédération afin que les personnes gérées dans ces systèmes externes puissent accéder aux ressources de celle-ci, pour autant que les conditions et les procédures

énoncées aux art. 22 et 23 soient respectées et que les exploitants s'engagent à respecter la présente ordonnance et les prescriptions qui en découlent:

a. systèmes IAM des Services du Parlement;

b. systèmes IAM de l'armée;

c. systèmes IAM comprenant des collaborateurs cantonaux et communaux au sens de l'art. 9, let. a;

d. systèmes IAM reconnus par le secteur TNI de la ChF qui sont destinés à la fédération d'identités dans le cadre de la cyberadministration;

e. fédérations d'identités ou systèmes IAM étrangers dont le raccordement mutuel est prévu dans un traité international, ou

f. registres des attributs qui mettent à disposition des données relatives à des fonctions professionnelles selon l'annexe, let. b.

II

L'annexe est remplacée par la version ci-jointe.

III

La présente ordonnance entre en vigueur le … 2023.

…

Au nom du Conseil fédéral suisse:

Le président de la Confédération, …
Le chancelier de la Confédération, Walter Thurnherr

Annexe
(art. 11 et 13, al. 1 et 2)

Catégories de données

Remarque préliminaire: pour la signification des astérisques (*), voir l'art. 11, al. 2.

	Services d'annuaires et systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
a. Données relatives à la personne		
1. Nom*	x	x
2. Prénom*	x	x
3. Date de naissance	x	x
4. Sexe	x	x
5. Civilité*	x	x
6. Titre*	x	x
7. Initiales*	x	x
8. Identificateurs personnels locaux	x	x
9. Profession*	x	x
10. Langue de correspondance*	x	x
11. Caractéristiques biométriques personnelles particulières, en particulier scan de l'iris, rétine, scan des veines, empreinte digitale, empreinte palmaire, caractéristiques de la forme du visage et profil de la voix	x	
12. Numéro AVS	x	x
b. Données relatives au rapport avec l'employeur/le mandant		
1. Rapports de travail (interne/externe)*	x	
2. Informations relatives à l'unité d'organisation et aux postes de travail*	x	x
3. Futur rattachement à une unité d'organisation	x	
4. Catégorie de personnel	x	
5. Numéro personnel (y c. cantonal)	x	
6. Fonction*	x	
7. Poste*	x	
8. Identification du système d'information du personnel (source)	x	
9. Date d'entrée et date de départ	x	

	Services d'annuaires et systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
10. Numéro de pièce d'identité et/ou de badge	x	x
c. Données de contact		
1. Adresse du lieu de travail et adresse postale professionnelle*	x	x
2. Numéro du bureau*	x	
3. Composantes de l'adresse professionnelle* telles qu'adresse électronique*, numéro de téléphone*, numéro de fax*, adresse VoIP*	x	x
4. Composantes de l'adresse externe* (pour les collaborateurs et les mandataires*) ou de l'adresse privée	x	x
d. Données concernant les fonctions professionnelles		
1. Indications issues des registres professionnels officiels (médecin, personne habilitée à dresser des actes authentiques, avocat, etc.)	x	x
2. Fonction selon le registre du commerce et d'autres registres des représentations	x	x
e. Données techniques		
1. Appareils, raccordements, systèmes, applications, etc.	x	x
2. Composantes de l'adresse, numéros d'identification, etc.	x	
3. Langue du système des appareils, des raccordements, etc.	x	x
4. Clés publiques des certificats numériques*	x	x
5. Groupes d'autorisations	x	x
6. Noms pour la connexion aux systèmes informatiques	x	x
7. Mots de passe	x	x
8. Dernière ouverture de session	x	x
9. Échecs lors d'ouvertures de session	x	x
10. Statut (actif/passif)	x	x
f. Données relatives au contrôle de sécurité relatif aux personnes, si celui-ci a abouti à une déclaration de sécurité sans réserve ou si l'autorité décisionnelle a rendu une décision positive		
1. Degré de contrôle	x	
2. Durée de validité de la déclaration de sécurité	x	

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

du … Avant-projet du 25 juillet 2022

Le Conseil fédéral suisse,

vu les art. 48, 83, al. 3, 84, al. 1, et 86, al. 4, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],
vu l'art. 41*b*, al. 5, de la loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI)[2],
vu l'art. 119 de la loi du 26 juin 1998 sur l'asile (LAsi)[3],
vu l'art. 6*a*, al. 5, de la loi du 22 juin 2001 sur les documents d'identité (LDI)[4],
vu l'art. 37, al. 1, de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[5],
vu les art. 14, al. 2, et 150, al. 1, de la loi du 3 février 1995 sur l'armée (LAAM)[6],
vu l'art. 24, al. 4, de la loi du 21 mars 2003 sur l'énergie nucléaire (LENu)[7],
vu l'art. 20*a*, al. 2, de la loi du 23 mars 2007 sur l'approvisionnement en électricité (LApEl)[8],

arrête:

Section 1 Dispositions générales

Art. 1 Objet

(art. 2, al. 3 et 4, 28, 30, 31 et 48 LSI)

1 La présente ordonnance régit les procédures suivantes:

a. le contrôle de sécurité relatif aux personnes (CSP) selon la LSI;

b. les contrôles de sécurité visés aux art. 41*b*, al. 2, LEI et 6*a*, al. 2, LDI;

c. les contrôles de loyauté visés aux art. 29*a* LAsi, 20*b* LPers, 14 LAAM et 20*a* LApEl;

RS .....
1 RS **128**
2 RS **142.20**
3 RS **142.31**
4 RS **143.1**
5 RS **172.220.1**
6 RS **510.10**
7 RS **732.1**
8 RS **734.7**

d. les contrôles de sécurité relatifs aux personnes visés à l'art. 23, al. 2, let. d, et 103, al. 3, let. d, LAAM;

e. l'évaluation du potentiel d'abus ou de dangerosité visée à l'art. 113, al. 4, let. d, LAAM;

f. les contrôles de fiabilité visés à l'art. 24 LENu.

2 Elle régit également:

a. l'organisation des services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes (services spécialisés CSP);

b. le certificat international de sécurité;

c. les responsabilités en matière de protection des données traitées dans le système d'information visé à l'art. 45 LSI et la sécurité des données;

d. le contrôle périodique, réalisé par un organe externe, du traitement des données personnelles dans le cadre des contrôles de sécurité relatifs aux personnes.

3 Elle détermine les aspects suivants qui relèvent du domaine de compétence du Conseil fédéral:

a. les fonctions impliquant l'exercice d'une activité visée à l'al. 1;

b. l'attribution d'un degré de contrôle aux activités sensibles;

c. les services chargés de demander le contrôle et les instances décisionnelles.

Art. 2 Champ d'application

La présente ordonnance s'applique aux autorités et aux organisations visées à l'art. 2 LSI, sous réserve des art. 84, al. 3, LSI et 2, al. 2–5, de l'ordonnance du … sur la sécurité de l'information[9].

Section 2 Listes des fonctions

Art. 3 Attribution
(art. 28, al. 1, LSI et 24, al. 1, LENu)

1 Les listes des fonctions suivantes s'appliquent dans l'administration fédérale:

a. pour les contrôles de sécurité relatifs aux personnes selon la LSI: la liste de l'annexe 1;

b. pour les contrôles de loyauté selon la LAsi: la liste de l'annexe 2;

c. pour les contrôles de loyauté selon la LPers: la liste de l'annexe 3.

2 Les listes des fonctions suivantes s'appliquent à l'armée:

a. pour les contrôles de sécurité relatifs aux personnes selon la LSI: la liste de l'annexe 4;

9 RS **128.xxx**

b. pour les contrôles de loyauté visés à l'art. 14 LAAM: la liste de l'annexe 5.

3 La liste de l'annexe 6 s'applique aux fonctions visées à l'art. 20*a*, al. 1, LApEl.

4 Le titulaire d'une autorisation de construire ou d'exploiter une installation nucléaire et le destinataire d'une décision de désaffectation tiennent la liste des fonctions requérant un contrôle de fiabilité visé à l'art. 24, al. 1, LENu. L'Inspection fédérale de la sécurité nucléaire (IFSN) fixe dans des directives les exigences auxquelles doivent répondre ces listes et leur mise à jour.

Art. 4 Modification

Sur demande des départements et de la Chancellerie fédérale, le DDPS peut compléter ou modifier les listes des fonctions figurant dans les annexes 1 à 6. Il consulte au préalable le service spécialisé de la Confédération pour la sécurité de l'information.

Art. 5 Publication, conservation et communication

1 En vertu de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles[10], les annexes 1, 4 et 6 ne sont pas publiées dans le recueil officiel.

2 Le DDPS conserve les listes des fonctions figurant dans les annexes 1, 4 et 6 et les communique aux services et aux personnes accomplissant des tâches prévues par la présente ordonnance.

Art. 6 Contrôle de l'actualité
(art. 28, al. 2, LSI)

1 Les départements et la Chancellerie fédérale contrôlent l'actualité des listes des fonctions relevant de leur domaine de compétence:

a. au moins tous les quatre ans;

b. en cas de réorganisation ou de prise ou de remise de tâches.

2 Ils rendent compte de leur contrôle au DDPS et lui adressent si nécessaire une demande de modification conformément à l'art. 4.

Section 3 Contrôles sans listes des fonctions

Art. 7 Contrôle extraordinaire

Le DDPS décide dans chaque cas sur demande du département ou de la Chancellerie fédérale si une personne appelée à exercer une fonction qui ne figure pas encore sur une liste des fonctions visées aux annexes 1 à 7 sera contrôlée ou non. Il consulte au préalable le service spécialisé de la Confédération pour la sécurité de l'information.

10 RS **170.512**

Art. 8 Contrôles du personnel cantonal et des tiers
(art. 29, al. 1, let. b et c, art. 3 LSI et 24, al. 1, LENu)

1 Le DDPS décide à la demande du canton quelles fonctions du personnel cantonal sont soumises à un contrôle de sécurité visé à l'art. 29, al. 1, let. b, LSI. Il consulte au préalable le service spécialisé de la Confédération pour la sécurité de l'information.

2 La décision quant à savoir si les tiers exécutant un mandat sensible pour l'administration fédérale en vertu de l'art. 49 LSI sont soumis à un contrôle de sécurité est prise par:

a. dans le cadre de la procédure de sécurité relative aux entreprises: le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises ;

b. dans tous les autres cas: le préposé à la sécurité de l'information du département ou de la Chancellerie fédérale.

Art. 9 Contrôle de fiabilité extraordinaire de l'IFSN

L'IFSN prend la décision quant à la fiabilité des personnes n'ayant accès que durant une brève période à des informations classifiées concernant les systèmes de sûreté ou de sécurité relatifs à des installations ou des matières nucléaires. Elle peut ne pas procéder à un contrôle de fiabilité visé à l'art. 24, al. 1, LENu et se référer notamment à des renseignements fournis par les instances suivantes:

a. une entreprise suisse ou étrangère pour laquelle la personne concernée travaille ou a travaillé;

b. une chambre de commerce suisse ou étrangère;

c. une autorité du pays étranger dont la personne concernée est originaire.

Section 4 Degrés de contrôle

Art. 10 Contrôles de sécurité relatifs aux personnes selon la LSI
(art. 30 LSI)

1 Les activités sensibles suivantes visées dans la LSI requièrent un contrôle de sécurité de base:

a. le traitement des informations classifiées «confidentiel»;

b. l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques relevant de la catégorie de sécurité «protection élevée»;

c. l'accès à des zones de sécurité, en particulier aux zones de protection 2 et 3 d'un ouvrage au sens de la législation sur la protection des ouvrages militaires;

d. les activités soumises en vertu d'un traité international à un contrôle correspondant à ce degré de contrôle.

2 Les activités sensibles suivantes visées dans la LSI requièrent un contrôle de sécurité élargi:

a. le traitement des informations classifiées «secret»;

b. l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques relevant de la catégorie de sécurité «protection très élevée»;

c. les activités sensibles des employés de la Confédération ou des collaborateurs externes:
   1. du Service de renseignement de la Confédération (SRC),
   2. du Renseignement militaire (RM),
   3. du Centre des opérations électroniques (COE) de la Base d'aide au commandement,
   4. de l'autorité de surveillance indépendante des activités de renseignement (AS-Rens);

d. les activités sensibles des collaborateurs des autorités d'exécution cantonales visées à l'art. 9 de loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[11];

e. les activités soumises en vertu d'un traité international à un contrôle correspondant à ce degré de contrôle.

Art. 11 Contrôle de loyauté selon la LPers

[1] Les activités suivantes visées à l'art. 20*b* LPers requièrent un contrôle de sécurité de base:

a. activités relevant de la puissance publique accomplies par des employés de la Confédération affectés à l'étranger et par des employés du Département fédéral des affaires étrangères (DFAE) soumis à la discipline des transferts;

b. activités visées à l'art. 20*b*, al. 1, let. b, LPers, dont l'exécution déloyale peut provoquer un préjudice de 50 millions à 500 millions de francs suisses;

c. activités accomplies dans le cadre de tâches de poursuite pénale ou de police:
   1. concernant les moyens et les méthodes opérationnelles de lutte contre les crimes ou les délits,
   2. concernant l'identité des personnes exposées,
   3. du personnel de l'Office fédéral de la police (fedpol) et de l'Office fédéral de la justice;

d. activités exercées par des personnes directement subordonnées à un chef de département ou au chancelier de la Confédération ou appartenant à leur état-major le plus étroit.

[2] Les activités suivantes visées à l'art. 20*b* LPers requièrent un contrôle de sécurité élargi:

a. activités des fonctions dont le Conseil fédéral est compétent pour conclure, modifier et résilier les rapports de travail en vertu de l'art. 2, al. 1, de l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération (OPers)[12];

11 RS **121**
12 RS **172.220.111.3**

b. activités exercées dans le cadre de rapports de travail dont la conclusion, la modification ou la résiliation relèvent de la compétence du chef de département ou du chancelier de la Confédération en vertu de l'art. 2, al. 1bis, OPers;

c. activités des responsables des unités administratives décentralisées visées à l'art. 2, al. 1, let. e, LPers;

d. activités visées à l'art. 20*b*, al. 1, let. b, LPers, dont l'exécution déloyale peut provoquer un préjudice supérieur à 500 millions de francs suisses;

e. activités des employés des services spécialisés CSP.

Art. 12 Contrôles selon la LAAM

1 Les activités et les contrôles suivants visés dans la LAAM requièrent un contrôle de sécurité de base:

a. activités exercées en uniforme à l'étranger visées à l'art. 14, al. 1, let. a, LAAM dans le cadre de la représentation officielle de la Suisse ou de la diplomatie et militaire;

b. activités visées à l'art. 14, al. 1, let. b, LAAM, dont l'exécution déloyale peut provoquer un préjudice de 50 millions à 500 millions de francs suisses;

c. contrôles visées à l'art. 23, al. 2, let. d, LAAM.

2 Un contrôle de sécurité relatif aux personnes visé à l'art. 103, al. 3, let. d, LAAM ne peut être exigé pour les candidats que:

a. s'il existe un motif justifiant le contrôle visé à l'art. 10, al. 1, et

b. si le délai minimal fixé pour la répétition du contrôle à l'art. 43, al. 1, LSI est échu.

Art. 13 Contrôles de fiabilité selon la LENu

1 Les contrôles de fiabilité des personnes suivantes visés à l'art. 24, al. 1, LENu requièrent un contrôle de sécurité de base:

a. les personnes engagées auprès du titulaire d'une autorisation de construire ou d'exploiter une installation nucléaire ou du destinataire d'une décision de désaffectation et qui ont accès à des informations classifiées «confidentiel» relatives à des installations ou des matières nucléaires;

b. les personnes ayant accès durant une longue période à des informations classifiées concernant les systèmes de sûreté ou de sécurité relatifs à des installations ou des matières nucléaires;

c. les personnes exerçant une activité dans le domaine de la sûreté des installations nucléaires, en particulier le personnel de surveillance.

2 Les contrôles de fiabilité des personnes engagées auprès du titulaire d'une autorisation de construire ou d'exploiter une installation nucléaire ou du destinataire d'une décision de désaffectation et qui ont accès à des informations classifiées

«secret» relatives à des installations ou des matières nucléaires requièrent un contrôle de sécurité élargi.

Art. 14 Contrôles de loyauté selon la LApEl

1 Les activités de la société nationale du réseau de transport visée à l'art. 18 LApEl dont l'accomplissement exige un accès aux informations critiques en matière de sécurité d'approvisionnement, aux applications et aux infrastructures critiques requièrent un contrôle de sécurité de base.

2 Les activités de la société nationale du réseau de transport dont l'accomplissement exige un accès aux informations extrêmement critiques en matière de sécurité d'approvisionnement, aux applications et aux infrastructures extrêmement critiques requièrent un contrôle de sécurité élargi.

Section 5 Procédure

Art. 15 Services qui demandent le contrôle et instances décisionnelles
(art. 31, al. 1, LSI)

1 Les départements et la Chancellerie fédérale désignent pour leur domaine de compétence les services qui demandent le contrôle et les instances décisionnelles et en informent les services spécialisés CSP.

2 Si la compétence en matière de sélection des personnes ou de changement de mandat ou de fonction relève du Conseil fédéral, celui-ci est l'instance décisionnelle.

3 Les contrôles de fiabilité visés à l'art. 24, al. 1, LENu relèvent de la compétence des services suivants:

a. les services qui demandent le contrôle: les titulaires d'une autorisation de construire ou d'exploiter une installation nucléaire ou les destinataires d'une décision de désaffectation;

b. l'instance décisionnelle: l'IFSN.

4 La société nationale du réseau de transport est le service qui demande le contrôle et l'instance décisionnelle en matière de contrôles de loyauté visés à l'art. 20*a* LApEl.

5 Les autorités soumises à la LSI et les cantons informent les services spécialisés CSP des services qui demandent le contrôle et des instances décisionnelles dans leur domaine de compétences.

Art. 16 Services spécialisés CSP
(art. 31, al. 2, LSI)

1 Les services spécialisés CSP sont:

a. le service spécialisé CSP de la Chancellerie fédérale (Service spécialisé CSP ChF);

b. le service spécialisé CSP du Département fédéral de la défense, de la protection de la population et des sports (Service spécialisé CSP DDPS).

2 Le Service spécialisé CSP ChF est chargé de contrôler les personnes exerçant les fonctions suivantes:

a. fonctions dont le Conseil fédéral est compétent pour conclure, modifier et résilier les rapports de travail en vertu de l'art. 2, al. 1, OPers[13], à l'exception des fonctions au sein de la Chancellerie fédérale;

b. activités exercées dans le cadre de rapports de travail dont la conclusion, la modification ou la résiliation relèvent de la compétence du chef de département ou du chancelier de la Confédération en vertu de l'art. 2, al. 1bis, OPers;

c. fonctions au sein du Service spécialisé CSP DDPS;

d. fonctions du DDPS impliquant des tâches de conduite envers le Service spécialisé CSP DDPS.

3 Le Service spécialisé CSP DDPS est chargé de tous les autres contrôles.

Art. 17 Contrôle des conditions du contrôle
(art. 31, al. 2, LSI)

1 Après l'ouverture de la procédure, les services spécialisés CSP vérifient si:

a. la fonction concernée figure sur la liste des fonctions;

b. la procédure a été ouverte par le service compétent;

c. la personne soumise au contrôle y a consenti, pour autant que son consentement soit nécessaire;

d. le cas échéant, le service compétent visé à l'art. 7 ou 8 (al. 2) a donné son accord.

2 Lors de la répétition extraordinaire du contrôle, ils vérifient si cette répétition est suffisamment fondée.

3 Si l'une des conditions visées aux al. 1 et 2 n'est pas remplie, les services spécialisés CSP n'effectuent pas le contrôle et en informent immédiatement le service qui a demandé le contrôle.

Art. 18 Collaboration
(art. 32, al. 3, LSI)

1 La personne soumise au contrôle doit notamment:

a. présenter les documents et les données utiles au contrôle;

b. donner des renseignements conformes à la vérité.

2 Si la personne soumise au contrôle ne respecte pas son obligation de collaborer malgré un avertissement, les services spécialisés CSP le prennent en considération dans le cadre de l'évaluation des risques.

13 RS **172.220.111.3**

3 Si la personne soumise au contrôle refuse de collaborer de sorte qu'il n'est pas possible de l'évaluer de manière appropriée de procéder à une évaluation, le service spécialisé CSP rend une constatation au sens de l'art. 39, al. 1, let. d, LSI.

Art. 19 Collecte des données
(art. 34 LSI)

1 Les services spécialisés CSP peuvent collecter et traiter les données visées à l'annexe 7.

2 Une audition visée à l'art. 34, al. 2, let. d, LSI est menée si:

a. le Conseil fédéral est compétent pour conclure, modifier et résilier les rapports de travail en vertu de l'art. 2, al. 1, OPers[14];

b. le chef de département ou le chancelier de la Confédération est compétent pour conclure, modifier et résilier les rapports de travail en vertu de l'art. 2, al. 1[bis], OPers;

c. la personne soumise au contrôle exerce une fonction dans l'un des services suivants ou s'il est prévu qu'elle exerce une telle fonction:
   1. SRC,
   2. autorités d'exécution cantonales visées à l'art. 9 LRens[15],
   3. RM,
   4. COE,
   5. AS-Rens,
   6. fedpol,
   7. services spécialisés CSP;

d. en tant qu'employée de la Confédération, la personne soumise au contrôle doit traiter des informations classifiées «secret», et:
   1. a ainsi largement connaissance d'importants dossiers de la politique de sécurité sur lesquels elle peut exercer une influence, ou
   2. assume des tâches de coordination et de surveillance concernant les fonctions visées à la let. c;

f. elle est prescrite en vertu d'un traité international.

3 Il n'est pas nécessaire de procéder à une audition en cas de répétition du contrôle de sécurité.

4 Les tiers suivants peuvent être auditionnés en vertu de l'art. 34, al. 3, LSI ou de l'art. 113, al. 5, let. e, LAAM:

a. les spécialistes du domaine médical ou psychologique qui s'occupent ou se sont occupés de la personne soumise au contrôle;

b. les institutions de formation auprès desquelles la personne soumise au contrôle a suivi des formations;

14 RS **172.220.111.3**
15 RS **121**

c. les supérieurs professionnels ou militaires anciens ou actuels de la personne soumise au contrôle;

d. les autres personnes susceptibles de posséder des informations utiles concernant la personne soumise au contrôle.

5 Les services spécialisés CSP peuvent auditionner les personnes à l'aide de moyens audiovisuels.

Art. 20 Assistance administrative
(art. 35 LSI)

1 Les autorités ou les organisations visées à l'art. 34 LSI chargées de collecter les données à l'étranger les transmettent aux services spécialisés CSP:

a. en indiquant la source des données;

b. en fournissant une évaluation de la fiabilité des données et des sources des données.

2 Sont considérées comme pertinentes pour la sécurité au sens de l'art. 35, al. 2, LSI toutes les données qui en elles-mêmes ou en lien avec d'autres données sont susceptibles de receler des indices concrets de risque pour la sécurité.

Art. 21 Regroupement des procédures de contrôle

1 Si une activité requiert plusieurs contrôles visés à l'art. 1, al. 1, seule une procédure a lieu.

2 Si l'activité visée à l'al. 1 correspond à plusieurs degrés de contrôle, la procédure est réalisée selon les exigences du degré le plus élevé; l'art. 27 est réservé.

3 Si le contrôle relève tant du service spécialisé CSP ChF que du service spécialisé CSP DDPS, il est réalisé par le service spécialisé CSP ChF. Les évaluations du potentiel d'abus ou de dangerosité visées à l'art. 113, al. 4, let. d, LAAM, qui sont toujours effectuées par le service spécialisé CSP DDPS, en sont exclues.

4 Le service spécialisé CSP compétent inscrit le résultat de l'évaluation de chaque contrôle dans la déclaration visée à l'art. 39, al. 1, LSI.

Art. 22 Conditions
(art. 39, al. 1, let. b, LSI)

Les services spécialisés CSP peuvent recommander aux instances décisionnelles:

a. d'obliger la personne concernée à communiquer des données personnelles à l'instance décisionnelle, notamment:

1. les données sur des relations avec des tiers,
2. les données financières, y compris celles qui concernent les comptes bancaires et les impôts,
3. les données concernant les examens visés à la let. b,
4. les données sur les procédures en cours au moment de la déclaration;

b. de procéder à des examens médicaux ou psychologiques, notamment pour ce qui est de la capacité de jugement et de décision de la personne soumise au contrôle et sa consommation de drogue et de stupéfiants;

c. de prendre les mesures visées à l'art. 25 LPers;

d. de prendre les autres mesures concernant la possession de l'arme personnelle, si la personne soumise au contrôle est un militaire;

e. de prendre les autres mesures qui semblent à même, dans le cas d'espèce, à ramener à un niveau supportable le risque pour la sécurité qui a été constaté.

Art. 23 Communication
(art. 40 LSI)

1 S'il existe plusieurs motifs successifs justifiant un contrôle concernant une personne et si un service spécialisé CSP constate un risque pour la sécurité lors d'un contrôle ultérieur, ce service communique sa déclaration aux instances décisionnelles des contrôles précédents.

2 Les services spécialisés CSP communiquent leurs constatations intermédiaires s'il existe des signes de risque pour la sécurité requérant une action immédiate. Lors des contrôles des conscrits ou des militaires, ces signes peuvent prendre les formes suivantes:

a. les condamnations pénales;

b. les enquêtes policières, les enquêtes pénales ou les procédures pénales en cours pour soupçon de délit ou de crime; la communication ne peut avoir lieu que si, selon l'évaluation du service qui dirige l'enquête ou la procédure, elle ne met pas en danger la procédure en cours menée;

c. les signes ou les indices sérieux visés à l'art. 113, al. 1, LAAM ou les soupçons de signes ou d'indices sérieux;

d. les signes ou les indices d'une aptitude au service militaire limitée, d'une inaptitude au service militaire ou d'une incapacité à assumer ses fonctions;

e. les signes ou les indices sérieux laissant présumer qu'ils pourraient constituer un danger pour eux-mêmes ou pour autrui.

3 Les instances décisionnelles communiquent aux services spécialisés CSP à quelle personne ou à quel service et les communications visées aux al. 1 et 2 doivent être adressées.

Section 6 Conséquences de la déclaration

Art. 24 Exercice de l'activité
(art. 41 LSI)

1 L'instance décisionnelle ne laisse la personne contrôlée exercer l'activité que si elle évalue les risques reconnus comme admissibles ou pouvant être ramenés à un niveau supportable à l'aide de conditions visées à l'art. 22.

2 En cas de déclaration visée à l'art. 39, al. 1, let. b à d, LSI, elle communique sa décision à la personne contrôlée est au service spécialisé CSP compétent dans l'intervalle d'un mois. En cas de déclaration de sécurité visée à l'art. 39, al. 1, let. a, LSI, l'autorisation d'exercer l'activité est présumée.

Art. 25 Utilisation de la déclaration pour d'autres activités sensibles
(art. 42 LSI)

1 Si une personne est l'objet d'une déclaration valable reposant sur un contrôle antérieur, l'instance décisionnelle peut ne pas procéder à une nouvelle évaluation:

a. si l'évaluation précédente est fondée sur les mêmes facteurs de risque que le nouveau contrôle, et

b. s'il n'y a aucune raison de procéder à une répétition extraordinaire du contrôle.

2 Les risques pour la sécurité constatés lors d'une évaluation correspondant à un degré de contrôle plus élevé ne peuvent être pris en considération que si:

a. ces risques peuvent également être décelés à l'aide des données collectées qui correspondent à un degré de contrôle moins élevé, ou

b. les intérêts publics visés à l'art. 1, al. 2, LSI l'emportent sur les droits de la personnalité de la personne contrôlée.

Art. 26 Répétition ordinaire du contrôle
(art. 43, al. 1 et 2, LSI)

1 Un contrôle est d'ordinaire répété:

a. dans les trois mois qui précèdent l'expiration du délai maximal fixé à l'art. 43, al. 1, LSI: si une déclaration de sécurité visée à l'art. 39, al. 1, let. a, LSI a été rendue lors du contrôle précédent;

b. dans les trois mois qui succèdent à l'expiration du délai minimal fixé à l'art. 43, al. 1, LSI: si une déclaration ou une constatation visée à l'art. 39, al. 1, let. b à d, LSI a été rendue lors du contrôle précédent;

c. pour les fonctions de l'armée et de la protection civile requérant un contrôle de sécurité de base: si la personne soumise au contrôle exercera sa fonction probablement encore pendant cinq ans au moins.

2 Les délais fixés dans un traité international sont réservés.

Art. 27 Répétition extraordinaire du contrôle
(art. 43, al. 3, LSI)

1 Lorsque l'instance décisionnelle a des raisons de penser que des risques importants sont apparus depuis le dernier contrôle qui ne peuvent être évalués sans nouveau contrôle, elle lance immédiatement une répétition extraordinaire du contrôle.

2 Lorsqu'elle a des raisons de penser que les risques constatés lors du dernier contrôle n'existent plus, elle peut lancer une répétition extraordinaire du contrôle.

Art. 28 Effet de la répétition
(art. 43 LSI)

1 Jusqu'à la nouvelle décision selon l'art. 24, al. 2, la personne concernée est considérée comme contrôlée conformément à la décision valable jusqu'ici.

2 Si des signes de nouveaux risques pour la sécurité apparaissent avant la notification de la nouvelle décision, l'instance des décisionnelle prend les mesures préventives nécessaires.

Art. 29 Voies de droit
(art. 44, al. 3, LSI)

Les services spécialisés CSP sont autorisés à interjeter un recours auprès du Tribunal fédéral contre les décisions du Tribunal administratif fédéral concernant leurs déclarations.

Art. 30 Certificat international de sécurité
(art. 48, let. c, LSI)

1 Le service spécialisé de la Confédération pour la sécurité de l'information est compétent pour délivrer les certificats internationaux de sécurité.

2 Un certificat de sécurité est délivré sur demande si:

a. un contrôle correspondant au degré de contrôle requis a été réalisé;

b. la personne concernée a été autorisée à exercer l'activité, et

c. il peut être prouvé que la personne concernée a été formée pour exercer l'activité.

3 Si le service qui demande le contrôle ne fait pas partie de l'administration fédérale et n'a pas besoin du certificat de sécurité pour accomplir un mandat de la Confédération, il assume les coûts de la procédure.

Section 7 Traitement des données personnelles

Art. 31 Responsabilité en matière de protection et de sécurité des données
(art. 48, let. d, LSI))

1 Le Service spécialisé CSP DDPS est responsable de la protection et de la sécurité du système d'information visé à l'art. 45 LSI et des données qu'il contient.

2 Le service chargé du traitement est responsable de la protection et de la sécurité des données traitées en dehors du système d'information visé à l'art. 45, al. 5, LSI.

Art. 32 Contrôle périodique du traitement des données personnelles
(art. 48, let. e, LSI)

Le DDPS et la Chancellerie fédérale veillent à ce qu'un organe indépendant contrôle au moins tous les cinq ans la licéité du traitement des données personnelles par leurs services spécialisés CSP.

Section 8 Dispositions finales

Art. 33 Gestion électronique des affaires
(art. 48, let. a, LSI)

Après avoir consulté la Chancellerie fédérale, le DDPS règle la gestion électronique des affaires.

Art. 34 Émoluments

1 Les services spécialisés CSP perçoivent, en fonction du temps consacré, des émoluments pour les contrôles effectués auprès des services n'appartenant pas à l'administration fédérale centrale.

2 Le tarif horaire est de 100 à 400 francs. Il dépend de l'urgence du mandat et de la fonction occupée par le personnel qui conduit le contrôle.

3 Pour le reste, l'ordonnance générale du 8 septembre 2004 sur les émoluments (OGEmol)[16] s'applique.

Art. 35 Prestations des services spécialisés CSP en faveur des cantons
(art. 86, al. 4, LSI)

1 Les cantons peuvent recourir aux prestations du Service spécialisé CSP DDPS pour leur propre sécurité de l'information:

a. lorsqu'ils disposent d'une base légale suffisante pour les contrôles à effectuer en vertu de la présente ordonnance;

b. lorsqu'ils entendent effectuer des évaluations à l'instar de la Confédération pour garantir la sécurité de l'information, et

c. lorsqu'ils ont conclu une convention de prestations avec le DDPS.

2 Le DDPS règle notamment dans les conventions de prestations visées à l'al. 1, let. c:

a. le nombre de contrôles à réaliser;

b. les services qui demandent le contrôle et les instances décisionnelles des cantons;

c. le financement des prestations, y compris ses modalités.

3 Le montant des émoluments est calculé en fonction du temps consacré. Le tarif horaire est de 100 à 400 francs. Il dépend de l'urgence du mandat et de la fonction occupée par le personnel qui conduit le contrôle. Pour le reste, l'ordonnance générale du 8 septembre 2004 sur les émoluments (OGEmol)[17] s'applique.

Art. 36 Abrogation d'autres actes

Sont abrogées:

16 RS **172.041.1**
17 RS **172.041.1**

a. l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes[18];

b. l'ordonnance de la Chancellerie fédérale du 30 novembre 2011 sur les contrôles de sécurité relatifs aux personnes[19];

c. l'ordonnance du DEFR du 2 novembre 2011 sur les contrôles de sécurité relatifs aux personnes[20];

d. l'ordonnance du DDPS du 12 mars 2012 concernant les contrôles de sécurité relatifs aux personnes[21];

e. l'ordonnance du DFAE du 14 août 2012 sur les contrôles de sécurité relatifs aux personnes[22];

f. l'ordonnance du DETEC du 15 février 2013 sur les contrôles de sécurité relatifs aux personnes[23];

g. l'ordonnance du DFJP du 26 juin 2013 sur les contrôles de sécurité relatifs aux personnes[24];

h. l'ordonnance du DFI du 12 août 2013 sur les contrôles de sécurité relatifs aux personnes[25];

i. l'ordonnance du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires[26].

Art. 37 Modification d'autres actes

La modification d'autres actes est réglée dans l'annexe 8.

Art. 38 Dispositions transitoires

[1] Les évaluations en cours à l'entrée en vigueur de la présente ordonnance sont poursuivies ou classées selon la LSI et la présente ordonnance.

[2] Les contrôles de sécurité relatifs aux personnes réalisés selon l'ancien droit correspondent durant la période transitoire visée à l'art. 90, al. 3, LSI aux degrés de contrôle du nouveau droit comme suit:

a. contrôle de sécurité de base selon l'ancien droit: contrôle de sécurité de base selon le nouveau droit;

b. contrôle de sécurité élargi selon l'ancien droit: contrôle de sécurité élargi selon le nouveau droit;

18 [RO **2011** 5903, **2012** 1153 3631 3765 5527 6669, **2013** 3041, **2014** 4567, **2016** 1785, **2017** 4151 4231, **2020** 5893]
19 [RO **2011** 6077, **2016** 1365]
20 [RO **2011** 4999, **2013** 1335]
21 [RO **2012** 1161 1597]
22 [RO **2012** 4241]
23 [RO **2013** 765]
24 [RO **2013** 2633]
25 [RO **2013** 2675]
26 [RO **2006** 2481, **2008** 547, **2011** 1031]

c. contrôle de sécurité élargi avec audition selon l'ancien droit: contrôle de sécurité élargi selon le nouveau droit.

3 Les personnes ayant des fonctions requérant un contrôle ou un contrôle correspondant à un degré de contrôle supérieur selon le nouveau droit sont considérées comme étant contrôlées jusqu'à la décision visée à l'art. 24, al. 2, si le nouveau contrôle requis est réalisé dans les trois mois après l'entrée en vigueur de la présente ordonnance. Si le contrôle révèle des signes de risque pour la sécurité, l'instance décisionnelle décide des mesures de prévention nécessaires.

4 Les contrôles de sécurité que la société nationale du réseau de transport a reçus sur la base du droit privé avant l'entrée en vigueur de la présente ordonnance et avant l'échéance du délai fixé à l'al. 5 restent applicables comme suit dans le cadre des délais fixés pour les répétitions visés aux art. 26 et 27:

a. contrôles de sécurité pour les fonctions critiques: en tant que contrôle de sécurité de base selon la présente ordonnance;

b. contrôles de sécurité pour les fonctions extrêmement critiques: en tant que contrôle de sécurité élargi selon la présente ordonnance.

5 La société nationale du réseau de transport est autorisée à faire réaliser des contrôles de loyauté en vertu de l'art. 20*a* LApEl sur la base du droit privé jusqu'à un an après l'entrée en vigueur de la présente ordonnance.

Art. 39 Entrée en vigueur

La présente ordonnance entre en vigueur le … 2023.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ignazio Cassis
Le chancelier de la Confédération, Walter Thurnherr

Annexe 1[27]
(art. 3, al. 1, let. a)

Fonctions de l'administration fédérale requérant un contrôle de sécurité relatif aux personnes selon la LSI

1. du degré de contrôle de contrôle de sécurité de base:

Unité administrative	Fonction	Motif du contrôle selon l'art. 10, al. 1		
		Let. a	Let. b	Let. c

2. du degré de contrôle de contrôle de sécurité élargi:

Unité administrative	Fonction	Motif du contrôle selon l'art. 10, al. 2			
		Let. a	Let. b	Let. c	Let. d

27 En application de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles (RS **170.512**), ce texte n'est pas publié dans le RO.

Annexe 2
(art. 3, al. 1, let. b)

Fonctions de l'administration fédérale requérant un contrôle de loyauté selon la LAsi

a. …,

b. …;

c. ….

Annexe 3
(art. 3, al. 1, let. c)

Fonctions de l'administration fédérale requérant un contrôle de loyauté selon la LPers

1. du degré de contrôle de contrôle de sécurité de base:

Unité administrative	Fonction	Motif du contrôle selon l'art. 11, al. 1			
		Let. a	Let. b	Let. c	Let. d

2. du degré de contrôle de contrôle de sécurité élargi:

Unité administrative	Fonction	Motif du contrôle selon l'art. 11, al. 2				
		Let. a	Let. b	Let. c	Let. d	Let. e

Annexe 4[28]
(art. 3, al. 2, let. a)

Fonctions de l'armée requérant un contrôle de sécurité relatif aux personnes selon la LSI

1. du degré de contrôle de contrôle de sécurité de base:

Échelon de l'articulation et de la structure	Fonction	Motif du contrôle selon l'art. 10, al. 1		
		Let. a	Let. b	Let. c

2. du degré de contrôle de contrôle de sécurité élargi:

Échelon de l'articulation et de la structure	Fonction	Motif du contrôle selon l'art. 10, al. 2	
		Let. a	Let. b

28 En application de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles (RS **170.512**), ce texte n'est pas publié dans le RO.

Annexe 5
(art. 3, al. 2, let. b)

Fonctions de l'armée requérant contrôle de loyauté selon l'art. 14 LAAM

du degré de contrôle de contrôle de sécurité de base:

Échelon de l'articulation et de la structure	Fonction	Motif du contrôle selon l'art. 12. al. 1, let. a et b	
		Let. a	Let. b

Annexe 6[29]
(art. 3, al. 3)

Fonctions visées à l'art. 20*a*, al. 1, LApEl

1. du degré de contrôle de contrôle de sécurité de base:

Fonction	Information, application ou infrastructure critique

2. du degré de contrôle de contrôle de sécurité élargi:

Fonction	Information, application ou infrastructure extrêmement critique

29 En application de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles (RS **170.512**), ce texte n'est pas publié dans le RO.

Annexe 7
(art. 19, al. 1)

Collecte et traitement des données

1. Données pouvant être traitées à tous les degrés de contrôle:

a. Données d'identité de la personne soumise au contrôle, notamment:
   1. Nom, nom avant mariage et prénoms
   2. Surnom, alias, pseudonyme et nom d'utilisateur
   3. Adresses
   4. Date de naissance
   5. Sexe ou genre
   6. Numéros de téléphone (réseaux fixe et mobile)
   7. Adresses e-mail (professionnelles et privées)
   8. Numéro AVS
   9. Nationalités
   10. En cas de nationalité autre que Suisse:
      – date de naturalisation
      – durée du séjour en Suisse
   11. Lieu d'origine
   12. Lieu de naissance
   13. Anciens lieux de domicile

b. Données sur le mode de vie de la personne soumise au contrôle, notamment:
   1. Carrière professionnelle
   2. Cursus scolaire
   3. Carrière au sein de l'armée, de la protection civile ou du service civil
   4. Formations
   5. Activités de loisirs
   6. Projets
   7. Activités associatives
   8. Bénévolat
   9. Opinions ou activités religieuses
   10. Opinions philosophiques
   11. Opinions ou activités politiques
   12. Opinions ou activités syndicales

c. Données sur les liaisons personnelles étroites et les relations familiales de la personne soumise au contrôle, notamment:

1. État civil
2. Sphère intime et sexualité
3. Relations avec la famille
4. Identité des parents
5. Cercle d'amis

d. Données sur les rapports avec l'étranger de la personne soumise au contrôle, notamment:
1. Vacances
2. Séjours linguistiques
3. Voyages d'affaires
4. Relations personnelles à l'étranger et contacts internationaux
5. Intérêts financiers à l'étranger

e. Données concernant la santé de la personne soumise au contrôle, notamment:
1. Maladies physiques et psychiques
2. Handicaps physiques et psychiques
3. Consommation de stupéfiants et d'alcool
4. Addictions et dépendances

f. Données financières de la personne soumise au contrôle, notamment:
1. Extraits de comptes bancaires
2. Immobilisations financières
3. Salaires
4. Hypothèques
5. Crédits
6. Patrimoine
7. Impôts
8. Dettes
9. Investissements

g. Données sur les poursuites et les sanctions administratives ou pénales, notamment:
1. Poursuites et faillites
2. Enquêtes pénales
3. Enquêtes administratives
4. Actions et procès judiciaires
5. Médiation
6. Retraits de permis

h. Données sur les facteurs de risque dans le cadre d'une activité sensible:

i. Données concernant des tiers, notamment:
   1. Données visées aux let. a à g concernant le partenaire, l'époux ou l'épouse, la famille proche ou le cercle d'amis étroit si ces données visées à l'art. 34, al. 3, LSI sont indispensables pour évaluer le risque pour la sécurité.
   2. Mandant et son adresse
   3. Projet

j. Données tirées de systèmes ou de sources d'information publiques, notamment:
   1. Toutes les données du casier judiciaire
   2. Toutes les données des autorités pénales civiles et militaires
   3. Les données suivantes des organes de la Confédération visés à l'art. 34, al. 1, let. c, LSI:
      - données de la plate-forme d'information sur les armes ARMADA
      - données du système d'information HOOGAN
      - données du système d'information JANUS
      - données de l'index national de police
      - données du système de recherches informatisées de police RIPOL
      - données des systèmes d'information du SRC et du RM
      - données du SIAC
      - données du JORASYS
      - données des systèmes d'information de l'OFDF
      - données du registre central des assurés des assurances sociales fédérales
      - données du SIPA
      - données concernant le recrutement des conscrits
      - données concernant l'examen de l'aptitude au service et de l'aptitude à faire du service des conscrits et des personnes astreintes au service militaire ou au service de protection civile, ainsi que des civils participant à un engagement de l'armée de durée déterminée
      - données de l'armée et de l'administration militaire concernant les conscrits et les militaires

4. Toutes les données des registres et dossiers des organes de sécurité des cantons et des organes de police
5. Toutes les données des registres des offices des poursuites et des faillites
6. Toutes les données datant de 10 ans ou moins et qui n'ont pas encore été archivées ou détruites visées à l'art. 47 LSI
7. Données de sources d'information publiques:
   - Internet: données librement accessibles à tout utilisateur d'Internet qui a ouvert un compte, payé des émoluments ou conclu un abonnement,
   - réseaux sociaux: données accessibles à tout utilisateur sans prise de contact personnelle avec un autre utilisateur.

2. Données pouvant être traitées dans le cadre du degré de contrôle de contrôle de sécurité élargi:

a. Toutes les données détenues par les autorités fiscales fédérales et cantonales

b. Toutes les données du registre du contrôle des habitants

c. Toutes les données détenues par les établissements financiers et banques visés à l'art. 34, al. 2, let. c, LSI

d. Toutes les données fournies par la personne concernée au cours d'une audition pour vérifier des faits qui ne ressortent pas ou pas clairement des autres collectes de données

Annexe 8
(art. 37)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports[30]

Art. 6, let. c

Abrogée

2. Ordonnance du 3 juillet 2001 sur le personnel de la Confédération[31]

Art. 94e Extrait du casier judiciaire et du registre des poursuites
(art. 20*a* LPers)

1 L'employeur peut exiger des candidats et de ses employés qu'ils produisent un extrait de casier judiciaire et du registre des poursuites si cela est approprié et nécessaire à des fins de prévention de la corruption ou de sécurité ou si des intérêts économiques ou politiques de l'employeur pourraient être mis en danger.

2 L'extrait peut être demandé tous les cinq ans ou en tout temps pour de justes motifs.

3 L'employeur prend à sa charge les coûts des extraits.

Art. 94f Contrôle de loyauté
(art. 20*b* LPers)

1 Les candidats et les employés peuvent être soumis à un contrôle de loyauté aux conditions fixées à l'art. 11 de l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[32].

2 La liste des fonctions, les degrés de contrôle et la procédure du contrôle sont régis par l'OCSP.

30 RS **172.214.1**
31 RS **172.220.111.3**
32 RS …

3. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[33]

Art. 5, al. 1, let. b

[1] La remise d'informations classifiées à des personnes ou à des organes étrangers et l'accès à des informations militaires classifiées, à du matériel classifié ou à des installations militaires en Suisse par des personnes étrangères sont soumis aux dispositions régissant la protection de l'information, notamment:

b. l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes[34];

4. Ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée[35]

Art. 67 et annexe 30

Abrogés

Art. 70n, let. e

Les données destinées à être versées au FABIS sont collectées:

e. dans le système d'information sur le contrôle de sécurité relatif aux personnes visé à l'art. 45, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information[36], pour les données visées au ch. 2 de l'annexe 33*c*.

Annexe 23a, ch. 36

36. Degré de contrôle selon l'art. 5 ou 6 de l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[37], date de l'entrée en force de la décision visée à l'art. 24 OCSP et date de la répétition ordinaire du contrôle de sécurité relatif aux personnes visée à l'art. 26 OCSP.

Annexe 33c, ch. 2

2. Degré de contrôle selon les art. 10 à 14 OCSP[38], date de l'entrée en force de la décision visée à l'art. 24 OCSP et date de la répétition ordinaire du contrôle de sécurité relatif aux personnes visée à l'art. 26 OCSP concernant une personne disposant des droits d'accès.

33 RS **510.215**
34 RS **…**
35 RS **510.911**
36 RS **126**
37 RS **…**
38 RS **…**

Annexe 33d, ch. 2

2. Degré de contrôle selon l'art. 5 ou 6 OCSP[39], date de l'entrée en force de la décision visée à l'art. 24 OCSP et date de la répétition ordinaire du contrôle de sécurité relatif aux personnes visée à l'art. 26 OCSP concernant une personne disposant des droits d'accès.

5. Ordonnance du 22 novembre 2017 sur les obligations militaires[40]

Art. 11, al. 3, let. g

3 La séance d'information renseigne les participants notamment sur:

g. les contrôles de sécurité relatifs aux personnes conformément à l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[41] et les conséquences lors de situation personnelle particulière conformément à l'art. 33, al. 2.

Art. 16, al. 3, let. b

3 Une personne apte au service militaire est provisoirement affectée à une fonction de recrutement de l'armée si elle:

b. doit avoir passé avec succès un contrôle de sécurité relatif aux personnes, mais qu'aucune décision n'a encore été rendue conformément à l'art. 24 OCSP[42], ou que l'information prévue à l'art. 23, al. 2, OCSP n'a pas encore été communiquée.

Art. 21, al. 1, let. b, ch. 3

1 Sur demande conjointe de la personne concernée et du commandement compétent, les spécialistes, les sous-officiers supérieurs et les officiers supérieurs peuvent voir leurs obligations militaires prolongées si:

b. la personne concernée remplit les conditions suivantes:
   3. l'instance décisionnelle visée à l'art. 24 OCSP[43] laisse la personne concernée exercer l'activité,

Art. 72, al. 2, let. c

2 Pour une incorporation dans une fonction particulière ou pour une promotion à un grade supérieur, les conditions suivantes doivent être remplies:

39 RS **…**
40 RS **512.21**
41 RS **…**
42 RS **…**
43 RS **…**

c. l'instance décisionnelle visée à l'art. 24 OCSP[44] laisse la personne concernée exercer l'activité.

Art. 80, al. 2, let. c

2 Des soldats, appointés, sous-officiers et sous-officiers supérieurs peuvent être nommés officiers spécialistes si:

c. l'instance décisionnelle visée à l'art. 24 OCSP[45] laisse la personne concernée exercer l'activité.

6. Ordonnance du 10 décembre 2004 sur l'énergie nucléaire[46]

Art. 33a Contrôles de fiabilité

1 Les contrôles de fiabilité périodiques des personnes exerçant des fonctions essentielles pour la sécurité nucléaire et pour la sûreté de l'installation nucléaire sont régis par l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[47].

2 Les coûts du contrôle sont à la charge du détenteur de l'autorisation d'exploiter l'installation nucléaire.

44 RS **…**
45 RS **…**
46 RS **732.11**
47 RS …

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

du … Avant-projet du 25 juillet 2022

Le Conseil fédéral suisse,

vu les art. 73 et 84, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],

arrête:

Section 1 Dispositions générales

Art. 1 Objet et champ d'application
(art. 2, 49 et 73 LSI)

[1] La présente ordonnance régit:

a. la procédure de sécurité relative aux entreprises visée aux art. 49 à 73 LSI;

b. l'application aux sous-contractants de la procédure de sécurité relative aux entreprises;

c. l'organisation du service spécialisé chargé de la sécurité relative aux entreprises (service spécialisé PSE);

d. les mesures nécessaires pour garantir la sécurité des données du système d'information visé à l'art. 70 LSI;

e. le contrôle périodique, réalisé par un organe externe, du traitement des données personnelles.

[2] La présente ordonnance s'applique aux autorités et aux organisations visées à l'art. 2 LSI, sous réserve des art. 84, al. 3, LSI et 2, al. 2–5, de l'ordonnance du … sur la sécurité de l'information[2] (OSI).

Art. 2 Entreprises concernées
(art. 50 LSI)

[1] La présente ordonnance s'applique aux entreprises dont le siège est en Suisse.

RS .....
1 RS **128**
2 RS **…**

2 La procédure s'appliquant aux entreprises dont le siège est à l'étranger est régie par un traité international conformément à l'art. 87 LSI.

Art. 3 Autorité compétente
(art. 51, al. 2, LSI)

1 Le [département compétent] exploite le service spécialisé PSE.

2 Le service spécialisé PSE coordonne les activités internationales avec le service spécialisé de la Confédération pour la sécurité de l'information visé à l'art. 83 LSI.

Section 2 Ouverture de la procédure

Art. 4 Demande d'ouverture de la procédure
(art. 52 LSI)

1 Les personnes relevant du Conseil fédéral et ayant la compétence de demander l'ouverture de la procédure au service spécialisé PSE sont les suivantes:

a. les préposés à la sécurité de l'information des unités administratives visés à l'art. 37 OSI;

b. les préposés à la sécurité relative aux entreprises en application de l'art. 12, al. 2, let. c.

2 Les autorités visées à l'art. 2, al. 1, LSI annoncent au service spécialisé PSE qui, dans leur domaine de compétence, est chargé de demander l'ouverture de la procédure.

3 La demande comprend notamment:

a. une description des travaux de construction, de la livraison ou des prestations;

b. des explications quant au niveau de sensibilité du mandat;

c. des informations sur la procédure d'adjudication prévue.

Art. 5 Examen de la demande
(art. 53 LSI)

1 Avant d'ouvrir la procédure, le service spécialisé PSE consulte l'adjudicateur, l'autorité étrangère ou l'organisation internationale compétente.

2 Il ouvre la procédure dans tous les cas lorsque l'une des conditions suivantes est remplie:

a. le mandat sensible comprend le traitement d'informations classifiées SECRET ou l'administration, l'exploitation, la maintenance ou le contrôle de moyens informatiques relevant de la catégorie de sécurité PROTECTION TRÈS ÉLEVÉE;

b. le mandat sensible comprend le traitement d'informations classifiées CONFIDENTIEL qui concernent plusieurs autorités ou départements;

c. le mandat sensible comprend l'administration, l'exploitation, la maintenance ou le contrôle de moyens informatiques relevant de la catégorie de sécurité PROTECTION ÉLEVÉE engagés pour accomplir des tâches concernant plusieurs autorités ou départements;

d. l'entreprise se porte candidate pour un mandat pour lequel elle requiert un certificat international de sécurité au sens de l'art. 66 LSI.

3 Le service spécialisé PSE informe l'adjudicateur dès qu'il sait que l'examen de la demande durera plus de 30 jours.

Art. 6 Examen de la demande avec des autorités de sûreté étrangères
(art. 52, al. 3, LSI)

1 Lorsque des entreprises étrangères entrent en compte pour accomplir le mandat sensible, le service spécialisé PSE transmet la demande au service spécialisé de la Confédération pour la sécurité de l'information.

2 Le service spécialisé de la Confédération pour la sécurité de l'information vérifie avec l'autorité de sûreté étrangère compétente si les entreprises concernées disposent d'une déclaration de sécurité relative aux entreprises valable. Si tel n'est pas le cas, ils demandent l'ouverture de la procédure correspondante.

Art. 7 Définition des exigences en matière de sécurité
(art. 54 LSI)

1 Les exigences en matière de sécurité de l'information pour la procédure d'adjudication et la phase d'exécution du mandat sont définies dans l'OSI[3] et dans l'ordonnance du … sur les contrôle de sécurité relatifs aux personnes[4].

2 Si la procédure est ouverte à la demande d'une autorité étrangère ou d'une organisation internationale, les exigences en matière de sécurité de l'information sont régies par un traité international.

3 Le service spécialisé PSE fixe en accord avec l'adjudicateur les tâches sensibles que ce dernier doit mettre en œuvre pendant la procédure d'adjudication et la phase d'exécution du mandat.

4 L'adjudicateur demeure responsable de la coordination des processus de la procédure d'adjudication.

3 RS …
4 RS …

Section 3 Évaluation des entreprises

Art. 8 Indication des entreprises qualifiées
(art. 55 LSI)

1 L'adjudicateur peut annoncer au service spécialisé PSE jusqu'à cinq entreprises entrant en considération. Dans des cas exceptionnels motivés, il peut lui demander d'en ajouter à ce nombre.

2 Le service spécialisé PSE vérifie si les entreprises entrant en considération ont consenti à la procédure.

3 Il informe l'adjudicateur dès qu'il sait que l'examen de la qualification durera plus de 30 jours.

Art. 9 Collecte des données
(art. 56 LSI)

1 Le service spécialisé PSE collecte toutes les données pertinentes pour la sécurité nécessaires à l'évaluation de la qualification de l'entreprise, notamment:

a. les données sur les rapports de propriété et les modifications prévues telles que les fusions, les participations ou les acquisitions;

b. les données sur la composition de la direction de l'entreprise;

c. les données sur les liens d'intérêts des membres de la direction de l'entreprise;

d. les données sur la solvabilité et les éventuelles procédures de saisie ou de faillite;

e. les données sur le paiement des impôts et des cotisations sociales;

f. les références de précédentes procédures d'acquisition;

g. les données sur les relations de l'entreprise avec des États, des organisations étrangères ou sur d'autres relations de dépendance.

2 Elle collecte les données concernant les tâches visées à l'art. 6, al. 1, let. a, de la loi fédérale du 25 septembre 2015 sur le renseignement 2015[5] auprès du Service de renseignement de la Confédération.

3 Les entreprises doivent communiquer au service spécialisé PSE:

a. les documents et les données utiles au contrôle des faits visés à l'al. 1;

b. des informations véridiques.

Art. 10 Exclusion de la procédure
(art. 57 et 58 LSI)

1 L'adjudicateur et le service spécialisé PSE s'informent mutuellement dès qu'il existe des indices selon lesquels l'une des entreprises entrant en considération pourrait être exclue de la procédure d'adjudication.

5 RS **121**

2 Le service spécialisé PSE poursuit la procédure tant que l'adjudicateur n'exclut pas l'entreprise concernée de la procédure d'adjudication.

3 Si l'adjudicateur exclut l'entreprise, la procédure de sécurité relative à cette entreprise est classée.

Art. 11 Échange d'informations
(art. 57 et 58 LSI)

Lors de l'échange d'informations visé à l'art. 10, al. 1, l'adjudicateur et le service spécialisé PSE se mettent mutuellement à disposition toutes les informations et données utiles à l'examen de la qualification ou à la vérification des faits visée à l'art. 44 de la loi fédérale du 21 juin 2019 sur les marchés publics (LMP)[6], sous réserve des art. 70, al. 3, et 71, al. 1, let. a, LSI.

Section 4 Plan de sécurité

Art. 12 Préposé à la sécurité de l'entreprise

1 Les entreprises entrant en considération pour l'exécution du mandat annoncent un préposé à la sécurité et un suppléant adéquat au service spécialisé PSE. Il est un membre de la direction ou agit sur son mandat direct.

2 Le préposé à la sécurité accomplit les tâches suivantes:

a. il est l'interlocuteur du service spécialisé PSE pour toutes les questions de sécurité de l'information;

b. il veille à la mise en œuvre du plan de sécurité;

c. il demande l'ouverture de la procédure de sécurité relative aux entreprises pour le sous-contractant, pour autant que l'adjudicateur ait autorisé l'entreprise à lui octroyer un mandat sensible.

Art. 13 Communication de l'adjudication
(art. 59, al. 1, LSI)

1 L'adjudication est communiquée séparément pour chaque marché dépendant d'un contrat-cadre.

2 En communiquant l'adjudication, l'adjudicateur transmet au service spécialisé PSE les informations nécessaires à l'établissement du plan de sécurité.

Art. 14 Contenu et contrôle du plan de sécurité
(art. 59, al. 2 et 3, LSI)

1 Le service spécialisé PSE fixe les directives auxquelles doit répondre le plan de sécurité après inspection de l'entreprise.

6 RS **172.056.1**

[2] Le plan de sécurité définit les mesures organisationnelles, personnelles, techniques et physiques permettant de garantir une exécution du mandat sensible tenant compte des risques pour la sécurité.

[3] Si le plan de sécurité ne correspond pas aux directives du service spécialisé PSE, ce dernier accorde à l'entreprise un délai approprié afin de l'adapter.

[4] Le service spécialisé PSE informe l'adjudicateur dès qu'il sait que le contrôle du plan de sécurité durera plus de 30 jours.

Art. 15 Contrôles de sécurité relatifs aux personnes
(art. 60 LSI)

[1] Le service spécialisé PSE désigne les personnes de l'entreprise qui font l'objet d'un contrôle de sécurité relatif aux personnes.

[2] Il peut autoriser l'entreprise à engager la procédure du contrôle de sécurité de manière autonome.

Section 5 Déclaration de sécurité relative aux entreprises et répétition de la procédure

Art. 16 Établissement de la déclaration de sécurité relative aux entreprises
(art. 61 et 62 LSI)

La déclaration de sécurité relative aux entreprises indique l'activité sensible que l'entreprise est autorisée à accomplir.

Art. 17 Information de la part de l'entreprise
(art. 63, al. 2, LSI)

[1] Par changements dans le domaine de la sécurité, on entend notamment:

a. le changement des rapports de propriété ou des structures de l'entreprise;
b. le changement du site de l'entreprise;
c. le changement de la composition de la direction de l'entreprise;
d. le changement des liens d'intérêts des membres de la direction de l'entreprise;
e. le changement de la solvabilité et les éventuelles procédures de saisie ou de faillite;
f. les litiges de droit privé ou public et les procédures pénales;
g. les changements concernant l'utilisation des moyens informatiques;
h. l'engagement de collaborateurs amenés à participer aux activités sensibles;
i. les changements dans les relations de l'entreprise avec des États, des organisations étrangères ou dans d'autres relations de dépendance;
j. l'acceptation de mandats suscitant un conflit d'intérêts ou une relation de dépendance par rapport à un adjudicateur.

2 Par incidents dans le domaine de la sécurité, on entend notamment:

a. l'accès illicite à l'entreprise;

b. l'utilisation abusive des moyens informatiques de l'entreprise;

c. une attaque, aboutie ou non, visant les moyens informatiques de l'entreprise;

d. la découverte de vulnérabilités et de failles de sécurité;

e. l'ouverture de procédures pénales ou de procédures de poursuite pour dettes contre du personnel de l'entreprise participant à l'exécution du mandat sensible;

f. les perquisitions et les mises sous séquestre.

3 Lorsque des indices concrets donnent à penser qu'un incident visé à l'al. 2 puisse s'être produit, cela doit également être annoncé.

4 L'entreprise doit également annoncer les changements et les incidents visés aux al. 1 et 2 qui concernent les fournisseurs, s'ils ont un impact sur l'exécution du mandat sensible.

5 Elle informe le service spécialisé PSE dès qu'il est prévisible que la déclaration de sécurité de l'entreprise échoit alors que l'entreprise exécute un mandat sensible.

Art. 18 Devoirs de l'adjudicateur

1 Si, lors de la collaboration avec l'entreprise, l'adjudicateur constate un changement ou un incident dans le domaine de la sécurité visé à l'art. 17, il prend sans délai les mesures nécessaires et informe immédiatement le service spécialisé PSE.

2 L'adjudicateur informe en outre le service spécialisé PSE dans les cas suivants:

a. il a connaissance d'indices justifiant la révocation de l'adjudication au sens de l'art. 44 LMP dans le cadre de l'exécution du mandat sensible;

b. il entend procéder à un changement du mandat dans le domaine de la sécurité;

c. il entend confier un autre mandat à l'entreprise.

Art. 19 Certificat international de sécurité
(art. 66 LSI)

1 Le service spécialisé PSE perçoit un émolument de 100 francs pour l'établissement d'un certificat international de sécurité.

2 Un émolument correspondant au temps consacré est de plus perçu si l'établissement d'un certificat international de sécurité requiert au préalable une procédure de sécurité relative aux entreprises. Le tarif horaire est de 100 à 400 francs. Il dépend de l'urgence du mandat et de la fonction occupée par le personnel qui conduit la procédure. Pour le reste, c'est l'ordonnance générale du 8 septembre 2004 sur les émoluments[7] qui s'applique.

7 RS **172.041.1**

3 Le service spécialisé de la Confédération pour la sécurité de l'information et le service spécialisé PSE peuvent remettre, sur demande, une copie du certificat international de sécurité à l'autorité étrangère ou à l'organisation internationale.

Art. 20 Révocation de la déclaration de sécurité et retrait du mandat
(art. 67 LSI)

1 Si le service spécialisé PSE a connaissance d'indices laissant supposer qu'il existe un motif de révocation de la déclaration de sécurité, il fixe, après avoir consulté l'adjudicateur, un délai à l'entreprise pour qu'elle remédie aux manquements.

2 Si le mandat est retiré en raison de ladite révocation, l'adjudicateur veille immédiatement à ce que:

a. toutes les activités sensibles soient stoppées sans attendre et que les droits d'accès qui sont liés soient retirés, et que

b. toutes les informations classifiées, tous les moyens informatiques et le matériel soient saisis.

3 Dans les dix jours après avoir été informé de la révocation, l'adjudicateur confirme au service spécialisé PSE qu'il a exécuté les mesures visées à l'al. 2.

Art. 21 Répétition de la procédure
(art. 68 LSI)

1 Le service spécialisé PSE est compétent pour ouvrir la répétition de la procédure.

2 Si la déclaration de sécurité de l'entreprise échoit lorsque la procédure est répétée, sa validité est prolongée jusqu'à ce qu'une décision d'établir une nouvelle déclaration soit prononcée ou que la procédure de sécurité relative aux entreprises soit classée.

3 Si la déclaration de sécurité de l'entreprise n'est pas renouvelée ou si la procédure de sécurité relative aux entreprises est classée, l'art. 20 s'applique par analogie. L'art. 58, al. 3, LSI est réservé.

Section 6 Traitement des données personnelles

Art. 22 Système d'information sur la procédure de sécurité relative aux entreprises
(art. 70 LSI)

Les données personnelles et les données de l'entreprise enregistrées dans le système d'information sur la procédure de sécurité relative aux entreprises figurent dans l'annexe.

Art. 23 Contrôle périodique du traitement des données personnelles
(art. 73, let. e, LSI)

Le [département compétent] veille à ce qu'un organe indépendant du service spécialisé PSE contrôle au moins tous les cinq ans la licéité du traitement des données personnelles par les services concernés.

Section 7 Dispositions finales

Art. 24 Abrogation et modification d'autres actes

1 L'ordonnance du 29 août 1990 concernant la sauvegarde du secret[8] est abrogée.

2 L'ordonnance du 24 juin 2009 concernant les relations militaires internationales[9] est modifiée comme suit:

Art. 5, al. 1, let. d

1 La remise d'informations classifiées à des personnes ou à des organes étrangers et l'accès à des informations militaires classifiées, à du matériel classifié ou à des installations militaires en Suisse par des personnes étrangères sont soumis aux dispositions régissant la protection de l'information, notamment:

d. l'ordonnance du … sur la procédure de sécurité relative aux entreprises[10].

3 L'ordonnance du 16 août 2017 sur le renseignement[11] est modifiée comme suit:

Annexe 3, ch. 10.6

Le SRC peut communiquer des données personnelles aux autorités et services suisses mentionnés ci-après aux conditions énumérées à l'art. 60 LRens aux fins suivantes:

10. Département fédéral de la défense, de la protection de la population et des sports:

10.5. service spécialisé chargé des contrôles de sécurité relatifs aux personnes: pour l'exécution des contrôles,

10.6. service spécialisé chargé de la sécurité relative aux entreprises: pour l'exécution des procédures de sécurité relatives aux entreprises;

4 L'ordonnance du 21 novembre 2018 sur la sécurité militaire[12] est modifiée comme suit:

Art. 3, let. b

Abrogée

Art. 6, al. 2, let. e et f

2 Ses tâches sont les suivantes:

e. elle exécute un *controlling* spécialisé au sein du DDPS et de l'armée et réglemente l'obligation de s'annoncer;

8 RO …
9 RS **510.215**
10 RS …..
11 RS **121.1**
12 RS **513.61**

f. elle dispose d'un droit de contrôle au sein du DDPS et de l'armée;

5 L'ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée[13] est modifiée comme suit:

Art. 68 et annexe 31

Abrogés

Art. 25 Dispositions transitoires

L'ancien droit s'applique aux mandats octroyés avant l'entrée en vigueur de la présente ordonnance et aux procédures de sauvegarde du secret en cours à l'entrée en vigueur de la présente ordonnance.

Art. 26 Entrée en vigueur

La présente ordonnance entre en vigueur le … 2023.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ignazio Cassis
Le chancelier de la Confédération, Walter Thurnherr

13 RS **510.911**

Annexe
(art. 22)

Données du système d'information sur la procédure de sécurité relative aux entreprises

Données personnelles

1. Nom
2. Prénom
3. Adresse
4. Numéro d'assuré
5. Nationalité
6. Lieu d'origine
7. Nom et adresse de l'employeur
8. État civil
9. Lieu de naissance
10. Date de naissance
11. Date de naturalisation
12. Séjour en Suisse depuis
13. Nom et prénom de l'époux/l'épouse ou du/de la partenaire
14. Fonction
15. Nom et adresse de l'adjudicateur
16. Projet

Données concernant l'entreprise

Entreprise

17. Numéro de dossier
18. Nom
19. Adresse
20. Téléphone
21. Fax
22. E-mail
23. Adresse Internet

Préposé à la sécurité de l'entreprise

24. Civilité
25. Nom

26. Prénom
27. Sexe
28. E-mail

Données d'examen

29. Date de l'examen de la qualification
30. Code de la branche correspondant à l'activité économique de l'entreprise (code NOGA)
31. Visite (date, indication chronologique avec la note de texte)
32. Contrôle (date, indication chronologique avec la note de texte)
33. Déclaration de sécurité (date, établissement, révocation, remise)
34. Plan de sécurité (dans l'ordre chronologique)

Dossiers

35. Numéro d'exemplaire
36. Expéditeur
37. Date de dossier
38. Date d'expédition
39. Date de contrôle
40. Date de remise
41. Désignation

Mandats

42. Désignation (mandat principal)
43. Adjudicateur
44. Désignation (mandats)
45. Classification
46. Date de communication
47. Début de la durée de validité
48. Fin de la durée de validité
49. Désignation succincte (branche)
50. Code de la branche correspondant à l'activité économique de l'entreprise (code NOGA)