Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordonnance portant dernière mise en vigueur partielle de la loi du 18 décembre 2020 sur la sécurité de l'information

du …

Le Conseil fédéral suisse,

vu l'art. 92, al. 2, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],

arrête:

Article unique

Les dispositions non encore en vigueur de la loi du 18 décembre 2020 sur la sécurité de l'information entrent en vigueur le 1er janvier 2024.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

1 RS **128**; dispositions entrées en vigueur précédemment: RO **2022** 232; 503; 750

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)

du …

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 la loi fédérale du 17 mars 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA)[3],

vu la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[4],
vu l'art. 27, al. 5 et 6, de la loi du 24 mars 2000 sur le personnel de la Confédération[5],
vu l'art. 186 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS[6],

Art. 2 Champ d'application

[1] Les art. 24 et 25 LSI ainsi que la présente ordonnance s'appliquent:

1 RS **172.010.59**
2 RS **128**
3 RS **…**
4 RS **172.010**
5 RS **172.220.1**
6 RS **510.91**

a. 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)[7];

b. à l'armée.

2 L'application de la présente ordonnance aux unités de l'administration fédérale décentralisée visées à l'art. 2, al. 3, LOGA et aux organisations visées à l'art. 2, al. 4, LOGA est régie par l'art. 2, al. 2, let. b, et al. 3, de l'ordonnance du … sur la sécurité de l'information[8].

Art. 5 Systèmes IAM

1 Les organes de la Confédération suivants sont responsables des systèmes IAM de l'administration fédérale centrale ci-après:

a. le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF), pour:
   1. tous les systèmes IAM proposés comme services standard et tous les systèmes IAM relevant explicitement du secteur TNI de la ChF, y compris leur mise à la disposition des cantons et des communes ainsi que d'organisations et de personnes de droit public ou de droit privé conformément à l'art. 11, al. 3, LMETA,
   2. le système IAM des processus de soutien en matière de finances, d'acquisition, de gestion immobilière et de logistique, y compris le raccordement aux services d'informatique en nuage *(cloud)*;

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

c. le Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports, pour les systèmes IAM exploités par le Groupement Défense (Groupement D);

d. l'Administration fédérale des finances, pour le système IAM de gestion des systèmes d'assurances sociales du premier pilier et de soutien à leurs processus exploité par la Centrale de compensation;

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 Ils veillent à ce que le traitement des données personnelles figurant dans les systèmes IAM dont ils sont responsables soit contrôlé au moins tous les quatre ans par un organe externe.

7 RS **172.010.1**
8 RS …

3 Les organes suivants sont responsables des systèmes IAM ci-après:

a. le Groupement D, pour les systèmes IAM de l'armée;

b. les unités administratives concernées, pour les systèmes IAM des unités de l'administration fédérale décentralisée;

c. les organisations concernées, pour les systèmes IAM des organisations visées à l'art. 2, al. 4, LOGA.

4 Les autorités visées à l'art. 2, al. 1, let. a et c à e, LSI auxquelles la présente ordonnance s'applique en vertu de l'art. 84, al. 3, LSI déterminent quels organes de la Confédération sont responsables dans leur domaine.

5 La responsabilité du système en aval, et en particulier de l'accès à celui-ci, continue d'incomber au service technique responsable du système.

Art. 6, let. b, ch. 3

Les organes de la Confédération responsables des services d'annuaires extérieurs aux systèmes IAM sont:

b. pour les autres annuaires, les fournisseurs de prestations informatiques qui exploitent ces systèmes, à savoir:

3. le Groupement D,

Art. 7, let. b

Les personnes concernées font valoir leurs droits relatifs aux systèmes IAM et aux services d'annuaires auprès des organes suivants:

b. droit de rectification et de suppression:

1. auprès du service du personnel de leur unité administrative ou de leur organisation ou auprès du service chargé de gérer leurs données,

2. dans le cas de l'art. 9, let. b: auprès des organes responsables.

Art. 9, let. b

Les données concernant les personnes suivantes peuvent être traitées dans les systèmes IAM en plus des données au sens de l'art. 8:

b. particuliers et représentants d'organisations qui accèdent à des systèmes d'information mis à disposition par la Confédération ou, pour l'exécution du droit cantonal, par les cantons et les communes ainsi que par des organisations et personnes de droit public ou de droit privé, tels que les applications de cyberadministration.

Art. 11, al. 2 et 3

2 Aucun profilage au sens de l'art. 5, let. f et g, de la loi fédérale du 25 septembre 2020 sur la protection des données[9] 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. Fait exception le traitement de données biométriques par les systèmes IAM à des fins d'identification des personnes visées aux art. 8 et 9, let. a, en fonction du risque (art. 20, al. 2, LSI).

Art. 12, al. 4

4 Ils peuvent obtenir automatiquement les données de personnes externes auprès des systèmes IAM externes raccordés aux systèmes IAM de la Confédération conformément aux art. 21 à 24.

Art. 13, al. 4, let. a

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. 6 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[10], 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 en vertu de la présente ordonnance établit un règlement de traitement conformément à l'art. 6 OPDo[11].

2 Les systèmes IAM et les services d'annuaires qui ne sont pas gérés par des organes visés à l'art. 2 ou sur mandat de ces derniers peuvent être raccordés à des sys-

9 RS **235.1**
10 RS **235.11**
11 RS **235.11**

tèmes IAM ou des services d'annuaires internes à l'administration fédérale uniquement s'ils respectent les exigences minimales concernant la sécurité de l'information.

Art. 20 Système global IAM

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

Art. 21, phrase introductive et let. a

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 leurs exploitants s'engagent à respecter la présente ordonnance et les prescriptions qui en découlent ou, dans le cas des cantons, que ces derniers garantissent une sécurité de l'information au moins équivalente:

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

Art. 24, al. 1, let. a

1 Les systèmes IAM de la Confédération peuvent être raccordés en qualité de fournisseurs de données d'identification et d'authentification à un système IAM externe ou à une fédération d'identités externe aux conditions suivantes:

a. le raccordement sert à octroyer aux personnes visées aux art. 8 ou 9 un accès:

   1. à des systèmes d'information qui sont gérés par un exploitant externe sur mandat de la Confédération ou à des systèmes d'information tiers dont elles ont besoin pour exécuter leurs tâches légales, ou

   2. à des systèmes d'information qui sont mis à disposition, pour l'exécution du droit cantonal, par les cantons et les communes ainsi que par des organisations et personnes de droit public ou de droit privé, tels que les applications de cyberadministration.

II

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

III

La présente ordonnance entre en vigueur le 1er janvier 2024.

…

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
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. 4.

	Services d'annuaires	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	x
2. Prénoms*	x	x	x
3. Date de naissance		x	x
4. Lieu de naissance			x
5. Nationalité			x
6. Sexe		x	x
7. Civilité*	x	x	x
8. Titre*	x	x	x
9. Initiales*	x	x	x
10. Identificateurs personnels locaux	x	x	x
11. Profession*	x	x	x
12. Langue de correspondance*	x	x	x
13. 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	
14. Photo du visage	x	x	x
15. Numéro AVS	x	x	x
b. Données relatives au rapport avec l'employeur/le mandant			
1. Rapports de travail (interne/externe)*	x	x	
2. Informations relatives à l'unité d'organisation et aux postes de travail*	x	x	x
3. Futur rattachement à une unité d'organisation	x	x	
4. Catégorie de personnel		x	
5. Numéro personnel (y c. cantonal)	x	x	
6. Fonction*	x	x	
7. Poste*	x	x	

	Services d'annuaires	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
8. Identification du système d'information du personnel (source)	x	x	
9. Date d'entrée et date de départ	x	x	
10. Numéro de pièce d'identité et/ou de badge	x	x	x
c. Données de contact			
1. Lieu de travail et adresse postale professionnelle*	x	x	x
2. Adresse postale privée			x
3. Numéro du bureau*	x	x	
4. Composantes de l'adresse professionnelle* telles qu'adresse électronique*, numéro de téléphone*, numéro de fax*, adresse VoIP*	x	x	x
5. Composantes de l'adresse externe* (pour les collaborateurs et les mandataires*) ou de l'adresse privée	x	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	x
2. Composantes de l'adresse, numéros d'identification, etc.	x		
3. Langue du système des appareils, des raccordements, etc.	x	x	x
4. Clés publiques des certificats numériques*	x	x	x
5. Groupes d'autorisations	x	x	x
6. Noms pour la connexion aux systèmes informatiques	x	x	x
7. Mots de passe (sécurisés cryptographiquement)		x	x
8. Dernière ouverture de session		x	x
9. Échecs lors d'ouvertures de session		x	x
10. Statut (actif/passif)		x	x
11. Qualité de l'authentification		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			

	Services d'annuaires	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
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 la sécurité de l'information dans l'administration fédérale et l'armée

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

du …

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 et 3 LSI)

[1] La présente ordonnance s'applique:

a. au Conseil fédéral;

b. aux départements;

c. à la Chancellerie fédérale (ChF), aux secrétariats généraux, aux groupements et aux offices fédéraux;

d. à l'armée.

[2] Les dispositions suivantes de la LSI et de la présente ordonnance s'appliquent aux unités de l'administration fédérale décentralisée au sens de l'art. 2, al. 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[2] et aux organisations visées à l'art. 2, al. 4, LOGA:

RS .....

1 RS **128**

2 RS **172.010**

a. les art. 5, 6, 9, 10, 12 à 15, 20 à 23 et 27 à 73 LSI et les art. 16, 21, 24, 26, 32, 34 et 35 de la présente ordonnance, lorsqu'elles traitent des informations classifiées de la Confédération;

b. les art. 5, 6, 9, 10 et 16 à 73 LSI et les art. 10 à 12, 27 et 29 à 35 de la présente ordonnance, lorsqu'elles accèdent 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)[3] ou délèguent l'exploitation de leurs moyens informatiques à ces fournisseurs.

3 La ChF et les départements peuvent, dans leur domaine de compétence, soumettre les unités de l'administration fédérale décentralisée qui exercent constamment des activités sensibles à l'ensemble des dispositions de la LSI.

4 Les dispositions suivantes de la présente ordonnance s'appliquent aux cantons, sous réserve de l'art. 3, al. 2, LSI:

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

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

5 Le Groupement Défense assume pour l'armée les tâches, compétences et responsabilités que la présente ordonnance assigne aux unités administratives visées à l'art. 2, al. 1, let. c.

Section 2 Principes

Art. 3 Objectifs de sécurité

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

1 Les organisations visées à l'art. 2, al. 1, veillent ensemble à protéger leurs informations et leurs moyens informatiques en fonction du risque et à faire preuve d'une résilience appropriée face aux risques pour la sécurité de l'information.

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

3 Elles œuvrent à l'harmonisation, sur le plan national et international, des prescriptions et des niveaux en matière de sécurité afin de permettre l'interaction des autorités fédérales avec d'autres autorités de la Confédération ainsi qu'avec les cantons, les communes et les partenaires internationaux.

3 RS **172.010.58**

Art. 4 Responsabilité

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

[2] Elles assument toutes les tâches relevant de leur domaine de compétence que la présente ordonnance ou d'autres dispositions du 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 des informations ou utilisent des moyens informatiques de la Confédération sont responsables du respect des prescriptions en la matière.

[4] Les supérieurs de tous les échelons sont responsables de la formation liée à la sécurité de l'information de leurs collaborateurs et des militaires qui leur sont subordonnés en fonction de leurs tâches et s'assurent que ceux-ci respectent les prescriptions.

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 visées à l'art. 2, al. 1, let. c, 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 leur département et veillent à améliorer continuellement 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 obligations contractuelles
(art. 7, al. 1, LSI)

Les unités administratives visées à l'art. 2, al. 1, let. c, 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.

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

[1] Les unités administratives visées à l'art. 2, al. 1, let. c, dressent l'inventaire de leurs objets à protéger et le tiennent à jour.

[2] Par objets à protéger, on entend des objets indépendants, plusieurs objets de même nature ou des objets connexes:

a. les collections d'informations traitées dans le but d'exécuter un processus d'affaires de la Confédération;

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

3 L'inventaire mentionne:

a. le besoin de protection des objets à protéger;

b. les responsabilités liées aux objets à protéger;

c. la participation de tiers;

d. le résultat de l'évaluation des risques;

e. la mise en œuvre des mesures de sécurité et l'acceptation des risques qui ne peuvent pas être réduits de manière suffisante (risques résiduels);

f. les contrôles et les audits périodiques;

g. le cas échéant, l'utilisation partagée des objets à protéger.

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

1 Les unités administratives visées à l'art. 2, al. 1, let. c, évaluent en continu les risques pour leurs objets à protéger et assument 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, l'Office fédéral de la cybersécurité (OFCS), les unités administratives qui fournissent des prestations et les organes de sécurité de la Confédération informent les unités administratives visées à l'art. 2, al. 1, let. c, et les départements des menaces et vulnérabilités actuelles et des risques qui les concernent. Ils recommandent au besoin des mesures de limitation des risques.

3 Les unités administratives visées à l'art. 2, al. 1, let. c, 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 liste des exceptions
(art. 7, al. 1, LSI)

1 Si une unité administrative n'est pas en mesure d'observer une consigne contraignante pour elle d'une directive générale et abstraite visée à l'art. 85 LSI concernant un objet à protéger, elle doit obtenir une autorisation exceptionnelle du service ayant émis la directive.

2 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 ChF sur la transformation 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 visé à l'art. 4, al. 1, OTNI[4].

3 Les unités administratives visées à l'art. 2, al. 1, let. c, les départements et le service spécialisé de la Confédération pour la sécurité de l'information établissent la liste de leurs autorisations exceptionnelles en vigueur.

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

1 Les unités administratives visées à l'art. 2, al. 1, let. c, évaluent les risques pour leurs objets à protéger lors de la collaboration avec des tiers et leur dépendance vis-à-vis de 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)[5] collaborent à l'évaluation et mettent les informations nécessaires à disposition.

3 Le service spécialisé de la Confédération pour la sécurité de l'information, après avoir consulté l'OFCS et la Conférence des achats de la Confédération visée à l'art. 24 Org-OMP, émet des recommandations quant aux dispositions relatives à la sécurité de l'information devant figurer dans tous les contrats d'acquisition ou 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 visées à l'art. 2, al. 1, let. c, 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 établissent la liste des formations et des participants.

2 Les formations portent notamment sur:

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

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 interlocuteurs en cas de questions relatives à la sécurité de l'information;

e. les tâches de contrôle des supérieurs;

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

4 RS **172.010.58**
5 RS **172.056.15**

3 Les unités administratives visées à l'art. 2, al. 1, let. c, 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 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 visées à l'art. 2, al. 1, let. c, fixent en accord avec leurs fournisseurs de prestations la manière dont les incidents et les failles de sécurité sont annoncés et maîtrisés ou traités. Elles règlent la compétence d'ordonner des mesures immédiates.

2 Si un fournisseur de prestations découvre des incidents ou des failles de sécurité qui concernent une unité administrative à laquelle il fournit des prestations, il les lui annonce immédiatement et l'aide à les maîtriser ou à les traiter.

3 Le service spécialisé de la Confédération pour la sécurité de l'information et l'OFCS peuvent aider les unités administratives visées à l'art. 2, al. 1, let. c, et les départements à maîtriser les incidents de sécurité et à traiter les failles de sécurité.

4 Les unités administratives visées à l'art. 2, al. 1, let. c, 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 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 visé à 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 fixée 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 ou en déléguer la direction à l'OFCS avec son approbation. Ils ont dans ce cadre les tâches et les compétences suivantes:

a. ils peuvent obliger les unités administratives, les fournisseurs de prestations et les tiers concernés à leur communiquer toutes les informations nécessaires;

b. ils peuvent ordonner des mesures immédiates;

c. ils peuvent demander l'aide de spécialistes externes;

d. ils informent la direction des unités administratives concernées 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 ou l'OFCS rend la direction des opérations 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 visées à l'art. 2, al. 1, let. c, 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 des 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.

3 Le service spécialisé de la Confédération pour la sécurité de l'information recueille 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.

4 Il peut, en accord avec la ChF ou le département responsable, réaliser des audits ou en confier la réalisation 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 La ChF, les départements, l'OFCS et les fournisseurs internes de prestations informatiques visés à l'art. 9 OTNI[6] 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. Ils collectent les informations nécessaires auprès des unités administratives et de leurs fournisseurs de prestations.

2 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.

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

6 RS **172.010.58**

Art. 15 Directives relatives à la 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 toutes les organisations visées à l'art. 2, al. 1 et 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 et 14 LSI)

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

2 Si des informations sont regroupées dans un recueil, il faut réévaluer la classification.

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

1 Les unités administratives visées à l'art. 2, al. 1, let. c, et les départements fixent dans un catalogue de classification la manière de classifier les informations souvent traitées dans leur domaine de compétence et la durée de la classification.

2 Le service spécialisé de la Confédération pour la sécurité de l'information contrôle les catalogues de classification et émet si nécessaire une recommandation.

3 Après avoir consulté la Conférence des préposés à la sécurité de l'information, il fixe dans des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, la manière de classifier les informations souvent traitées par plusieurs départements et la durée de la classification.

4 Les personnes et les services suivants sont compétents pour classifier et déclassifier les informations qui ne figurent pas dans les catalogues de classification:

a. le personnel de la Confédération et les militaires;

b. les adjudicateurs, lorsque des informations de la Confédération sont traitées par des tiers.

5 Le personnel de la Confédération, les militaires et les tiers sont compétents pour marquer formellement les supports d'information qu'ils établissent ou les informations qu'ils communiquent oralement.

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

1 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 processus de conduite important de l'armée est 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 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.

2 Sont également classifiées «interne» les informations permettant de tirer des conclusions sur des informations classifiées «confidentiel» ou «secret» si elles sont portées à la connaissance d'une personne non autorisée.

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 et 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 d'opérations des autorités de poursuite pénale, du SRC, de l'armée ou des autres organes de sécurité de la Confédération conforme aux objectifs est compromise;

c. les moyens et les méthodes opérationnels des services de renseignement et des autorités de poursuite pénale de la Confédération ou l'identité de sources et de 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 rompues;

h. la position de la Suisse est temporairement 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 troupe de l'armée sont annihilées durant des jours ou entravées 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. des 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 durant des semaines dans une mesure particulièrement importante 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 des 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 des 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 toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent le traitement des informations classifiées et fixe les exigences de sécurité minimales en matière d'organisation, de personnel et de construction, de même que sur le plan technique. Il tient compte pour ce faire des normes internationales en la matière.

2 Il consulte au préalable les services suivants:

a. l'OFCS;

b. le service cryptographique de l'armée;

c. les services ayant la compétence d'acheter des biens cryptologiques visés à l'art. 10, al. 1, let. d, Org-OMP[7];

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

3 La ChF règle le traitement des affaires classifiées du Conseil fédéral.

4 Le traitement des informations classifiées provenant de l'étranger est régi par les prescriptions correspondant à l'échelon de classification étranger. Les dispositions 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 fermé d'utilisateurs clairement identifiable, les personnes suivantes peuvent, après avoir consulté le service spécialisé de la Confédération pour la sécurité de l'information, arrêter 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 et de la sécurité des frontières.

2 Les personnes visées à l'al. 1 veillent à ce qu'il soit clairement indiqué sur les supports d'information que les prescriptions de traitement simplifié s'appliquent.

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

1 Les moyens informatiques sont certifiés sur le plan de la sécurité avant leur mise en exploitation si cela est nécessaire à la collaboration nationale ou internationale.

2 La certification de sécurité est effectuée par le service spécialisé de la Confédération pour la sécurité de l'information, après consultation du service cryptographique de l'armée et des services ayant la compétence d'acheter des biens cryptologiques visés à l'art. 10, al. 1, let. d, Org-OMP[8].

3 Elle atteste que le moyen informatique remplit les exigences minimales correspondant à l'échelon de classification concerné et que les risques résiduels sont acceptables en fonction de l'état des connaissances techniques.

7 RS **172.056.15**
8 RS **172.056.15**

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

5 Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) fixe la procédure relative à la certification de sécurité en tenant compte des normes internationales en la matière.

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

1 Quiconque constate que des informations classifiées ont été compromises, ont disparu ou qu'il en a été fait une utilisation abusive ou encore que des informations n'ont pas été classifiées alors qu'elles auraient dû l'être ou qu'elles ont été classifiées de manière erronée prend les mesures de protection nécessaires.

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

Art. 25 Contrôle du besoin de protection et cercle des 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 les examinent 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 dispositions 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 Les archives cessent d'être classifiées une fois que le délai de protection est échu. La prolongation du délai de protection est régie par l'art. 14 de l'ordonnance du 8 septembre 1999 sur l'archivage[9].

Section 5 Sécurité des moyens informatiques

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

1 Les unités administratives visées à l'art. 2, al. 1, let. c, doivent pouvoir démontrer le besoin de protection de leurs objets à protéger et leur importance pour la gestion de la continuité des activités.

9 RS **152.11**

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

3 Elles démontrent les risques résiduels.

4 Les responsables de la sécurité de l'information (art. 36) décident si les risques résiduels sont 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 ou la situation de l'organisation.

6 Les unités administratives visées à l'art. 2, al. 1, let. c, contrôlent chaque année si un changement important a eu lieu.

7 Le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent la procédure de sécurité visée à l'art. 16 LSI.

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 visé à l'art. 19 ou un dommage de 50 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 visé à l'art. 20 ou un dommage supérieur à 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 toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences minimales pour les catégories de sécurité visées à l'art. 17 LSI.

2 Il tient compte des exigences concernant la sécurité des données personnelles 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 applicables aux moyens informatiques suivants doit être contrôlée avant leur mise en exploitation, ainsi que durant l'exploitation en cas de changements importants des risques, mais au moins tous les cinq ans:

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 La ChF et les départements 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 visées à l'art. 2, al. 1, let. c, veillent à ce que les responsabilités en matière de sécurité de l'information au niveau opérationnel soient consignées 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 visées à l'art. 2, al. 1, let. c, des départements et du service spécialisé de la Confédération pour la sécurité de l'information les informations dont ceux-ci ont besoin pour assurer la sécurité de l'information.

3 Ils veillent à disposer, sur le plan du personnel et des finances, des capacités et compétences nécessaires à la détection précoce, à l'analyse technique et à la maîtrise ou au traitement des incidents et des failles de sécurité qui les concernent ou qui concernent les bénéficiaires de leurs prestations dans le cadre des accords et conventions visés à l'al. 1.

4 Ils surveillent l'utilisation de leur infrastructure informatique et l'examinent régulièrement à la recherche de menaces et de vulnérabilités techniques. Ils peuvent charger des tiers d'effectuer cet examen.

5 Le traitement des données personnelles dans le cadre de la surveillance et de l'examen visés à l'al. 4 est régi par l'ordonnance du 22 février 2012 sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération[10].

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 peut émettre des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences techniques minimales auxquelles doit satisfaire la vérification, en fonction 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

10 RS **172.010.442**

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[11].

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 visées à l'art. 2, al. 1, let. c, veillent à ce que les collaborateurs soumis à un contrôle de sécurité relatif aux personnes visé dans l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes (OCSP)[12] soient sensibilisés chaque année à l'activité sensible déterminante et aux risques qui y sont liés.

2 Ces collaborateurs sont tenus d'annoncer à leur employeur les circonstances privées ou professionnelles susceptibles de les empêcher d'exercer leur activité sensible dans le respect des prescriptions.

Art. 33 Soupçon 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, la ChF et les départements transmettent le dossier de l'enquête et les procès-verbaux d'audition 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 de protection physique
(art. 22 et 85 LSI)

1 Après avoir consulté les organes de l'administration fédérale et de l'armée responsables de la sécurité des objets, le service spécialisé de la Confédération pour la sécurité de l'information peut émettre des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences minimales de 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;

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

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

1 Les unités administratives visées à l'art. 2, al. 1, let. c, peuvent établir les zones de sécurité suivantes:

11 RS **172.010.59**
12 RS ...

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 Ces locaux et ces espaces ne sont considérés comme des zones de sécurité que si l'organe de l'administration fédérale ou de l'armée responsable de la sécurité des objets 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 de l'administration fédérale et de l'armée responsables de la sécurité des objets, le service spécialisé de la Confédération pour la sécurité de l'information émet des directives générales et abstraites s'appliquant à toutes les organisations visées à l'art. 2, al. 1 à 3, qui concernent les exigences en matière de sécurité pour les zones de sécurité et leur établissement.

4 Les unités administratives visées à l'art. 2, al. 1, let. c, peuvent prendre des mesures aux alentours des zones de sécurité afin d'identifier les actes d'espionnage électromagnétique et de s'en protéger.

Section 7 Organisation de sécurité

Art. 36 Responsables de la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c

(art. 7, al. 1, LSI)

1 Le chancelier de la Confédération, les secrétaires généraux et les directeurs des unités administratives visées à l'art. 2, al. 1, let. c, sont responsables de la sécurité de l'information dans leur domaine de compétence.

2 Ils peuvent déléguer la responsabilité en matière de sécurité de l'information 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 l'information des unités administratives visées à l'art. 2, al. 1, let. c, 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 qui ont une influence déterminante sur 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 la formation et la 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 administratives visées à l'art. 2, al. 1, let. c, confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 37 et s'assurent:

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

b. qu'ils ne se voient confier aucune tâche susceptible d'entraîner un conflit d'intérêts avec les tâches visées à l'art. 37.

Art. 37 Préposés à la sécurité de l'information des unités administratives visées à l'art. 2, al. 1, let. c

(art. 7, al. 1, LSI)

1 Les unités administratives visées à l'art. 2, al. 1, let. c, désignent un ou plusieurs préposés à la sécurité de l'information et leurs suppléants.

2 Les préposés à la sécurité de l'information accomplissent les tâches et assument les compétences suivantes:

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

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

c. ils sont les interlocuteurs principaux de l'unité administrative pour les questions de sécurité de l'information et conseillent les personnes et les services responsables et les aident à accomplir leurs tâches et à exécuter leurs obligations 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 proposent au responsable de la sécurité de l'information l'organisation de mesures de formation et de sensibilisation supplémentaires;

g. ils demandent l'ouverture de la procédure de sécurité relative aux entreprises visée à l'art. 4 de l'ordonnance du ... sur la procédure de sécurité relative aux entreprises[13];

h. ils coordonnent la maîtrise des incidents de sécurité et le traitement des failles de sécurité dans l'unité administrative et auprès des tiers mandatés;

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

13 RS **128.xxx**

j. ils contrôlent périodiquement la présence de supports d'information classifiés «secret» et la sécurité de ceux-ci dans leur domaine de compétence;

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

l. ils rendent compte chaque semestre au responsable de la sécurité de l'information 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[14].

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

3 Les préposés à la sécurité de l'information assument les tâches visées à l'art. 37, al. 2, pour les services standard et informent l'administration fédérale et l'armée des risques pour la sécurité de l'information.

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

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

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 visés à l'art. 37;

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

c. ils surveillent le SMSI des unités administratives visées à l'art. 2, al. 1, let. c, et relèvent les indicateurs nécessaires à cette fin;

d. ils fixent des objectifs annuels de sécurité pour les unités administratives visées à l'art. 2, al. 1, let. c, et vérifient qu'elles les ont atteints;

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

f. ils confient des tâches à leurs préposés à la sécurité de l'information visés à l'art. 40 et s'assurent:

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

14 RS **172.010.58**

2. qu'ils ne se voient confier aucune tâche susceptible d'entraîner un conflit d'intérêts avec les tâches visées à l'art. 40.

3 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.

4 Pour autant que le chef de département n'en décide pas autrement, la sécurité de l'information dans le département relève de la responsabilité du secrétaire général qui agit sous son mandat.

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 tâches 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 de l'information et lui proposent des mesures à prendre;

c. ils coordonnent la maîtrise des incidents de sécurité et le traitement des failles de sécurité impliquant plusieurs unités administratives visées à l'art. 2, al. 1, let. c;

d. ils établissent la planification annuelle de contrôle et d'audit du département et la soumettent au responsable de la sécurité de l'information pour approbation;

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

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

g. ils vérifient périodiquement et en cas de changement ou de départ d'un membre du Conseil fédéral ou du chancelier de la Confédération que tous les supports d'information classifiés «secret» sont présents et au complet;

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

Art. 41 Préposé à la sécurité de l'information du Conseil fédéral
(art. 81, al. 1, let. a, LSI)

Le DDPS nomme le préposé à la sécurité de l'information du Conseil fédéral et son suppléant.

Art. 42 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 et assume les compétences suivantes pour l'administration fédérale et l'armée:

a. il élabore des stratégies sur des thèmes pertinents pour la sécurité;

b. il peut demander des informations, émettre des avis et proposer des modifications concernant des projets dans le domaine de la sécurité;

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

d. il prépare des modèles et des aides;

e. il aide les préposés à la sécurité de l'information à contrôler les supports d'information classifiés «secret»;

f. il assume la responsabilité des solutions de sécurité certifiées utilisées dans toute l'administration fédérale et l'armée.

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

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

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

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

c. il exécute les contrôles prévus dans les traités internationaux ou les fait exécuter;

d. il représente la Suisse dans des organismes internationaux spécialisés;

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

f. il délivre les certificats de sécurité visés à l'art. 30 OCSP[15].

4 Il fait partie du Secrétariat d'État à la politique de sécurité du DDPS.

Art. 43 Tâches et compétences de l'OFCS
(art. 7, al. 1, et 84, al. 1, LSI)

1 L'OFCS accomplit les tâches et assume les compétences suivantes:

a. il conseille l'administration fédérale et l'armée ainsi que les organes de sécurité visés aux art. 81 à 83 LSI pour toutes les questions liées à la sécurité technique de l'information;

15 RS ...

b. il siège à la Conférence des préposés à la sécurité de l'information visée à l'art. 82 LSI;

c. il peut, afin d'évaluer et d'améliorer la situation en matière de sécurité technique de l'information de la Confédération, rechercher des menaces et des vulnérabilités techniques sur Internet ou, en concertation avec les responsables de la sécurité de l'information et les fournisseurs de prestations, dans l'infrastructure informatique de l'administration fédérale; il peut en charger d'autres services de l'administration fédérale ou des tiers.

2 Il coordonne ses activités avec celles du service spécialisé de la Confédération pour la sécurité de l'information.

Section 8 Coûts et évaluation

Art. 44 Coûts

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

2 Les unités administratives visées à l'art. 2, al. 1, let. c, veillent à ce que les coûts soient 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 de 100 francs pour établir et envoyer les certificats de sécurité visés à art. 30 OCSP[16] pour les personnes qui n'exercent pas d'activité sensible de la Confédération.

Art. 45 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 au sein de la Confédération.

Section 9 Traitement des informations et des données personnelles

Art. 46 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 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 des organisations nationales, internationales ou étrangères de droit public ou privé, dans la mesure où:

16 RS **128.xxx**

a. cela est utile à la sécurité de l'information;

b. aucune obligation de maintien du secret légale ou contractuelle n'est violée;

c. les dispositions de la législation fédérale en matière de protection des données sont respectées, et

d. ces organisations assument des tâches légales dans le domaine de la sécurité de l'information qui correspondent à celles de l'autorité ou de l'organisation qui communique les informations.

3 Pour autant que cela soit nécessaire pour maîtriser un incident de sécurité ou traiter une faille de sécurité, ils peuvent également traiter et échanger des données sensibles visées à l'art. 5, let. c, de la loi fédérale du 25 septembre 2020 sur la protection des données[17] de personnes qui ont ou auraient participé à l'incident ou à la faille de sécurité ou qui sont ou seraient concernées par l'incident ou la faille de sécurité.

4 Si, lors d'un incident de sécurité survenant au sein de la Confédération ou auprès de tiers collaborant avec la Confédération, des informations de la Confédération sont dérobées et publiées sur Internet, ils peuvent télécharger et analyser ces informations afin d'évaluer l'atteinte portée à la Confédération et de prendre les mesures de protection nécessaires. Ils ne peuvent pas traiter les données qui ne sont pas utiles à cette évaluation.

5 Ils peuvent appliquer ces mesures en cas de soupçon concret.

Art. 47 Application SMSI

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

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. 46, 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. 48 Services électroniques de formulaire

1 Le service spécialisé de la Confédération pour la sécurité de l'information peut exploiter des services électroniques de formulaire et les relier à son application SMSI dans les buts suivants:

a. gérer les déplacements visés à l'art. 42, al. 3, let. e;

b. établir et envoyer les certificats internationaux de sécurité visés à l'art. 30 OCSP[18];

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

17 RS **235.1**
18 RS **128.xxx**

2 Les données personnelles figurant dans l'annexe 1 peuvent être traitées à l'aide des services de formulaire 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 des 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 formulaire visés à l'al. 3, elles peuvent traiter les données personnelles, y compris les données sensibles visées à l'art. 46, al. 3, qui sont nécessaires à la maîtrise des incidents de sécurité et au traitement des failles de sécurité. Elles doivent effacer ces données du service de formulaire immédiatement après leur communication. Elles peuvent provisoirement les enregistrer avant l'envoi durant 24 heures au plus.

Section 10 Dispositions finales

Art. 49 Dispositions d'exécution particulières

Le DDPS peut déclarer contraignantes pour les cantons des versions datées des directives générales et abstraites visées aux art. 17, al. 3, 21, al. 1, 29, al. 1 et 34, al. 1.

Art. 50 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées dans l'annexe 2.

Art. 51 Dispositions transitoires

1 Les directives en matière de sécurité informatique émises par le Centre national pour la cybersécurité (NCSC) et les exceptions qu'il a autorisées avant l'entrée en vigueur de la présente ordonnance conservent leur validité durant trois 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 ou le NCSC prend les décisions concernant les changements des directives et des exceptions autorisées émises par le NCSC avant l'entrée en vigueur de la présente ordonnance.

3 Les directives en matière de protection de l'information 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 deux ans au plus après l'entrée en vigueur de la présente ordonnance.

4 Les unités administratives visées à l'art. 2, al. 1, let. c, mettent en place leur SMSI (art. 5) dans les trois ans après l'entrée en vigueur de la présente ordonnance.

5 Les catalogues de classification (art. 17) doivent être établis au plus tard un an après l'entrée en vigueur de la présente ordonnance.

6 L'OFCS assume jusqu'au 30 juin 2025 les tâches et les compétences du service spécialisé de la Confédération pour la sécurité de l'information visées aux art. 9, al. 2 et 3, 11, al. 3 et 4, 12, al. 3 et 6 à 8, 15, 27, al. 7, 29, al. 1, et 31, al. 1.

7 Les directives émises par l'OFCS en application de l'al. 6 conservent leur validité durant deux ans au plus après l'entrée en vigueur de la présente ordonnance.

Art. 52 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2024.

…

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Annexe 1
(art. 48)

Traitement des données à l'aide de services électroniques de formulaire

Les données personnelles suivantes peuvent être traitées à l'aide des services de formulaire ci-dessous:

1. Service de formulaire pour le but visé à l'art. 48, al. 1, let. a
   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 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 coordonnées 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 suivies d'un astérisque (*) sont communiquées à l'autorité de sécurité étrangère.

2. Service de formulaire pour le but visé à l'art. 48, al. 1, let. b,

   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 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 et autres coordonnées, en particulier électroniques, de la personne de référence
      5. Motif de l'établissement du certificat

3. Service de formulaire pour le but visé à l'art. 48, al. 1, let. c

   a. Données relatives à l'entreprise:
      1. Nom complet*
      2. Forme juridique*
      3. Numéro d'identification de l'entreprise
      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 et autres coordonnées, en particulier électroniques, de la personne de référence

   b. Données concernant la déclaration de sécurité relative aux entreprises:
      1. Date d'établissement et durée de validité*

2. Champ d'application et charges*
3. Échelon de classification ou catégorie de sécurité le plus élevé autorisé*

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

4. Service de formulaire visé à l'art. 48, al. 3

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 2
(art. 50)

Abrogation et modification d'autres actes

I

L'ordonnance du 27 mai 2020 sur les cyberrisques[19] est abrogée.

II

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN[20]

Art. 9, al. 7

7 Les autorités mentionnées à l'al. 1 veillent au respect des dispositions relatives à la protection des données et à la sécurité de l'information.

Art. 13, al. 1, let. b

1 Pour garantir la sécurité des données, sont applicables:

b. l'ordonnance du ... sur la sécurité de l'information[21].

2. Ordonnance du 16 août 2017 sur les systèmes d'information et les systèmes de stockage de données du Service de renseignement de la Confédération[22]

Art. 13, al. 1, let. b et c

1 Pour assurer la sécurité des données s'appliquent:

b. l'ordonnance du ... sur la sécurité de l'information[23].

c. *abrogée*

19 RO **2020** 2107; **2020** 5871; **2021** 132
20 RS **120.52**
21 RS **...**
22 RS **121.2**
23 RS **...**

Art. 15 Transmission de données hors du réseau SiLAN

La transmission de données hors du réseau SiLAN est régie par l'ordonnance du ... sur la sécurité de l'information[24].

3. Ordonnance du 10 novembre 2021 sur le système d'entrée et de sortie[25]

Art. 20, al. 2, let. b

[2] S'agissant des autorités fédérales, la sécurité des données est régie en outre par:

b. l'ordonnance du ... sur la sécurité de l'information[26].

4. Ordonnance 3 du 11 août 1999 sur l'asile[27]

Art. 12, let. b

La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[28];

5. Ordonnance VIS du 18 décembre 2013[29]

Art. 34, let. b

La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[30];

6. Ordonnance SYMIC du 12 avril 2006[31]

Art. 17, titre et al. 1, let. b

Sécurité des données et de l'information

[1] La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[32].

24 RS **...**
25 RS **142.206**
26 RS **...**
27 RS **142.314**
28 RS **...**
29 RS **142.512**
30 RS **...**
31 RS **142.513**
32 RS **...**

7. Ordonnance du 5 décembre 2008 concernant la gestion de l'immobilier et la logistique de la Confédération[33]

Art. 41, al. 2, let. b

[2] L'OFCL édicte des instructions pour le domaine de la logistique. Sont réservées:

b. l'ordonnance du ... sur la sécurité de l'information[34].

8. Ordonnance GEVER du 3 avril 2019[35]

Art. 11 Traitement d'informations classifiées

[1] Les informations classifiées CONFIDENTIEL en vertu de l'art. 19 de l'ordonnance du ... sur la sécurité de l'information (OSI)[36] sont chiffrées dans les systèmes de gestion des affaires.

[2] Les informations classifiées SECRET en vertu de l'art. 20 OSI ne doivent pas être traitées dans les systèmes de gestion des affaires.

9. Ordonnance du 22 février 2012 sur le traitement des données personnelles et des données des personnes morales lors de l'utilisation de l'infrastructure électronique de la Confédération[37]

Art. 3 Conservation sécurisée des données

Les données doivent être conservées de manière sécurisée conformément aux dispositions de l'ordonnance du ... sur la sécurité de l'information[38].

10. Ordonnance SIVIP du 18 novembre 2015[39]

Titre de la section 3

Section 3 Protection des données et sécurité de l'information

Art. 11, al. 1, phrase introductive et let. b

[1] La sécurité des données et la sécurité de l'information sont régies par:

b. l'ordonnance du ... sur la sécurité de l'information[40].

33 RS **172.010.21**
34 RS **...**
35 RS **172.010.441**
36 RS **...**
37 RS **172.010.442**
38 RS **...**
39 RS **172.211.21**
40 RS **...**

11. Ordonnance Web-DFAE du 5 novembre 2014[41]

Titre de la section 3

Section 3 Protection des données et sécurité de l'information

Art. 12, al. 1, phrase introductive et let. b

1 La sécurité des données et la sécurité de l'information sont régies par:

b. l'ordonnance du ... sur la sécurité de l'information[42].

12. Ordonnance du 17 août 2016 sur le système d'information E-VERA[43]

Art. 14, al. 1, phrase introductive et let. b

1 La sécurité des données et la sécurité de l'information sont régies par:

b. l'ordonnance du ... sur la sécurité de l'information[44];

13. Ordonnance du 7 novembre 2012 sur la protection extraprocédurale des témoins[45]

Art. 4, al. 2

2 Pour le reste, les dispositions de l'ordonnance du … sur la sécurité de l'information[46] s'appliquent.

Art. 12, al. 4

4 Le traitement des données par le destinataire est régi par les dispositions de l'ordonnance du … sur la sécurité de l'information[47].

Art. 15, al. 1, let. b

1 La sécurité des données est garantie par:

b. l'ordonnance du … sur la sécurité de l'information[48];

41 RS **172.220.111.42**
42 RS ...
43 RS **235.22**
44 RS **...**
45 RS **312.21**
46 RS **...**
47 RS ...
48 RS **...**

14. Ordonnance du 20 septembre 2013 relative au système d'information en matière pénale de l'Office fédéral de la douane et de la sécurité des frontières[49]

Art. 18, al. 1

[1] La garantie de la sécurité des données est régie par les art. 1 à 4 et 6 de l'OPDo[50] et par les dispositions de l'ordonnance du ... sur la sécurité de l'information[51].

15. Ordonnance du 19 octobre 2022 sur le casier judiciaire[52]

Art. 11, al. 1, let. b

[1] La sécurité des données est régie notamment par:

b. l'ordonnance du … sur la sécurité des données[53].

16. Ordonnance GPDA du 23 septembre 2016[54]

Titre précédant l'art. 13

Section 6 Exactitude des données, sécurité de l'information, durée de conservation, archivage et statistique

Art. 14, titre et al. 1, phrase introductive et let. b

Sécurité des données et de l'information

[1] La sécurité des données et de l'information est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[55];

17. Ordonnance SNE du 15 octobre 2008[56]

Art. 26, let. b

La sécurité des données est garantie par:

49 RS **313.041**
50 RS **235.11**
51 RS ...
52 RS **331**
53 RS **...**
54 RS **351.12**
55 RS **...**
56 RS **360.2**

b. l'ordonnance du ... sur la sécurité de l'information (OSI)[57].

Art. 29n, al. 1, phrase introductive et let. b

1 La sécurité des données est garantie par:

b. l'OSI[58].

Art. 29w, al. 1, phrase introductive et let. b

1 La sécurité des données est garantie par:

b. l'OSI[59].

18. Ordonnance RIPOL du 26 octobre 2016[60]

Remplacement d'une expression

Dans tout l'acte, «sécurité informatique» *est remplacé par* «sécurité de l'information».

Art. 9, al. 5

5 La communication de données doit être assortie d'une remarque précisant que les renseignements doivent être traités de manière interne conformément à l'ordonnance du ... sur la sécurité de l'information[61] et qu'ils ne peuvent être transmis à d'autres intéressés.

Art. 14, al. 2, let. b

2 La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[62].

19. Ordonnance IPAS du 15 octobre 2008[63]

Art. 12, let. b

La sécurité des données est garantie par:

b. l'ordonnance du ... sur la sécurité de l'information[64].

57 RS ...
58 RS ...
59 RS ...
60 RS **361.0**
61 RS ...
62 RS ...
63 RS **361.2**
64 RS ...

20. Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques[65]

Art. 14, let. b

La sécurité des données est garantie par:

b. l'ordonnance du ... sur la sécurité de l'information[66].

21. Ordonnance du 15 octobre 2008 sur l'index national de police[67]

Art. 12, al. 1, let. b

1 La sécurité des données est garantie par:

b. l'ordonnance du ... sur la sécurité de l'information[68].

22. Ordonnance N-SIS du 8 mars 2013[69]

Art. 53, al. 1, let. b

1 La sécurité des données se fonde sur:

b. l'ordonnance du ... sur la sécurité de l'information[70];

23. Ordonnance du 3 décembre 2004 sur les profils d'ADN[71]

Art. 19, al. 1, let. b

1 La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[72].

24. Ordonnance du 15 septembre 2017 sur les systèmes d'information dans le domaine de la formation professionnelle et des hautes écoles[73]

Art. 21, al. 1, phrase introductive et let. b

1 La sécurité des données et de l'information est régie par:

65 RS **361.3**
66 RS ...
67 RS **361.4**
68 RS ...
69 RS **362.0**
70 RS **...**
71 RS **363.1**
72 RS **...**
73 RS **412.108.1**

b. l'ordonnance du ... sur la sécurité de l'information[74].

25. Ordonnance du 30 juin 1993 concernant l'organisation de la statistique fédérale[75]

Art. 10, al. 2

2 La sécurité des données personnelles et des données des personnes morales est assurée par les dispositions spécifiques de la loi, ainsi que par celles de l'ordonnance du ... sur la sécurité de l'information[76] et de l'OPDo. L'OPDo s'applique par analogie pour les personnes morales.

26. Ordonnance du 9 juin 2017 sur le Registre fédéral des bâtiments et des logements[77]

Art. 18, al. 1, let. b

1 La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[78].

27. Ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements[79]

Art. 15, al. 1, let. b

1 La sécurité des données est régie par:

b. l'ordonnance du ... sur la sécurité de l'information[80].

28. Ordonnance du 20 avril 2016 sur le contrôle de l'origine licite des produits de la pêche maritime importés[81]

Art. 24 Sécurité de l'information

Les mesures pour garantir la sécurité de l'information sont régies par l'ordonnance du ... sur la sécurité de l'information[82].

74 RS **...**
75 RS **431.011**
76 RS **...**
77 RS **431.841**
78 RS ...
79 RS **431.903**
80 RS ...
81 RS **453.2**
82 RS ...

29. Ordonnance animex-ch du 1er septembre 2010[83]

Remplacement d'une expression

Dans tout l'acte, «sécurité informatique» *est remplacé par* «sécurité de l'information».

Art. 20, al. 1

[1] Les mesures pour garantir la sécurité de l'information sont régies par l'ordonnance du ... sur la sécurité de l'information[84].

30. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[85]

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;

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 18 décembre 2020 sur la sécurité de l'information[86];

b. l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes[87];

c. l'ordonnance du … sur la sécurité de l'information[88];

d. l'ordonnance du … sur la procédure de sécurité relative aux entreprises[89].

83 RS **455.61**
84 RS ...
85 RS **510.215**
86 RS **128**
87 RS **...**
88 RS **...**
89 RS **...**

31. Ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio[90]

Art. 7, al. 1

1 Les résultats des mandats d'exploration radio sont classifiés conformément à l'ordonnance du … sur la sécurité de l'information[91].

32. Ordonnance du 2 juillet 2008 sur les armes[92]

Art. 66c, al. 1, let. b

1 La sécurité des données est garantie conformément à:

b. l'ordonnance du … sur la sécurité de l'information[93].

33. Ordonnance du 12 août 2015 sur le bureau de notification pour les médicaments vitaux à usage humain[94]

Art. 8, al. 2, let. b

2 Sont en outre applicables:

b. l'ordonnance du … sur la sécurité de l'information[95].

34. Ordonnance du 19 août 2020 sur la garantie de l'approvisionnement en eau potable lors d'une pénurie grave[96]

Art. 4, al. 5

5 L'inventaire et les cartes numérisées sont à classifier «CONFIDENTIEL» selon l'art. 19, let. f, de l'ordonnance du … sur la sécurité de l'information (OSI)[97].

Art. 7, al. 4

4 Il est classifié «CONFIDENTIEL» en vertu de l'art. 19, let, f, OSI[98].

90 RS **510.292**
91 RS ...
92 RS **514.541**
93 RS ...
94 RS **531.215.32**
95 RS ...
96 RS **531.32**
97 RS ...
98 RS ...

Art. 8, al. 5

5 La documentation est classifiée «CONFIDENTIEL» en vertu de l'art. 19, let. f, OSI[99].

35. Ordonnance du 23 août 2017 sur le traitement des données dans l'OFDF[100]

Art. 12, al. 1

1 La sécurité des données est régie par les art. 1 à 4 et 6 de l'ordonnance du 31 août 2022 sur la protection des données[101] et par l'ordonnance du … sur la sécurité de l'information[102].

36. Ordonnance du 1er novembre 2017 sur l'énergie[103]

Art. 2, al. 2, let. d

2 Ne sont pas soumis à ces obligations les producteurs d'électricité dont les installations:

d. sont classifiées conformément à l'ordonnance du … sur la sécurité de l'information[104], ou

37. Ordonnance du 16 mars 2007 sur l'attribution d'organes[105]

Art. 34i, titre et al. 1, let. b

Sécurité des données

1 La sécurité des données est régie par:

b. l'ordonnance du … sur la sécurité de l'information[106].

99 RS ...
100 RS **631.061**
101 RS **235.11**
102 RS ...
103 RS **730.01**
104 RS ...
105 RS **810.212.4**
106 RS ...

38. Ordonnance du 31 octobre 2018 concernant le système d'information sur les antibiotiques en médecine vétérinaire[107]

Art. 15 Sécurité de l'information

Les mesures pour garantir la sécurité de l'information sont régies par l'ordonnance du ... sur la sécurité de l'information[108].

39. Ordonnance du 20 août 2014 sur le système d'information du service civil[109]

Art. 11, al. 1, let. b

1 La sécurité des données est régie par les dispositions suivantes:

b. l'ordonnance du … sur la sécurité de l'information[110];

40. Ordonnance du 31 octobre 2007 sur les allocations familiales[111]

Art. 18h, titre et al. 1, phrase introductive et let. b

Protection des données et sécurité de l'information

1 La protection des données et la sécurité de l'information sont régies par les dispositions suivantes:

b. l'ordonnance du … sur la sécurité de l'information[112];

41. Ordonnance du 18 novembre 2015 réglant les échanges d'importation, de transit et d'exportation d'animaux et de produits animaux avec les pays tiers[113]

Art. 102g Sécurité de l'information

Les mesures pour garantir la sécurité de l'information sont régies par l'ordonnance du … sur la sécurité de l'information[114].

107 RS **812.214.4**
108 RS ...
109 RS **824.095**
110 RS ...
111 RS **836.21**
112 RS ...
113 RS **916.443.10**
114 RS ...

42. Ordonnance du 12 août 2015 sur le système de traitement des données relatives aux prestations de sécurité privées[115]

Art. 9, al. 1, phrase introductive et let. b

1 La sécurité des données et de l'information est régie par:

b. l'ordonnance du … sur la sécurité de l'information[116].

43. Ordonnance du 8 mai 1934 sur le contrôle des métaux précieux[117]

Art. 34e

Les droits des personnes concernées, en particulier le droit d'accès aux données, à leur rectification et à leur destruction, sont régis par la loi fédérale du 25 septembre 2020 sur la protection des données[118].

Art. 34g, al. 1

1 Les art. 1 à 4 et 6 de l'ordonnance du 31 août 2022 sur la protection des données[119] et l'ordonnance du … sur la sécurité de l'information[120] sont applicables pour garantir la sécurité des données.

44. Ordonnance du 27 novembre 2000 sur les explosifs[121]

Art. 117j, al. 1, let. b

1 La sécurité des données est garantie conformément à:

b. l'ordonnance du … sur la sécurité de l'information[122].

45. Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent[123]

Art. 19, al. 1, let. b

1 La sécurité des données est régie par:

b. l'ordonnance du … sur la sécurité de l'information[124].

115 RS **935.412**
116 RS ...
117 RS **941.311**
118 RS **235.1**
119 RS **235.11**
120 RS ...
121 RS **941.411**
122 RS ...
123 RS **955.23**
124 RS ...

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

du …

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. les modalités de 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. les tâches et les compétences du service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE);

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

e. les modalités du contrôle périodique réalisé par un organe externe du traitement des données personnelles.

[2] Elle s'applique:

a. aux autorités visées à l'art. 2, al. 1, LSI;

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[2];

RS .....
1 RS **128**
2 RS **172.010.1**

c. à l'armée.

3 L'application de la présente ordonnance aux unités de l'administration fédérale décentralisée visées à l'art. 2, al. 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[3] et aux organisations visées à l'art. 2, al. 4, LOGA est régie par l'art. 2, al. 2 et 3, de l'ordonnance du … sur la sécurité de l'information (OSI)[4].

Art. 2 Entreprises concernées
(art. 50 LSI)

1 La procédure de sécurité visée dans la présente ordonnance est menée auprès des entreprises dont le siège est en Suisse.

2 Les traités internationaux visés à l'art. 87 LSI régissent l'exécution de la procédure de sécurité s'appliquant aux entreprises dont le siège est à l'étranger.

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

1 Le Secrétariat d'État à la politique de sécurité du Département fédéral de la défense, de la protection de la population et des sports (DDPS) exploite le service spécialisé PSE.

2 Le service spécialisé PSE coordonne ses activités internationales avec celles du service spécialisé de la Confédération pour la sécurité de l'information (art. 83 LSI).

Section 2 Ouverture de la procédure

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

1 Dans le domaine de compétence du Conseil fédéral, les préposés à la sécurité de l'information des unités administratives visés à l'art. 37 OSI ont la compétence de demander l'ouverture de la procédure. L'art. 13, al. 2, let. c, est réservé.

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 de la prestation;

b. des explications sur le caractère sensible du mandat;

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

3 RS **172.010**
4 RS **…**

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 La procédure doit impérativement être ouverte 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 l'accomplissement de tâches concernant plusieurs autorités ou départements;

d. l'entreprise soumissionne pour un mandat dont l'exécution requiert un certificat international de sécurité au sens de l'art. 66 LSI.

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

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

1 Lorsque des entreprises étrangères entrent en considération pour l'exécution du 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 sécurité étrangère compétente si les entreprises concernées disposent d'une déclaration de sécurité relative aux entreprises valable. Si tel n'est pas le cas, il demande à l'autorité de sécurité étrangère d'ouvrir la procédure de sécurité relative aux entreprises.

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[5] et dans l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes[6].

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 le traité international pertinent.

5 RS **…**
6 RS **…**

3 Le service spécialisé PSE fixe en accord avec l'adjudicateur les tâches sensibles que ce dernier doit mettre en œuvre pour 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.

Section 3 Évaluation des entreprises

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

1 L'adjudicateur peut indiquer au service spécialisé PSE jusqu'à cinq entreprises entrant en considération. Dans des cas motivés, le service spécialisé PSE peut autoriser un nombre plus élevé à la demande de l'adjudicateur.

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

3 Il informe l'adjudicateur dès lors qu'il est prévisible 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 marchés publics antérieurs;

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

2 Il recueille auprès du Service de renseignement de la Confédération les données que ce dernier a collectées dans l'accomplissement des tâches visées à l'art. 6, al. 1, let. a, de la loi fédérale du 25 septembre 2015 sur le renseignement[7].

7 RS **121**

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

[1] L'adjudicateur et le service spécialisé PSE s'informent mutuellement dès lors qu'il existe des indices laissant supposer qu'une entreprise entrant en considération pourrait être exclue de la procédure d'adjudication.

[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 visés à l'art. 44 de la loi fédérale du 21 juin 2019 sur les marchés publics (LMP)[8], sous réserve des art. 70, al. 3, et 71, al. 1, let. a, LSI.

Section 4 Plan de sécurité

Art. 12 Contenu et contrôle du plan de sécurité
(art. 59, al. 2 et 3, LSI)

[1] 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.

[2] Le service spécialisé PSE fixe les directives auxquelles doit répondre le plan de sécurité après inspection visuelle des locaux de l'entreprise. Il tient compte des conditions spécifiques de l'entreprise.

[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 lors qu'il est prévisible que le contrôle du plan de sécurité durera plus de 30 jours.

Art. 13 Préposé à la sécurité de l'entreprise

[1] Les entreprises entrant en considération pour l'exécution du mandat indiquent un préposé à la sécurité et son suppléant au service spécialisé PSE. Le préposé à la sécurité et son suppléant doivent être membres de la direction ou agir sur son mandat direct.

[2] Le préposé à la sécurité accomplit les tâches suivantes:

8 RS **172.056.1**

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

b. il veille à la mise en œuvre du plan de sécurité (art. 12, al. 1);

c. il demande l'ouverture de la procédure de sécurité relative aux entreprises pour le sous-contractant si l'adjudicateur a autorisé l'entreprise à octroyer un mandat sensible à un sous-contractant.

Art. 14 Communication de l'adjudication
(art. 59, al. 1, LSI)

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

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

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

1 Le service spécialisé PSE détermine les personnes de l'entreprise qui sont soumises à un contrôle de sécurité relatif aux personnes.

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

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

Art. 16 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 changement dans le domaine de la sécurité, on entend notamment:

a. un changement des rapports de propriété ou des structures de l'entreprise;

b. un changement du site de l'entreprise;

c. un changement de la composition de la direction de l'entreprise;

d. un changement des liens d'intérêts des membres de la direction de l'entreprise;

e. un changement de la solvabilité et d'éventuelles procédures de saisie ou de faillite;

f. l'existence de litiges de droit privé ou public ou de procédures pénales;

g. un changement concernant l'utilisation des moyens informatiques;

h. l'engagement de collaborateurs amenés à participer aux activités sensibles;

i. un changement dans les relations de l'entreprise avec des États étrangers ou des organisations étrangères ou dans d'autres relations de dépendance;

j. l'acceptation de mandats suscitant un conflit d'intérêts ou créant une relation de dépendance par rapport à un adjudicateur.

2 Par incident 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 visant les moyens informatiques de l'entreprise, qu'elle ait abouti ou non;

d. la découverte de vulnérabilités ou 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 effectuées dans l'entreprise.

3 L'entreprise doit également annoncer les changements et les incidents dans le domaine de la sécurité qui concernent leurs fournisseurs si ces changements ou incidents sont susceptibles d'avoir un impact sur l'exécution du mandat sensible.

4 Elle informe le service spécialisé PSE dès lors qu'il est prévisible que la déclaration de sécurité de l'entreprise arrivera à échéance alors que l'entreprise sera en train d'exécuter 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, 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, dans le cadre de l'exécution du mandat sensible, d'indices justifiant la révocation de l'adjudication au sens de l'art. 44 LMP[9];

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

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

9 RS **172.056.1**

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 de la tâche et de la fonction occupée par le personnel qui conduit la procédure. Pour le reste, l'ordonnance générale du 8 septembre 2004 sur les émoluments[10] s'applique.

3 Le service spécialisé de la Confédération pour la sécurité de l'information et le service spécialisé PSE peuvent transmettre, 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 la révocation de la déclaration de sécurité, l'adjudicateur veille immédiatement à ce que:

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

b. toutes les informations classifiées, tous les moyens informatiques et tout 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 de sécurité relative aux entreprises.

2 Si la déclaration de sécurité de l'entreprise échoit alors que la procédure est en cours de répétition, sa validité est prolongée jusqu'à ce qu'une nouvelle déclaration soit rendue 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.

10 RS **172.041.1**

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 concernant l'entreprise enregistrées dans le système d'information sur la procédure de sécurité relative aux entreprises figurent dans l'annexe 1.

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

Le DDPS 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 Prestations du service spécialisé PSE en faveur des cantons
(art. 86, al. 4, LSI)

Art. 24

1 Les cantons peuvent demander au service spécialisé PSE une évaluation de la qualification au sens des art. 55 à 57 LSI en vue de l'exécution d'un mandat sensible selon le droit cantonal:

a. lorsqu'ils disposent d'une base légale suffisante;

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 La convention de prestation visée à l'al. 1, let. c, règle notamment:

a. le nombre d'évaluations à réaliser;

b. les services cantonaux autorisés à demander de telles évaluations;

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

3 Le montant des émoluments est régi par l'art. 19, al. 2.

Section 8 Dispositions finales

Art. 25 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées dans l'annexe 2.

Art. 26 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. 27 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2024.

…

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Annexe 1
(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 AVS
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. Date du début du séjour en Suisse
13. Nom et prénom du conjoint ou du 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, restitution)
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 du mandat principal
43. Adjudicateur
44. Désignation des mandats
45. Classification
46. Date de communication
47. Début de la durée de validité
48. Fin de la durée de validité
49. Désignation succincte de la branche
50. Code de la branche correspondant à l'activité économique de l'entreprise (code NOGA)

Annexe 2
(art. 25)

Abrogation et modification d'autres actes

I

L'ordonnance du 29 août 1990 concernant la sauvegarde du secret[11] est abrogée.

II

Les actes mentionnés ci-après sont modifiés comme suit:

1. Ordonnance du 16 août 2017 sur le renseignement[12]

Annexe 3, phrase introductive et 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:
    10.6. service spécialisé chargé de la procédure de sécurité relative aux entreprises: pour l'exécution des procédures de sécurité relatives aux entreprises;

2. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[13]

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[14].

11 RO **1990** 1774
12 RS **121.1**
13 RS **510.215**
14 RS **…**

3. L'ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée et du DDPS[15]

Art. 68 et annexe 31

Abrogés

15 RS **510.911**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

du …

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. les contrôles de sécurité relatifs aux personnes visés dans la LSI;

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

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**

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

d. les contrôles de sécurité relatifs aux personnes visés aux 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, al. 1, 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 de sécurité relatif aux personnes;

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 fixe dans le domaine de compétence du Conseil fédéral:

a. les fonctions requérant un contrôle visé 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

1 La présente ordonnance s'applique:

a. aux autorités visées à l'art. 2, al. 1, LSI;

b. aux unités de l'administration fédérale centrale visées à l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration[9];

c. à l'armée;

d. aux cantons.

2 L'application de la présente ordonnance aux unités de l'administration fédérale décentralisée visées à l'art. 2, al. 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[10] et aux organisations visées à 2, al. 4, LOGA est régie par l'art. 2, al. 2 et 3, de l'ordonnance du … sur la sécurité de l'information (OSI)[11].

3 Sont réservées les dispositions d'exécution visées à l'art. 84, al. 1, LSI édictées par les autorités soumises à la LSI et portant sur:

9 RS **172.010.1**
10 RS **172.010**
11 RS **...**

a. les fonctions qui impliquent l'exercice d'une activité sensible;

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

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

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 à l'administration fédérale et aux organisations visées à l'art. 2, al. 4, LOGA[12]:

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

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

c. pour les contrôles de loyauté visés dans 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 visés dans la LSI: la liste de l'annexe 4;

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 Les responsables de projet d'une nouvelle installation nucléaire, les titulaires d'une autorisation générale, d'une autorisation de construire ou d'une autorisation d'exploiter une installation nucléaire et les destinataires d'une décision de désaffectation tiennent une 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 ou de la Chancellerie fédérale, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) peut décider s'il y a lieu de compléter ou de 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[13], les annexes 1, 4 et 6 ne sont pas publiées dans le Recueil officiel du droit fédéral.

12 RS **172.010**
13 RS **170.512**

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 trois 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
(art. 29, al. 3, LSI)

Le DDPS décide des contrôles extraordinaires visés à l'art. 29, al. 3, LSI. Il consulte au préalable le service spécialisé de la Confédération pour la sécurité de l'information.

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

1 Le DDPS décide à la demande du canton si une fonction du personnel cantonal comprend l'exercice d'une activité sensible. Il consulte au préalable le service spécialisé de la Confédération pour la sécurité de l'information. L'art. 10, al. 2, let. e, est réservé.

2 Avant de soumettre un tiers à un contrôle de sécurité relatif aux personnes, les services suivants vérifient l'existence d'une activité sensible:

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 concerné ou de la Chancellerie fédérale.

Art. 9 Contrôle de fiabilité extraordinaire de l'IFSN

Les fonctions qui ne remplissent que brièvement les conditions visées à l'art. 24, al. 1, LENu ne sont pas mentionnées dans les listes de fonctions visées à l'art. 3, al. 4. L'IFSN statue sur la fiabilité des personnes concernées. Elle peut renoncer à réaliser le contrôle de fiabilité visé à l'art. 24, al. 1, LENu et se référer notamment aux renseignements fournis par les entités 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 Attribution aux degrés de contrôle

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

1 Les activités sensibles visées dans la LSI suivantes 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 une zone de sécurité 1 visée à l'art. 35, al. 1, let. a, OSI[14] ou à une zone de protection 2 visée à l'art. 3, al. 2, let. b, de l'ordonnance du 2 mai 1990 sur la protection des ouvrages[15];

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

2 Les activités sensibles visées dans la LSI suivantes 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. l'accès à une zone de sécurité 2 visée à l'art. 35, al. 1, let. b, OSI ou à une zone de protection 3 visée à l'art. 3, al. 2, let. c, de l'ordonnance sur la protection des ouvrages;

d. les activités sensibles des employés de la Confédération et des collaborateurs externes:
   1. du Service de renseignement de la Confédération (SRC),
   2. du Renseignement militaire (RM),
   3. du service Actions dans le cyberespace et dans l'espace électromagnétique (ACEM),
   4. de l'autorité de surveillance indépendante des activités de renseignement (AS-Rens);

e. les activités sensibles des collaborateurs des autorités d'exécution cantonales visées à l'art. 9, al. 1, de loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[16];

14 RS **…**
15 RS **510.518.1**
16 RS **121**

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

Art. 11 Contrôle de loyauté visés dans la LPers

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

a. les activités relevant de la puissance publique visées à l'art. 20*b*, al. 1, let. a, LPers accomplies par des employés de la Confédération affectés à l'étranger et par des employés du Département fédéral des affaires étrangères soumis à la discipline des transferts;

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

c. les activités visées à l'art. 20*b*, al. 1, let. c, LPers exercées par le personnel de l'Office fédéral de la police (fedpol), de l'Office fédéral de la justice ainsi que de l'Office fédéral de la douane et de la sécurité des frontières, notamment en rapport avec les moyens et les méthodes opérationnels de lutte contre les crimes ou les délits ou avec l'identité de personnes exposées;

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

a. les activités exercées dans le cadre de rapports de travail dont la conclusion, la modification et la résiliation relèvent de la compétence du Conseil fédéral en vertu de l'art. 2, al. 1, de l'ordonnance du 3 juillet 2001 sur le personnel de la Confédération (OPers)[17];

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

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

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

e. les activités visées à l'art. 20*b*, al. 1, let. c, LPers du personnel de fedpol dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de compromettre gravement la lutte contre la grande criminalité relevant de la compétence de la Confédération;

f. les activités des employés des services spécialisés CSP.

17 RS **172.220.111.3**

Art. 12 Contrôles visés dans la LAAM

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

a. les 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 militaire;

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

c. les contrôles visés 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'al. 1 ou à l'art. 10 concernant la nouvelle fonction, et

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

3 Font l'objet d'une évaluation du potentiel d'abus ou de dangerosité visée à l'art. 113, al. 4, let. d, LAAM, sur demande du commandement de l'Instruction:

a. tous les conscrits;

b. tous les membres du Service de la Croix-Rouge qui sont équipés d'une arme personnelle;

c. tout militaire, lorsque ont été communiqués des soupçons laissant présumer:

1. qu'il pourrait utiliser son arme personnelle d'une manière dangereuse pour lui-même ou pour des tiers, ou

2. qu'il pourrait faire un usage abusif de son arme personnelle ou que des tiers pourraient en faire un usage abusif.

4 Concernant les conscrits, les procédures de contrôle s'effectuent dans le cadre du recrutement.

Art. 13 Contrôles de fiabilité visés dans la LENu

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

a. les personnes qui ont accès à des informations classifiées «confidentiel» relatives à des installations ou à des matières nucléaires;

b. les personnes exerçant des activités dont l'exécution déloyale est susceptible de compromettre considérablement le respect des objectifs fondamentaux de protection visés à l'art. 1, let. d, de l'ordonnance du DETEC du 17 juin 2009 sur les hypothèses de risque et sur l'évaluation de la protection contre les défaillances dans les installations nucléaires[18];

18 RS **732.112.2**

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 qui ont accès à des informations classifiées «secret» relatives à des installations ou à des matières nucléaires requièrent un contrôle de sécurité élargi.

Art. 14 Contrôles de loyauté visés dans 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 à des informations critiques en matière de sécurité de l'approvisionnement ou à des applications ou des 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 à des informations extrêmement critiques en matière de sécurité de l'approvisionnement ou à des applications ou des 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 ou de changement d'office ou de fonction relève du Conseil fédéral, celui-ci est l'instance décisionnelle.

3 En cas de décision de renoncer à la procédure de sécurité en vertu de l'art. 53, al. 2, LSI, l'adjudicateur est le service qui demande le contrôle et l'instance décisionnelle.

4 Pour les contrôles de fiabilité visés à l'art. 24, al. 1, LENu, les services compétents sont les suivants:

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

b. instance décisionnelle: l'IFSN.

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

6 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 compétence.

7 Le service qui demande le contrôle est chargé d'apporter la preuve du consentement donné aux contrôles pour autant que le système d'information visé à l'art. 45 LSI ne la fournisse pas.

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 DDPS (Service spécialisé CSP DDPS).

2 Le Service spécialisé CSP DDPS fait partie du Secrétariat d'État à la politique de sécurité du DDPS.

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

a. les fonctions visées à l'art. 2, al. 1, OPers[19], à l'exception des fonctions au sein de la Chancellerie fédérale;

b. les fonctions visées à l'art. 2, al. 1bis, OPers;

c. les fonctions au sein du Service spécialisé CSP DDPS;

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

4 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 les conditions formelles suivantes sont remplies:

a. la fonction concernée figure sur la liste des fonctions ou les conditions visées à l'art. 7 ou 8 sont remplies;

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. toutes les données de la personne soumise au contrôle nécessaires à la collecte des données et à la conduite des procédures sont disponibles.

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

3 Si l'une des conditions n'est pas remplie, ils n'effectuent pas le contrôle et en informent immédiatement le service qui a demandé le contrôle.

19 RS **172.220.111.3**

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

1 La personne soumise au contrôle doit notamment:

a. fournir 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, cela peut être pris en considération dans l'évaluation des risques.

Art. 19 Collecte des données
(art. 27 et 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 auprès:

a. des personnes ayant des rapports de travail visés à l'art. 2, al. 1, OPers[20];

b. des personnes ayant des rapports de travail visés à l'art. 2, al. 1bis, OPers;

c. des personnes exerçant une fonction dans l'un des services suivants ou dont il est prévu qu'elles exercent une telle fonction:
   1. le SRC,
   2. les autorités d'exécution cantonales visées à l'art. 9 LRens[21],
   3. le RM,
   4. l'ACEM,
   5. l'AS-Rens,
   6. fedpol,
   7. les services spécialisés CSP;

d. des personnes qui, en tant qu'employés de la Confédération, doivent traiter des informations classifiées «secret» et qui:
   1. ont ainsi largement connaissance d'importants dossiers de la politique de sécurité sur lesquels elles peuvent exercer une influence importante, ou
   2. assument des tâches de coordination ou de surveillance concernant les fonctions visées à la let. c;

e. des personnes pour lesquelles elle est prescrite par un traité international.

3 Il n'est pas nécessaire de procéder à une audition en cas de répétition du contrôle de sécurité si les données disponibles sont suffisantes à l'évaluation du risque pour la 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:

20 RS **172.220.111.3**
21 RS **121**

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;

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 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 de leur source.

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 fournir des indices concrets de risques pour la sécurité.

Art. 21 Regroupement des procédures de contrôle

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

2 Si l'activité correspond à plusieurs degrés de contrôle, la procédure est réalisée selon les exigences du degré le plus élevé.

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, constituent une exception.

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 discernement et de décision de la personne soumise au contrôle et de la consommation d'alcool, de drogue, de stupéfiants ou d'autres substances addictives;

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

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

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

Art. 23 Communication
(art. 40 LSI)

1 Si une personne est soumise à différents motifs de contrôle et qu'un service spécialisé CSP constate un facteur de risque lors d'un contrôle ultérieur, il communique sa déclaration aux instances décisionnelles des contrôles précédents. L'art. 25, al. 2, est réservé.

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

b. 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;

c. les signes ou les indices sérieux laissant présumer que la personne concernée pourrait constituer un danger pour elle-même ou pour des tiers.

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

Section 6 Conséquences de la déclaration

Art. 24 Communication de la décision sur l'exercice de l'activité
(art. 41 LSI)

1 L'instance décisionnelle communique sa décision sur l'exercice de l'activité (art. 41, al. 2, LSI) à la personne contrôlée et au service spécialisé CSP compétent dans un délai d'un mois.

2 Lorsqu'une déclaration de sécurité visée à l'art. 39, al. 1, let. a, LSI est rendue, l'autorisation d'exercer l'activité est présumée. L'instance décisionnelle peut ne pas communiquer sa décision.

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 antérieure 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 Le contrôle est l'objet d'une répétition ordinaire:

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 suivent 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.

2 Les délais fixés dans un traité international sont réservés.

3 Pour les fonctions de l'armée et de la protection civile, le contrôle de sécurité de base n'est pas l'objet d'une répétition ordinaire s'il est probable que la personne soumise au contrôle n'exercera plus sa fonction que pour une période inférieure à cinq ans.

4 Les évaluations du potentiel d'abus ou de dangerosité visées à l'art. 113, al. 4, let. d, LAAM ne sont pas l'objet d'une répétition ordinaire.

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)

La dernière décision rendue reste valable jusqu'à ce que la nouvelle décision visée à l'art. 41, al. 1, LSI soit rendue.

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

Les services spécialisés CSP ont qualité pour recourir auprès du Tribunal fédéral contre les décisions du Tribunal administratif fédéral concernant leurs déclarations.

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

1 Le service spécialisé de la Confédération pour la sécurité de l'information est chargé de délivrer les certificats nationaux et 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 a besoin du certificat de sécurité pour un motif autre que l'accomplissement d'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 La protection et de la sécurité des données traitées en dehors du système d'information conformément à l'art. 45, al. 5, LSI incombe au service chargé de leur traitement.

3 Les données produites lors du contrôle de sécurité relatif aux personnes ne doivent pas être utilisées à d'autres fins.

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 d'exécution

Art. 33 Communication électronique
(art. 48, let. a, LSI)

1 La communication entre la personne soumise au contrôle, les autorités, les tiers et les instances judiciaires s'effectue par voie électronique.

2 Les personnes qui ne sont pas des employés de la Confédération peuvent demander que la communication avec elles s'effectue en format papier.

3 Les services spécialisés CSP peuvent utiliser des plateformes de messagerie et des listes d'identité autorisées.

Art. 34 Émoluments

1 Les services spécialisés CSP perçoivent des émoluments pour les contrôles qu'ils effectuent auprès des services n'appartenant pas à l'administration fédérale centrale ou à l'armée; ces émoluments correspondent au temps consacré.

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

3 Aucun émolument n'est perçu pour les contrôles de sécurité relatifs aux personnes visés dans la LSI ni pour les contrôles de loyauté visés à l'art. 20*b* LPers.

4 Pour le reste, l'ordonnance générale du 8 septembre 2004 sur les émoluments (OGEmol)[22] 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 La convention de prestations visée à l'al. 1, let. c, règle notamment:

a. le nombre de contrôles à réaliser;

b. les services qui demandent le contrôle et les instances décisionnelles du canton;

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

22 RS **172.041.1**

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'OGEmol[23] s'applique.

Section 9 Dispositions finales

Art. 36 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont réglées dans l'annexe 8.

Art. 37 Dispositions transitoires

1 La LSI et la présente ordonnance s'appliquent aux évaluations en cours au moment de l'entrée en vigueur de la présente ordonnance. Les services spécialisés CSP vérifient en collaboration avec les services qui demandent le contrôle si les conditions à satisfaire pour la réalisation du contrôle sont toujours remplies.

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;

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 premier contrôle ou un contrôle correspondant à un degré de contrôle plus élevé selon le nouveau droit sont contrôlées dans les six mois. L'instance décisionnelle détermine si la personne est autorisée à continuer d'exercer des activités sensibles jusqu'à ce que soit rendue la décision visée à l'art. 41, al. 2, LSI. Si le contrôle en cours révèle des signes de risque pour la sécurité, l'instance décisionnelle prend les mesures préventives nécessaires.

4 Les contrôles de sécurité que la société nationale du réseau de transport a reçus sur la base du droit privé avant et jusqu'à un an après l'entrée en vigueur de la présente ordonnance 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.

23 RS **172.041.1**

Art. 38 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2024.

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, Alain Berset
Le chancelier de la Confédération, Walter Thurnherr

Annexe 1[24]
(art. 3, al. 1, let. a)

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

Cette liste n'est pas publiée

24 En application de l'art. 6 de la loi du 18 juin 2004 sur les publications officielles (RS **170.512**), le texte de la présente annexe 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 visé dans la LAsi

Unité administrative	Fonction	Contrôle de sécurité de base
SEM, Dom. dir. AS/Div. Analyses et services	Interprètes	x
SEM, Dom. dir. AS/ Div. Analyses et services	Traducteurs	x

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

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

1. Degré de contrôle «contrôle de sécurité de base»:

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
		Let. a	Let. b	Let. c
1. Chancellerie fédérale				
Aucune				
2. DFAE				
Secrétariat d'État du DFAE, Représentations à l'étranger	Carrière diplomatique	x		
	Carrière CGF	x		
	Carrière de coopération internationale	x		
	Personnel spécialisé transférable	x		
3. DFI				
Aucune				

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
4. DFJP				
OFJ, Extraditions	Co-chef/Co-cheffe AUSL			x
	Spécialiste pour les recherches internationales de personnes			x
	Juriste			x
	Collaborateur spécialisé / Collaboratrice spécialisée			x
	Secrétaire			x
	Chef/Cheffe suppl. AUSL			x
OFJ, Entraide judiciaire internationale	Chef/Cheffe IRH, sous-directeur/sous-directrice			x
	Assistant/Assistante de domaine de direction			x
	Procureur/e de liaison de la Suisse auprès d'Eurojust (NL)			x
OFJ, Traités internationaux	Chef/Cheffe INTV			x
	Juriste			x
	Chef/Cheffe suppl. INTV			x
OFJ, Entraide judiciaire I	Chef/Cheffe RH I			x
	Chef/Cheffe suppl. RH I			x
	Expert/Experte en économie et finances			x
	Juriste			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
	Collaborateur spécialisé/ Collaboratrice spécialisée, assistant/assistante			x
OFJ, Entraide judiciaire II	Chef/Cheffe RH II, chef/cheffe suppl. IRH			x
	Chef/Cheffe suppl. RH II			x
	Responsable des demandes d'entraide judiciaire			x
	Juriste			x
	Secrétaire			x
OFJ, Protection internationale des droits de l'homme	Chef/Cheffe IMRS, agent du gouvernement	x		
OFJ, Trova Services (TS)	Intérim/Intérimaire			x
	Spécialiste TROVA I			x
	Spécialiste TROVA I			x
	Chef/Cheffe TS			x
	Collaborateur spécialisé/ Collaboratrice spécialisée			x
	Chef/Cheffe suppl. TS, spécialiste TROVA I			x
OFJ, Infostar	Chef/Cheffe FIS			x
	Collaborateur spécialisé/ Collaboratrice spécialisée II			x
	Chef/Cheffe suppl. FIS / Manager des exigences			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
OFJ, Casier judiciaire	Chef/Cheffe SSR			x
	Chef/Cheffe suppl. SSR			x
	Juriste			x
	Collaborateur spécialisé/ Collaboratrice spécialisée I VOSTRA			x
	Collaborateur spécialisé/ Collaboratrice spécialisée II VOSTRA			x
	Secrétaire			x
	Spécialiste I VOSTRA			x
	Spécialiste II VOSTRA			x
OFJ, Informatique juridique	Responsable de l'application VOSTRA			x
	Responsable de l'application VOSTRA interfaces			x
5. DDPS				
Aucune				
6. DFF				
AFF, Trésorerie fédérale	Collaborateur/Collaboratrice Front Office Trésorerie		x	
	Collaborateur/Collaboratrice Back Office Trésorerie		x	
	Collaborateur/Collaboratrice caisse d'épargne du personnel fédéral		x	

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
AFF, Finances et comptabilité de la Confédération	Chef/Cheffe Comptabilité centrale		x	
	Collaborateur /Collaboratrice Gestion des paiements		x	
AFF, Monnaie fédérale Swissmint	Directeur/Directrice		x	
	Chef/Cheffe Systèmes de gestion		x	
	Chef/Cheffe Marketing et ventes		x	
	Spécialiste administration / ventes		x	
	Spécialiste design de pièces de monnaie / atelier de gravure		x	
	Chef/Cheffe technique		x	
	Spécialiste production d'outils		x	
	Spécialiste production		x	
OFPER, Service financier	Chef/Cheffe service financier		x	
OFDF, P+P	Chef/Cheffe planification et pilotage			x
OFDF, P+P, Programmes/DaziT/ Informatique	Chef/Cheffe ICT COO			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
OFDF, P+P, Développement d'entreprise et gestion du portefeuille	Chef/Cheffe de division + rempl			x
	Commissaire à la protection des données OFDF			x
	Préposés à la sécurité de l'information OFDF (ISBO)			x
OFDF. Bases	Chef/Cheffe Bases			x
OFDF, Bases, aide à la conduite	Chef/Cheffe aide à la conduite			x
OFDF, Bases, sécurité de la frontière	Chef/Cheffe sécurité de la frontière			x
	Chef/Cheffe sécurité des personnes et collaboration nationale en matière de sécurité			x
	Spécialiste sécurité des personnes et collaboration nationale en matière de sécurité			x
	Chef/Cheffe systèmes de contrôle aux frontières			x
	Spécialiste systèmes de contrôle aux frontières			x
	Chef/Cheffe sécurité des marchandises			x
	Expert/e attaché/e Frontex	x		x
OFDF, Analyse des données et des risques, Business Intelligence/Analytics	Chef/Cheffe Business Intelligence & Analytics			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
OFDF, Analyse des données et des risques, Data Services	Chef/Cheffe Data Services			x
OFDF, Analyse des données et des risques, information et situation	Chef/Cheffe Information et situation et suppl.			x
	Chef/Cheffe Gestion de l'information			x
	Expert/e Gestion de l'information			x
	Chef/Cheffe Situation et suppl.			x
	Expert/e Situation			x
	Chef/Cheffe Réseau de renseignements			x
	Attaché/e OFDF	x		x
	Officier/Officière de liaison fedpol			x
	Officier/Officière de liaison Réseau de renseignements			x
	Officier/Officière de liaison SRC			x
OFDF, Analyse des données et des risques, Analyse des données et des risques	Chef/Cheffe Analyse des données et des risques			x
	Chef/Cheffe Analyse des risques			
	Chef/Cheffe Money			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
	Expert/e Money			x
	Chef/Cheffe Security			x
	Expert/e Security			x
	Chef/Cheffe Safety			x
	Expert/e Safety			x
	Chef/Cheffe Analyse des risques Niveaux régionaux			x
	Spécialiste Analyse des risques Niveaux régionaux			x
	Spécialiste Analyse des risques Niveaux régionaux et suppl.			x
OFDF, Poursuites pénales	Chef/Cheffe Poursuites pénales			x
OFDF, Poursuites pénales, Recherche d'informations et Enquêtes préliminaires	Chef/Cheffe Recherche d'informations et Enquêtes préliminaires			x
	Expert/e coopération douanière policière			x
	Officier/Officière de liaison OFDF (Europol)	x		x
	Chef/Cheffe Recherche d'informations			x
	Inspecteur/Inpsectrice Digital forensics			x
	Inspecteur/Inspectrice OSINT et Analyse de réseau			x
	Chef/Cheffe Enquêtes préliminaires			x
	Chef/Cheffe Enquêtes préliminaires et suppl.			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
	Inspecteur/Inspectrice Enquêtes préliminaires			x
OFDF, Poursuites pénales, MEK	Chef/Cheffe Commandement d'intervention mobile (MEK) Helvetia			x
	Suppl.			x
	Chef/Cheffe Coordination engagement MEK			x
	Chef/Cheffe groupe MEK			x
	Chef/Cheffe d'équipe MEK			x
	Spécialiste Observation MEK			x
	Chef/Cheffe groupe Technique MEK			x
	Spécialiste Technique MEK			x
OFDF, Poursuites pénales, Antifraude douanière	Chef/Cheffe Antifraude douanière			x
	Chef/Cheffe Antifraude douanière et suppl.			x
	Assistant/e Antifraude douanière			x
	Chef/Cheffe Groupe d'enquêtes Antifraude douanière			x
	Chef/Cheffe Groupe d'enquêtes Antifraude douanière et suppl.			x
	Inspecteur/Inspectrice Antifraude douanière			x
OFDF, Soutien,	Chef/Cheffe Soutien			x
OFDF, OP, Niveau direction	Chef/Cheffe Opérations			x

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
	Chef/Cheffe État-major Opérations			x
	Coordinateur/Coordinatrice Tiger/ Fox Opérations			x
OFDF, OP, Niveau région	Chef/Cheffe Niveau région NR			x
OFDF, OP, Niveau Local	Chef/Cheffe Niveau Local NL			x
PUBLICA, Comptabilité	Spécialiste Comptabilité		x	
	Chef/Cheffe suppl. Comptabilité		x	
PUBLICA, Immobilier	Chef/Cheffe Immobilier		x	
	Stv. Chef/Cheffe Immobilier		x	
	Portfolio Manager		x	
PUBLICA, Gestion de portefeuille	Portfolio Manager		x	
	Senior Portfolio Manager		x	
PUBLICA, Private Markets	Private Markets Specialist		x	
PUBLICA, Operations, Risk & Compliance	Collaborateur spécialisé/Collaboratrice spécialisée ORC		x	
	Chef/Cheffe suppl ORC		x	
PUBLICA, Asset Management	Chef/Cheffe Asset Management		x	

Unité administrative	Fonction	Contrôle de sécurité de base (art. 11, al. 1, OCSP)		
7. DEFR				
SEFRI	Détaché/e	x		
SEFRI, Division Affaires spatiales	Chef/Cheffe		x	
	Responsable du groupe		x	
	Conseiller/Conseillère scientifique, responsable de programme		x	
8. DETEC				
Aucune				

2. Degré de contrôle «contrôle de sécurité élargi»

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
		Let. a	Let. b	Let. c	Let. d	Let. e	Let. f	
1. Chancellerie fédérale								
ChF, Service spécialisé CSP	Chef/Cheffe du Service spécialisé CSP						x	x
ChF, Service spécialisé CSP	Risk Profiler/in						x	x

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
ChF, Secteur TNI	Délégué à la transformation numérique et à la gouvernance de l'informatique	x						x
ChF, Secteur Conseil fédéral	Vice-chancelier de la Confédération	x						x
ChF, Secteur communication et stratégie	Vice-chancelier de la Confédération	x						x
2. DFAE								
Généralités	Secrétaire général, Secrétaire d'État, Directeur d'office	x						x
	Secrétaire général suppl., secrétaire d'État suppl., directeur d'office suppl.		x					x
	Chef/Cheffe de mission	x						x
3. DFI								
Généralités	Secrétaire général, directeur d'office	x						x
	Secrétaire général suppl. et directeur d'office suppl.		x					x

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 10, al. 2)
4. DFJP								
Généralités	Secrétaire général, secrétaire d'État, directeur d'office	x						x
	Secrétaire général suppl., secrétaire d'État suppl., directeur d'office suppl.		x					x
SCPT	Directeur/Directrice			x				
ISDC	Directeur/Directrice			x				
IPI	Directeur/Directrice			x				
ASR	Directeur/Directrice			x				
METAS	Directeur/Directrice			x				
5. DDPS								
Généralités	Secrétaire général, secrétaire d'État, directeur d'office	x						x
	Secrétaire général suppl., secrétaire d'État suppl. et directeur d'office suppl.		x					x
Office de l'auditeur en chef	Auditeur en chef	x						
	Chef/Cheffe Services centraux		x					

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
SEPOS	Personnel du Service spécialisé CSP DDPS						x	x
	Chef/Cheffe Stratégie et coopération	x						x
Groupement Défense, EM A	CdA	x						x
	Chef/Cheffe EM A	x						x
	CEM CdA	x						x
	CEMIO							x
	Chef/Cheffe Planification armée, rempl chef/cheffe EM A	x	x					x
	OSA CdA	x						x
	Chef/Cheffe projet cdmt Cyber	x						x
	Of gén Centre de politique de sécurité	x						x
	Coll spéc Engagements, cons mil chef/cheffe DDPS	x						x
	Représentant/e mil senior auprès de l'OTAN	x						x
	Chef/Cheffe Relations internationales Défense	x						x
	AD (of gén)	x						x
Groupement Défense, cdmt Opérations	Chef/Cheffe cdmt Opérations	x						x
	Rempl chef/cheffe cdmt Opérations	x	x					x

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
	Chef/Cheffe EM cdmt Opérations	x						x
	Chef/Cheffe RM & SPPA	x						x
	Commandant/e Forces terrestres	x						x
	Commandant/e brigade mécanisée 1	x						x
	Commandant/e brigade mécanisée 4	x						x
	Commandant/e brigade mécanisée 11	x						x
	Commandant/e div ter 1	x						x
	Rempl commandant/e div ter 1, commandant/e PdG	x						x
	CEM QG, chef/cheffe instruction div ter 1	x						x
	Commandant/e bur coord 1	x						x
	Commandant/e div ter 2	x						x
	Rempl commandant/e div ter 2	x						x
	Commandant/e div ter 3	x						x
	Rempl commandant/e div ter 3	x						x
	Commandant/e div ter 4	x						x
	Rempl commandant/e div ter 4	x						x
	Commandant/e LW	x						x
	Rempl commandant/e FA	x						x
	Commandant/e br DSA 33	x						x

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
	Commandant/e Police militaire	x						x
	CEM	x						x
	Chef/Cheffe délégation	x						x
Groupement Défense, Base logistique de l'armée	Chef/Cheffe BLA	x						x
	Rempl chef/cheffe BLA	x	x					x
	Chef/Cheffe Affaires sanitaires / Médecin en chef de l'armée	x						x
Groupement Défense, cdmt Cyber	Chef/Cheffe cdmt Cyber	x						x
	Commandant/e br aide cdmt 41	x						x
Groupement Défense, cdmt Instruction	Commandant/e école d'état-major	x						x
	Commandant/e FSCA / rempl chef/cheffe Instruction	x	x					x
	Commandant/e Académie militaire	x						x
	Commandant/e école centrale	x						x
	Commandant/e FOAP génie/sauv/NBC	x						x
	Commandant/e FOAP logistique	x						x
	Commandant/e FOAP blindés/artillerie	x						x
	Chef/Cheffe Personnel de l'armée	x						x
	Chef/Cheffe cdmt Instruction / rempl CdA	x	x					x

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 10, al. 3)
AS-Rens	Chef/Cheffe de l'AS-Rens			x				x
6. DFF								
Généralités	Secrétaire général, secrétaire d'État, directeur d'office	x						x
	Secrétaire général suppl., secrétaire d'État suppl., directeur d'office suppl.		x					x
OFPER, Gestion du personnel	Chef/Cheffe Gestion du personnel et budgétisation				x			
CDF	Directeur/Directrice			x				
PUBLICA	Directeur/ Directrice			x				
7. DEFR								
Généralités	Secrétaire général, secrétaire d'État, directeur d'office	x						x
	Secrétaire général suppl., secrétaire d'État suppl., directeur d'office suppl.		x					x
OFAG	Personnes travaillant en permanence à l'étranger pour l'OFAG				x			

Unité administrative	Fonction	Contrôle de sécurité élargi (art. 11, al. 2, OCSP)						Audition (art. 19, al. 2)
SECO, Direction de la promotion économique	Chef/Cheffe	x						x
Domaine des EPF, CEPF	Présidente/Président			x				
Domaine des EPF, EPFZ	Présidente/Président			x				
Domaine des EPF, EPFL	Présidente/Président			x				
Domaine des EPF, PSI	Directrice/Directeur			x				
Domaine des EPF, EMPA	Directrice/Directeur			x				
Domaine des EPF, WSL	Directrice/Directeur			x				
Domaine des EPF, Eawag	Directrice/Directeur			x				
8. DETEC								
Généralités	Secrétaire général, Secrétaire d'État, Directeur d'office	x						x
	Secrétaire général suppl., Secrétaire d'État suppl., Directeur d'office suppl.		x					x

Annexe 4[25]
(art. 3, al. 2, let. a)

Fonctions de l’armée requérant un contrôle de sécurité relatif aux personnes visé dans la LSI

Cette liste n’est pas publiée

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

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

Fonctions de l’armée requérant un contrôle de loyauté visé à l’art. 14 LAAM

Degré de contrôle «contrôle de sécurité de base»:

Organisation	**Fonction**	**Contrôle de sécurité de base (art. 12, al. 1, let. a et b. OCSP)**	
		Let. a	**Let. b**
EM A	AD en instr (sauf of gén)	x	
	Attaché de défense & suppl.	x	

Annexe 6[26]
(art. 3, al. 3)

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

Cette liste n'est pas publiée

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

Annexe 7
(art. 19, al. 1)

Collecte et traitement des données

1. Données pouvant être collectées et 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 biologique ou identité sexuelle,
   6. numéros de téléphone (réseaux fixe et mobile),
   7. adresses e-mail (professionnelles et privées),
   8. numéro AVS ou, pour les étrangers, numéro d'identification,
   9. données de la carte d'identité et du passeport,
   10. nationalités,
   11. naturalisation, expatriation,
   12. lieu d'origine,
   13. lieu de naissance,
   14. comptes et appartenance de réseaux sociaux;

b. données sur le mode de vie de la personne soumise au contrôle, notamment:
   1. cursus scolaire,
   2. formations,
   3. carrière professionnelle et activités professionnelles, y c. dossier personnel,
   4. activités accessoires,
   5. carrière au sein de l'armée, de la protection civile ou du service civil,
   6. loisirs,
   7. bénévolat,
   8. opinions ou activités religieuses,
   9. opinions philosophiques,
   10. opinions ou activités politiques,
   11. opinions ou activités syndicales,
   12. durée du séjour en Suisse ou dans des États tiers,
   13. anciens lieux de domicile et anciennes adresses;

c. données sur les relations personnelles étroites et 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. séjours à l'étranger,
2. relations d'affaires,
4. relations personnelles et contacts internationaux,
5. interdépendances financières à l'étranger;

e. données concernant la santé de la personne soumise au contrôle, notamment:
1. maladies ou troubles physiques et psychiques,
2. consommation de stupéfiants, d'alcool ou de substances psychotropes de tout type,
3. addictions et dépendances,
4. médicaments ;

f. données financières de la personne soumise au contrôle, notamment:
1. revenu et fortune,
2. prestations de soutien,
3. hypothèques et crédits,
4. dettes,
5. immobilisations financières et investissements;

g. données sur les procédures et sanctions de droit civil et de droit administratif ou les procédures et sanctions de droit pénal des mineurs ou de droit pénal impliquant la personne soumise au contrôle:
1. poursuites et faillites,
2. enquêtes pénales,
3. condamnations pénales,
4. données d'exécution,
5. enquêtes administratives,
6. actions et procès judiciaires,
7. médiation,
8. interdictions géographiques et de périmètre,
9. retraits d'armes et de permis,
10. confiscations et mises sous séquestre;

h. données sur les facteurs de risque dans le cadre d'une activité sensible exercée par la personne soumise au contrôle;

i. données concernant des tiers et des connaissances de la personne soumise au contrôle, notamment:
   1. données visées aux let. a à g concernant le partenaire, le conjoint, la famille proche ou le cercle d'amis étroit si ces données sont indispensables pour évaluer le risque pour la sécurité conformément à l'art. 34, al. 3, LSI,
   2. mandant et son adresse,
   3. employeur et partenaires commerciaux;

j. données fournies par la personne concernée au cours d'une audition orale ou écrite:
   1. lorsque des indices concrets fondés sur les données collectées laissent présumer qu'il existe un risque pour la sécurité, ou
   2. lorsque les données collectées sont insuffisantes et ne s'étendent pas sur une période suffisante pour réaliser l'évaluation;

k. données des sources suivantes:
   1. casier judiciaire: toutes les données,
   2. autorités civiles et militaires chargées de l'exécution des peines et mesures : toutes les données,
   3. systèmes et registres suivants des organes de la Confédération:
      – données de la plate-forme d'information sur les armes ARMADA
      – données du système d'information HOOGAN
      – données du système d'information NES
      – 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, des personnes astreintes au service militaire ou au service de protection civile et 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. organes de sécurité de la Confédération, SRC, organes de l'armée: toutes les données,
   5. autres organes de la Confédération: toutes les données nécessaires à l'évaluation du risque pour la sécurité,

6. registres et dossiers des organes de sécurité des cantons et des organes de police: toutes les données,
7. registres des offices des poursuites et des faillites: toutes les données,
8. dossiers des contrôles précédents: toutes les données datant de 10 ans ou moins qui n'ont pas encore été archivées ou détruites conformément à l'art. 47 LSI,
9. sources d'information publiques, notamment:
   - 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,
   - médias non électroniques: données accessibles à tout utilisateur avec ou sans conclusion d'un abonnement ou paiement d'émoluments.

2. Données supplémentaires pouvant être collectées et traitées dans le cadre du degré de contrôle «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 orale ou écrite.

Annexe 8
(art. 36)

Abrogation et modification d'autres actes

I

Sont abrogées:

1. l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes[27];
2. l'ordonnance de la Chancellerie fédérale du 30 novembre 2011 sur les contrôles de sécurité relatifs aux personnes[28];
3. l'ordonnance du DEFR du 2 novembre 2011 sur les contrôles de sécurité relatifs aux personnes[29];
4. l'ordonnance du DDPS du 12 mars 2012 concernant les contrôles de sécurité relatifs aux personnes[30];
5. l'ordonnance du DFAE du 14 août 2012 sur les contrôles de sécurité relatifs aux personnes[31];
6. l'ordonnance du DETEC du 15 février 2013 sur les contrôles de sécurité relatifs aux personnes[32];
7. l'ordonnance du DFJP du 26 juin 2013 sur les contrôles de sécurité relatifs aux personnes[33];
8. l'ordonnance du DFI du 12 août 2013 sur les contrôles de sécurité relatifs aux personnes[34];
9. l'ordonnance du 9 juin 2006 sur les contrôles de sécurité relatifs aux personnes dans le domaine des installations nucléaires[35].

II

Les actes mentionnés ci-après sont modifiés comme suit:

27 RO **2011** 1031, 5903; **2012** 1153, 3631, 3765, 5527, 6669; **2013** 3041; **2014** 4567; **2016** 1785; **2017** 4151, 4231; **2020** 5893; **2021** 589; **2022** 568, 698; **2023** 133
28 RO **2011** 6077; **2022** 118
29 RO **2011** 4999; **2013** 1335
30 RO **2012** 1161, 1597
31 RO **2012** 4241
32 RO **2013** 765
33 RO **2013** 2633
34 RO **2013** 2675
35 RO **2006** 2481; **2008** 5747; **2011** 1031

1. Ordonnance du 4 décembre 2009 sur les mesures de police administrative de l'Office fédéral de la police et sur le système d'information HOOGAN[36]

Art. 9, al. 1, let. f, et 3, let. c

1 Les autorités ci-après ont accès à HOOGAN exclusivement aux fins suivantes:

f. les services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes (services spécialisés CSP) visés à l'art. 31, al. 2, de la loi du 18 décembre 2020 sur la sécurité de l'information[37]: pour les procédures visées à l'art. 1, al. 1, de l'ordonnance du … sur les contrôles de sécurité relatifs aux personnes[38].

3 Disposent d'un accès complet:

c. les services spécialisés CSP.

Annexe, ligne Service, troisième case

OFDF, cantons, services spécialisés CSP

2. Ordonnance du 3 juillet 2001 sur le personnel de la Confédération[39]

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 leur casier judiciaire ou du registre des poursuites tous les cinq ans ou, pour de justes motifs, en tout temps.

2 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)[40].

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

36 RS **120.52**
37 SR **128**
38 RS ...
39 RS **172.220.111.3**
40 RS …

3. Ordonnance SNE du 15 octobre 2008[41]

Art. 19, al. 1, let. i, et 2, phrase introductive et let. h

1 Si cela lui est nécessaire pour obtenir les renseignements dont elle a besoin et motiver ses demandes d'entraide administrative, la PJF peut communiquer des données personnelles enregistrées dans le SNE à d'autres destinataires, à savoir:

i. les autorités fédérales chargées:
   1. des contrôles de sécurité relatifs aux personnes visés aux art. 27 à 48 de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[42],
   2. des mesures de protection au sens de l'art. 2, al. 2, let. b, LMSI[43];

2 La PJF peut en outre communiquer, sur demande, des données personnelles enregistrées dans le SNE aux autorités suivantes, pour autant qu'elles en aient besoin dans l'accomplissement de leurs tâches légales:

h. les autorités fédérales chargées des contrôles de sécurité relatifs aux personnes visés aux art. 27 à 48 LSI ou des mesures de protection au sens de l'art. 2, al. 2, let. b, LMSI;

4. Ordonnance du 24 juin 2009 concernant les relations militaires internationales[44]

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[45];

5. Ordonnance du 16 décembre 2009 sur les systèmes d'information de l'armée et du DDPS[46]

Art. 67

Abrogé

41 RS **360.2**
42 RS **128**
43 RS **120**
44 RS **510.215**
45 RS **…**
46 RS **510.911**

Art. 70s, let. e

Les données destinées à être versées au MIL PLATTFORM 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 (LSI)[47], pour les données visées à l'annexe 33*d*, ch. 2.

Annexe 23a, ch. 36

36. Degré de contrôle selon l'art. 30 LSI[48], date de l'entrée en force de la décision visée à l'art. 41, al. 2, LSI et date de la prochaine répétition ordinaire du contrôle de sécurité relatif aux personnes visée à l'art. 26 de l'ordonnance du ... sur les contrôles de sécurité relatifs aux personnes[49]

Annexe 30

Abrogée

Annexe 33d, ch. 2

2. Degré de contrôle selon les art. 10 à 14 OCSP[50], date de l'entrée en force de la décision visée à l'art. 24 OCSP et date de la prochaine répétition ordinaire du contrôle de sécurité relatif aux personnes visée à l'art. 26 OCSP concernant une personne disposant des droits d'accès.

6. Ordonnance du 22 novembre 2017 sur les obligations militaires[51]

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)[52] 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:

47 RS **128**
48 RS **128**
49 RS **...**
50 RS **...**
51 RS **512.21**
52 RS **…**

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[53], 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 officiers spécialistes, les spécialistes, les sous-officiers supérieurs et les officiers peuvent voir leurs obligations militaires prolongées si:

b. la personne concernée remplit les conditions suivantes:

3. l'instance décisionnelle laisse la personne concernée exercer l'activité conformément à l'art. 41, al. 2, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[54],

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:

c. l'instance décisionnelle laisse la personne concernée exercer l'activité conformément à l'art. 41, al. 2, LSI[55].

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 laisse la personne concernée exercer l'activité conformément à l'art. 41, al. 2, LSI[56].

7. Ordonnance du 10 décembre 2004 sur l'énergie nucléaire[57]

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)[58].

2 Les coûts du contrôle sont à la charge du service qui demande le contrôle visé à l'art. 15, al. 4, let. a, OCSP.

53 RS **…**
54 RS **128**
55 RS **128**
56 RS **128**
57 RS **732.11**
58 RS …