Loi fédérale sur la sécurité de l'information*

(Loi sur la sécurité de l'information, LSI)[1]

du 18 décembre 2020 (État le 1er avril 2025)

L'Assemblée fédérale de la Confédération suisse,
vu les art. 54, al. 1, 60, al. 1, 101, 102, al. 1, et 173, al. 1, let. a et b, et 2, de la Constitution[2],
vu le message du Conseil fédéral du 22 février 2017[3],
arrête:

Chapitre 1 Dispositions générales

Art. 1 But

1 La présente loi vise:

a. à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques;

b. à accroître la capacité de résilience de la Suisse face aux cybermenaces.[4]

2 Elle vise ainsi à protéger les intérêts publics suivants:

a. la capacité de décision et d'action des autorités et organisations de la Confédération;

b. la sécurité intérieure et extérieure de la Suisse;

c. les intérêts de la politique extérieure de la Suisse;

d. les intérêts économiques, financiers et monétaires de la Suisse;

e. l'accomplissement des obligations légales et contractuelles des autorités et organisations de la Confédération en matière de protection des informations.

RO **2022** 232

1 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

* Les termes désignant des personnes s'appliquent également aux femmes et aux hommes.

2 RS **101**

3 FF **2017** 2765

4 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

Art. 2 Autorités et organisations concernées

[1] La présente loi s'applique aux autorités suivantes:

a. l'Assemblée fédérale;

b. le Conseil fédéral;

c. les tribunaux de la Confédération;

d. le Ministère public de la Confédération et son autorité de surveillance;

e. la Banque nationale suisse.

[2] Elle s'applique également aux organisations suivantes:

a. les Services du Parlement;

b. l'administration fédérale;

c. les services administratifs des tribunaux de la Confédération;

d. l'armée;

e. les organisations visées à l'art. 2, al. 4, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[5], pour leurs tâches administratives.

[3] Le Conseil fédéral peut restreindre le champ d'application de la présente loi pour les organisations au sens de l'art. 2, al. 3 et 4, LOGA à celles qui:

a. exercent des activités sensibles, ou

b. recourent ou accèdent à des moyens informatiques de la Confédération dans l'accomplissement de leurs tâches.

[4] Il peut limiter à certaines dispositions de la présente loi le champ d'application au sens de l'al. 3. Il tient compte à cet égard de l'autonomie d'exécution des organisations concernées selon les actes organisationnels qui les régissent.

[5] Les organisations de droit public ou de droit privé qui exploitent des infrastructures critiques sans être visées par les al. 1 à 3 sont soumises aux art. 73*a* à 79.[6] La législation spéciale peut prévoir que d'autres dispositions de la présente loi leur sont applicables.

Art. 3 Application de la loi aux cantons

[1] Ne s'appliquent aux cantons que les dispositions relatives:

a. aux informations classifiées, lorsque les cantons traitent des informations classifiées de la Confédération, et

b. à la sécurité des moyens informatiques, lorsque les cantons accèdent à des moyens informatiques de la Confédération.

5 RS **172.010**

6 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

2 Ces dispositions ne s'appliquent pas lorsque les cantons garantissent une sécurité au moins équivalente de l'information.

Art. 4 Rapport avec d'autres lois fédérales

1 La loi du 17 décembre 2004 sur la transparence (LTrans)[7] prime la présente loi.[8]

1bis Les informations provenant de tiers dont l'Office fédéral de la cybersécurité (OFCS) prend connaissance dans son activité de réception et d'analyse des signalements conformément au chap. 5 ne peuvent être rendues accessibles en vertu de la LTrans. Les autorités, les organisations et les personnes visées à l'art. 2, al. 1, LTrans ne sont pas considérées comme des tiers.[9]

2 Lorsque la protection d'informations est également réglée dans d'autres lois fédérales, les dispositions de la présente loi s'appliquent à titre complémentaire.

Art. 5 Définitions

On entend par:

a. *moyen informatique:* moyen relevant des techniques de l'information et de la communication, notamment les applications, les systèmes d'information et les fichiers, ainsi que les installations, les produits et les services servant au traitement électronique des informations;

b. *activité sensible:*
   1. le traitement d'informations classifiées «confidentiel» ou «secret»,
   2. l'administration, l'exploitation, la maintenance et le contrôle de moyens informatiques relevant des catégories de sécurité «protection élevée» ou «protection très élevée»,
   3. l'accès à des zones de sécurité, en particulier aux zones de protection 2 ou 3 d'un ouvrage au sens de la législation sur la protection des ouvrages militaires;

c. *infrastructure critique:* l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population;

d.[10] *cyberincident:* un événement survenant lors de l'utilisation de moyens informatiques et ayant pour conséquence une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'informations ou à la traçabilité de leur traitement;

7 RS **152.3**

8 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

9 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 168, 173; FF **2023** 84).

10 Introduite par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

e.[11] *cyberattaque:* un cyberincident provoqué intentionnellement;

f.[12] *cybermenace:* toute circonstance ou tout événement pouvant entraîner un cyberincident;

g.[13] *vulnérabilité:* une cybermenace due à des failles ou à des erreurs dans les moyens informatiques.

Chapitre 2 Mesures générales

Section 1 Principes

Art. 6 Sécurité de l'information

[1] Les autorités et organisations soumises à la présente loi veillent à ce que le besoin de protection des informations relevant de leur compétence soit évalué en fonction de l'atteinte potentielle aux intérêts définis à l'art. 1, al. 2.

[2] Elles veillent à ce que les informations, en fonction de leur besoin de protection:

a. ne soient accessibles qu'aux personnes autorisées (confidentialité);

b. soient disponibles en cas de besoin (disponibilité);

c. ne puissent être modifiées sans droit ou par mégarde (intégrité);

d. soient traitées de manière à être traçables (traçabilité).

[3] Elles veillent à ce que les moyens informatiques auxquels elles recourent pour accomplir leurs tâches légales soient protégés contre les utilisations abusives et les perturbations.

[4] Elles tiennent compte à cet égard des principes de la proportionnalité, de l'économicité et de la simplicité d'emploi.

Art. 7 Responsabilité des autorités soumises à la présente loi

[1] Les autorités soumises à la présente loi veillent, chacune dans son domaine de compétence, à ce que la sécurité de l'information soit organisée, mise en œuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques.

[2] Elles fixent:

a. leurs objectifs en matière de sécurité de l'information;

b. les principes de gestion des risques;

11 Introduite par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

12 Introduite par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

13 Introduite par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

c. les conséquences d'une violation des prescriptions.

Art. 8 Gestion des risques

1 Les autorités et organisations soumises à la présente loi veillent, chacune dans son domaine de compétence, à ce que les risques en matière de sécurité de l'information soient constamment évalués.

2 Elles prennent les mesures nécessaires pour éliminer les risques ou les ramener à un niveau acceptable.

3 Les risques jugés acceptables doivent être formellement acceptés.

Art. 9 Collaboration avec les tiers

1 Lorsque les autorités et organisations soumises à la présente loi collaborent avec des tiers, elles veillent à ce que les exigences et mesures prévues par la présente loi soient reprises dans les accords et les contrats qu'elles concluent à cet effet.

2 Elles veillent à ce que la mise en œuvre des mesures soit contrôlée de manière adéquate.

Art. 10 Procédure en cas de violation de la sécurité de l'information

1 Les autorités et organisations soumises à la présente loi veillent à ce que les violations de la sécurité de l'information soient décelées rapidement, leurs causes clarifiées et leurs conséquences limitées au maximum.

2 Les autorités soumises à la présente loi veillent à établir des plans d'action dans l'éventualité de graves violations de la sécurité de l'information susceptibles de menacer l'accomplissement de tâches indispensables de la Confédération; elles organisent des exercices à cet effet.

Art. 10*a*[14] Traitement des données personnelles

1 Les autorités et organisations peuvent traiter les données personnelles utiles à la sécurité de l'information, notamment dans les systèmes de gestion de la sécurité des informations prévus à cet effet (applications SGSI).

2 Elles peuvent échanger entre elles des données personnelles au sens de l'al. 1 ainsi qu'avec des organisations nationales, internationales ou étrangères de droit public, si les conditions suivantes sont remplies:

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

b. cela n'enfreint aucune obligation légale ou contractuelle de garder le secret;

c. les dispositions de la législation fédérale sur la protection des données sont respectées;

14 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

d. l'organisation qui reçoit les données assume des tâches légales dans le domaine de la sécurité de l'information qui correspondent à celles de l'autorité ou de l'organisation qui fait la communication.

3 Elles peuvent relier entre eux leurs systèmes d'information, notamment les applications SGSI, et échanger des données automatiquement ou sur demande par l'intermédiaire d'interfaces.

4 Elles peuvent administrer des formulaires électroniques servant à soumettre ou à traiter des demandes et des signalements dans le domaine de la sécurité de l'information et les relier à leurs applications SGSI ou à d'autres systèmes d'information.

5 Dans la mesure où cela est nécessaire pour gérer des violations de la sécurité de l'information ou pour éliminer des vulnérabilités, elles peuvent effectuer les actions suivantes avec des données sensibles au sens de l'art. 5, let. c, de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[15] relatives à des personnes qui sont impliquées dans ces violations ou ces vulnérabilités ou qui sont ou pourraient être concernées par elles:

a. les traiter;

b. les échanger entre elles ainsi qu'avec des organisations nationales, internationales ou étrangères de droit public, pour autant que la condition visée à l'al. 2, let. b, soit remplie.

6 Elles peuvent conserver les données sensibles jusqu'à deux ans après la gestion des violations de la sécurité de l'information ou l'élimination des vulnérabilités, mais dix ans au plus.

7 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

8 Le traitement de données personnelles par l'OFCS[16] dans le cadre de l'accomplissement de ses tâches est régi par les art. 75 à 79.

Section 2 Classification des informations

Art. 11 Principes régissant la classification

1 Les autorités et organisations soumises à la présente loi veillent à ce que les informations qui remplissent les critères définis à l'art. 13 soient classifiées.

2 La classification doit se limiter au strict nécessaire et être si possible temporaire.

Art. 12 Compétences

1 Les autorités soumises à la présente loi désignent les personnes et services compétents pour classifier les informations (auteurs de la classification).

15 RS **235.1**

16 Nouvelle expression selon le ch. I de l'O du 7 mars 2025, en vigueur depuis le 1er avr. 2025 (RO **2025** 168). Il a été tenu compte de cette mod. dans tout le texte.

2 Seuls l'auteur de la classification ou le service auquel il est subordonné peuvent modifier ou supprimer une classification.

3 Le Conseil fédéral règle la déclassification des archives.

Art. 13 Échelons de classification

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

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

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

Art. 14 Accès aux informations classifiées

1 Seules peuvent accéder aux informations classifiées les personnes qui offrent toutes les garanties qu'elles les traiteront correctement et qui remplissent l'une des conditions suivantes:

a. elles ont besoin des informations en question pour accomplir une tâche légale;

b. elles disposent d'une autorisation d'accès qui leur a été conférée contractuellement et ont besoin des informations en question pour accomplir les tâches qui leur ont été confiées.

2 L'accès aux archives classifiées est réglé par la législation sur l'archivage.

3 Les limitations d'accès prévues dans des traités internationaux au sens de l'art. 87 sont réservées.

Art. 15 Accès à des informations classifiées dans le cadre de procédures spéciales

1 L'accès à des informations classifiées relevant de l'Assemblée fédérale, des Services du Parlement, des tribunaux et des ministères publics est régi par le droit de procédure applicable.

2 Avant toute décision donnant accès à une information au sens de l'al. 1, l'organe parlementaire ou le tribunal compétent peut consulter l'auteur de la classification.

Section 3 Sécurité des moyens informatiques

Art. 16 Procédure de sécurité

1 Pour garantir la sécurité de l'information lors de l'utilisation de moyens informatiques, les autorités soumises à la présente loi élaborent une procédure de sécurité.

2 La procédure de sécurité définit en particulier:

a. les critères permettant d'évaluer le besoin de protection des informations avant la mise en service des moyens informatiques;

b. les modalités de mise en œuvre des mesures de sécurité et leur contrôle;

c. la compétence d'autoriser les moyens informatiques;

d. la procédure à suivre en cas de modification des risques.

3 L'exécution de la procédure de sécurité incombe aux autorités et organisations soumises à la présente loi qui décident de l'utilisation de moyens informatiques.

Art. 17 Catégories de sécurité

1 Les moyens informatiques relèvent de la catégorie de sécurité «protection de base», à moins qu'ils relèvent d'une catégorie de sécurité supérieure.

2 Ils relèvent de la catégorie de sécurité «protection élevée» dans les cas suivants:

a. une violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des informations qu'ils traitent risque de nuire considérablement aux intérêts définis à l'art. 1, al. 2;

b. leur utilisation abusive ou leur perturbation sont susceptibles de nuire considérablement aux intérêts définis à l'art. 1, al. 2.

3 Ils relèvent de la catégorie de sécurité «protection très élevée» dans les cas suivants:

a. une violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des informations qu'ils traitent risque de nuire gravement aux intérêts définis à l'art. 1, al. 2;

b. leur utilisation abusive ou leur perturbation sont susceptibles de nuire gravement aux intérêts définis à l'art. 1, al. 2.

Art. 18 Mesures de sécurité

1 Les autorités soumises à la présente loi fixent les exigences de sécurité minimales applicables aux catégories de sécurité définies à l'art. 17.

2 Tous les moyens informatiques doivent satisfaire aux exigences minimales de la catégorie de sécurité «protection de base».

3 L'efficacité des mesures applicables aux moyens informatiques de la catégorie de sécurité «protection très élevée» doit faire l'objet de contrôles périodiques.

Art. 19 Sécurité de l'exploitation

1 Les autorités et organisations soumises à la présente loi garantissent la sécurité des moyens informatiques qu'elles exploitent pour elles-mêmes ou sur mandat d'une autre autorité ou organisation.

2 Les art. 57*i* à 57*q* LOGA[17] s'appliquent par analogie au traitement des données personnelles dans le cadre de la surveillance des réseaux.

Section 4 Mesures relatives aux personnes

Art. 20 Conditions d'accès aux informations et aux moyens informatiques de la Confédération

1 Les autorités et organisations soumises à la présente loi veillent à ce que les personnes qui accèdent à des informations, des moyens informatiques, des locaux et d'autres infrastructures de la Confédération:

a. soient choisies avec soin;

b. soient identifiées en fonction de la sensibilité de l'activité concernée;

c. reçoivent une formation et une formation continue adaptées à leur niveau de responsabilité;

d. soient le cas échéant tenues au maintien du secret.

2 Elles peuvent recourir à des méthodes biométriques de vérification pour identifier les personnes, si la sensibilité de l'activité concernée le requiert. Les données biométriques sont détruites à l'échéance de l'autorisation d'accès.

3 Elles peuvent en outre utiliser systématiquement le numéro AVS au sens de l'art. 50*c* de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[18] comme identificateur de personnes.

Art. 21 Délivrance restrictive des autorisations

1 Les autorités et organisations soumises à la présente loi veillent à ce que des autorisations d'accès à des informations, des moyens informatiques, des locaux ou d'autres infrastructures de la Confédération ne soient délivrées qu'aux personnes qui en ont besoin pour accomplir leurs tâches.

2 Les autorisations sont retirées à la fin de l'engagement ou du contrat ou dès que la tâche concernée a été exécutée. Elles peuvent être bloquées ou retirées sans préavis lorsque des indices concrets donnent à penser que la sécurité est menacée.

Section 5 Protection physique

Art. 22 Principe

Les autorités et organisations soumises à la présente loi veillent à assurer une protection physique adéquate des informations et moyens informatiques dont elles sont responsables contre les utilisations abusives et les perturbations.

17 RS **172.010**
18 RS **831.10**

Art. 23 Zones de sécurité

1 Les autorités et organisations soumises à la présente loi peuvent instituer des zones de sécurité dans des locaux ou des espaces dans lesquels:

a. des informations classifiées «confidentiel» ou «secret» sont fréquemment traitées, ou

b. des moyens informatiques des catégories de sécurité «protection élevée» ou «protection très élevée» sont exploités.

2 Elles peuvent prendre les mesures suivantes:

a. interdire certains objets, en particulier les appareils de prises de vue et de son;

b. surveiller les secteurs sensibles avec des appareils de prises de vue et de son;

c. procéder à des fouilles;

d. procéder à des contrôles des locaux inopinés, même en l'absence des employés.

3 Elles peuvent exploiter, conformément à l'art. 34, al. 1ter, de la loi du 30 avril 1997 sur les télécommunications (LTC)[19], une installation perturbatrice dans les zones de sécurité où des informations classifiées «secret» sont fréquemment traitées ou des moyens informatiques de la catégorie de sécurité «protection très élevée» sont exploités.[20]

4 Les dispositions particulières relatives aux zones de sécurité établies en vertu des traités internationaux au sens de l'art. 87 et les dispositions applicables aux zones de protection des ouvrages au sens de la législation sur la protection des ouvrages militaires sont réservées.

Section 6 Systèmes de gestion des données d'identification

Art. 24 Exploitation de systèmes de gestion des données d'identification

1 Les autorités soumises à la présente loi peuvent exploiter des systèmes permettant une gestion centralisée des données servant à identifier les personnes qui ont accès aux informations, aux moyens informatiques, aux locaux et à d'autres infrastructures (systèmes de gestion des données d'identification).

2 Les systèmes de gestion des données d'identification vérifient l'identité et les profils d'accès des personne, des machines et des systèmes. Ils transmettent le résultat aux systèmes d'information raccordés pour la vérification des autorisations.

3 Les autorités soumises à la présente loi désignent un service responsable pour chaque système de gestion des données d'identification.

19 RS **784.10**

20 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

Art. 25 Échange et harmonisation des données

[1] Les systèmes de gestion des données d'identification permettent d'échanger des données et de les harmoniser avec les systèmes d'information raccordés, avec les répertoires de personnes et d'utilisateurs et avec d'autres systèmes de gestion des données d'identification exploités par des autorités soumises à la présente loi.

[2] L'échange et l'harmonisation sont limités aux données dont le traitement est autorisé dans le système concerné.

Art. 26 Dispositions d'exécution

Les autorités soumises à la présente loi édictent des dispositions d'exécution notamment dans les domaines suivants:

a. la protection et la sécurité des données;

b. les données personnelles traitées;

c. l'échange et l'harmonisation des données avec d'autres systèmes;

d. la journalisation et la transmission des données de journalisation aux systèmes d'information raccordés;

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

Chapitre 3 Contrôle de sécurité relatif aux personnes

Section 1 Dispositions générales

Art. 27 But et objet du contrôle

[1] Le contrôle de sécurité relatif aux personnes vise à déterminer si l'exercice d'une activité sensible par une personne dans le cadre de sa fonction ou d'un mandat présente un risque pour la sécurité de l'information.

[2] À cette fin, les services compétents collectent les données pertinentes pour la sécurité touchant au mode de vie de la personne concernée, notamment à ses relations personnelles étroites et familiales, à sa situation financière et à ses rapports avec l'étranger.

[3] Les données sur l'exercice des droits constitutionnels ne peuvent être traitées que s'il existe un soupçon concret que la personne soumise au contrôle exerce ces droits pour préparer ou accomplir des actes susceptibles de nuire considérablement aux intérêts définis à l'art. 1, al. 2.

Art. 28 Liste des fonctions

[1] Les autorités soumises à la présente loi édictent, chacune dans son domaine de compétence, une liste des fonctions qui impliquent l'exercice d'une activité sensible.

2 Elles contrôlent périodiquement l'exactitude de la liste et y apportent les corrections nécessaires.

Art. 29 Personnes soumises au contrôle

1 Sont soumis à un contrôle de sécurité:

a. les employés de la Confédération, les collaborateurs externes et les militaires qui exercent une fonction figurant sur l'une des listes visées à l'art. 28;

b. les employés cantonaux qui exercent une activité sensible;

c. les tiers qui exécutent pour une autorité ou une organisation soumise à la présente loi un mandat qui implique l'exercice d'une activité sensible;

d. les personnes soumises à un contrôle de sécurité en vertu d'un traité international au sens de l'art. 87.

2 Toute personne appelée à exercer une activité sensible pour le compte d'une autorité étrangère ou d'une organisation internationale est soumise à un contrôle de sécurité pour autant que la Suisse ait conclu un traité international au sens de l'art. 87 avec l'État ou l'organisation internationale en question.

3 Les personnes qui exercent une fonction qui ne figure pas encore sur l'une des listes visées à l'art. 28 peuvent exceptionnellement, sur approbation de l'autorité concernée, être soumises à un contrôle de sécurité. La liste des fonctions doit être complétée dès que possible.

4 Les candidats aux fonctions suivantes ne sont pas soumis à un contrôle de sécurité:

a. membre de l'Assemblée fédérale;

b. membre du Conseil fédéral et chancelier de la Confédération;

c. juge auprès d'un tribunal de la Confédération;

d. procureur général de la Confédération;

e. membre de l'Autorité de surveillance du Ministère public de la Confédération;

e^bis.[21] chef du Préposé fédéral à la protection des données et à la transparence;

f. général;

g. magistrat cantonal élu par le peuple ou par le parlement du canton concerné.

Art. 30 Degrés de contrôle

Les autorités soumises à la présente loi attribuent les degrés de contrôle suivants aux activités sensibles définies ci-après:

a. contrôle de sécurité de base: activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de nuire considérablement aux intérêts définis à l'art. 1, al. 2;

21 Introduite par le ch. I de la LF du 17 juin 2022 (Chef du Préposé fédéral à la protection des données et à la transparence), en vigueur depuis le 1er janv. 2024 (RO **2023** 734; FF **2022** 345, 432).

b. contrôle de sécurité élargi: activités sensibles dont l'exercice inadéquat ou contraire aux prescriptions est susceptible de nuire gravement aux intérêts définis à l'art. 1, al. 2.

Section 2 Procédure

Art. 31 Services compétents

1 Les autorités soumises à la présente loi et les cantons désignent les services qui ont les compétences suivantes:

a. ouvrir la procédure du contrôle de sécurité (services qui demandent le contrôle);

b. décider de confier l'activité sensible (instances décisionnelles).

2 Le Conseil fédéral désigne un ou plusieurs services spécialisés chargés de réaliser les contrôles de sécurité relatifs aux personnes (services spécialisés CSP). Ces services réalisent l'évaluation sans aucune instruction.

Art. 32 Consentement et collaboration

1 Aucun contrôle de sécurité ne peut être réalisé sans le consentement de la personne soumise au contrôle.

2 Les conscrits, les militaires et les membres de la protection civile peuvent être soumis à un contrôle de sécurité sans leur consentement.

3 La personne soumise au contrôle est tenue de collaborer à l'établissement des faits.

Art. 33 Moment du contrôle

1 Pour les personnes visées à l'art. 29, al. 1, let. a et b, la procédure de contrôle de sécurité doit être ouverte avant l'attribution de la fonction.

2 Pour les personnes visées à l'art. 29, al. 1, let. a, qui doivent être nommées par le Conseil fédéral, le contrôle de sécurité doit être achevé avant le dépôt de la proposition de nomination.

3 Pour les personnes visées à l'art. 29, al. 1, let. c, le contrôle de sécurité doit être achevé avant que l'activité sensible ne leur soit confiée.

4 Pour les personnes visées à l'art. 29, al. 1, let. d, le contrôle de sécurité a lieu au moment prévu par le traité applicable.

Art. 34 Collecte des données

1 Les services spécialisés CSP peuvent collecter les données suivantes relatives à une personne pour réaliser un contrôle de sécurité de base:

a. données du casier judiciaire;

b. données sur des procédures pénales en cours, classées ou suspendues, en demandant des renseignements ou des dossiers auprès des autorités pénales;

c. données nécessaires à l'évaluation du risque, auprès des organes de sécurité de la Confédération, du Service de renseignement de la Confédération (SRC), des organes de l'armée et d'autres organes de la Confédération;

d. données des registres et dossiers des organes de sécurité des cantons et des organes de police;

e. données des registres des offices des poursuites et des faillites;

f. données des dossiers établis lors de contrôles de sécurité antérieurs;

g. données de sources d'information publiques.

2 Ils peuvent au surplus collecter les données suivantes relatives à une personne pour réaliser un contrôle de sécurité élargi:

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

b. données du registre du contrôle des habitants;

c. données détenues par les établissements financiers et banques entretenant des relations d'affaires avec la personne concernée;

d. données fournies par la personne concernée au cours d'une audition.

3 Lorsque des indices concrets fondés sur les données collectées donnent à penser qu'il existe un risque pour la sécurité ou lorsque les données collectées sont insuffisantes ou ne s'étendent pas sur une période suffisante pour réaliser le contrôle, les services spécialisés CSP peuvent auditionner la personne concernée. Ils peuvent également interroger des tiers moyennant le consentement de la personne soumise au contrôle de sécurité; ils indiquent aux tiers concernés qu'ils sont libres de donner des renseignements ou non.

4 Les données relatives à des tiers qui sont indissociables des données relatives à la personne soumise au contrôle de sécurité peuvent être traitées si elles sont indispensables pour réaliser le contrôle. Les services spécialisés CSP informent les tiers concernés du traitement de leurs données.

Art. 35 Assistance administrative

1 L'autorité ou l'organisation concernée au sens de l'art. 34 collecte les données détenues par une autorité étrangère ou une organisation internationale.

2 Lorsque les données collectées fournissent des indices concrets de crime organisé ou de criminalité internationale, le service spécialisé CSP consulte les offices centraux de police criminelle de la Confédération. Les offices centraux ne communiquent au service spécialisé CSP que les données personnelles pertinentes pour la sécurité.

Art. 36 Prise en charge des coûts

1 Les autorités et organisations de droit public auprès desquelles les services spécialisés CSP peuvent collecter des données ou qui sont tenues de participer à la procédure prêtent leur concours gratuitement.

2 Les tiers auxquels la procédure occasionne une charge considérable sont indemnisés.

3 La Confédération supporte les coûts du contrôle pour les employés cantonaux visés à l'art. 29, al. 1, let. b.

Art. 37 Classement de la procédure

1 Les services spécialisés CSP classent la procédure lorsque la personne concernée revient sur son consentement ou qu'elle n'entre plus en considération pour exercer la fonction prévue ou pour exécuter le mandat.

2 Ils communiquent le classement de la procédure à la personne concernée et au service qui a demandé son ouverture. La personne concernée est réputée ne pas avoir été contrôlée.

Section 3 Évaluation du risque pour la sécurité

Art. 38 Risque pour la sécurité

1 Il existe un risque pour la sécurité lorsque des indices concrets fondés sur les données collectées laissent supposer avec une probabilité élevée que la personne contrôlée exécutera l'activité sensible de manière inadéquate ou contraire aux prescriptions.

2 La probabilité d'un exercice inadéquat ou contraire aux prescriptions d'une activité sensible peut notamment être jugée élevée lorsque des indices concrets donnent à penser que la personne présente l'une des caractéristiques suivantes:

a. elle manque d'intégrité ou de loyauté;

b. elle est susceptible de céder au chantage ou à la corruption;

c. elle ne dispose pas d'une pleine capacité de jugement ou de décision.

3 L'évaluation doit se fonder sur des faits concernant la situation personnelle de la personne soumise au contrôle, indépendamment de toute faute commise.

Art. 39 Résultat de l'évaluation

1 Les services spécialisés CSP rendent l'une des déclarations suivantes, qui a la signification indiquée ci-après:

a. déclaration de sécurité: il n'existe aucun risque pour la sécurité;

b. déclaration de sécurité sous réserve: il existe un risque pour la sécurité, mais celui-ci peut être ramené à un niveau acceptable en respectant certaines conditions; les services spécialisés CSP recommandent les conditions à fixer;

c. déclaration de risque: il existe un risque pour la sécurité;

d. constatation: les données sont insuffisantes ou ne s'étendent pas sur une période suffisante pour évaluer le risque pour la sécurité.

2 Dans les cas visés à l'al. 1, let. b à d, ils donnent au préalable la possibilité à la personne soumise au contrôle de donner son avis.

Art. 40 Communication

1 Les services spécialisés CSP communiquent par écrit à la personne concernée et à l'instance décisionnelle la déclaration qu'ils ont rendue.

2 Pour les nominations par le Conseil fédéral, les services spécialisés CSP communiquent leur déclaration au département qui propose la nomination.

3 Ils peuvent communiquer la déclaration à une autre instance décisionnelle dans les cas suivants:

a. la personne soumise au contrôle est appelée à exercer une autre activité sensible au sens de la présente loi qui requiert un contrôle de sécurité;

b. la personne est soumise à un contrôle de loyauté en vertu d'une autre loi fédérale;

c. la personne est soumise à une évaluation en vertu de l'art. 113 de la loi du 3 février 1995 sur l'armée[22].

4 Si les services spécialisés CSP disposent, avant la clôture de l'évaluation, d'indices concrets d'un risque pour la sécurité, ils peuvent communiquer leurs constatations intermédiaires par écrit aux autorités et instances visées aux al. 1 à 3 et à la personne contrôlée.

Section 4 Conséquences de la déclaration

Art. 41 Exercice de l'activité sensible

1 Les déclarations des services spécialisés CSP ont valeur de recommandation.

2 Le service visé à l'art. 31, al. 1, let. b décide, après avoir pris connaissance de la déclaration, si la personne contrôlée peut exercer l'activité sensible en question.

3 Il peut fixer des conditions à l'exercice de l'activité.

4 Il communique sa décision au service spécialisé CSP.

Art. 42 Utilisation de la déclaration pour d'autres activités sensibles

Il n'est pas nécessaire de réaliser un nouveau contrôle de sécurité lorsque la personne concernée a déjà obtenu une déclaration pour un degré de contrôle au moins équivalent:

a. en vue d'une autre activité sensible au sens de la présente loi;

b. dans le cadre d'un contrôle de loyauté en vertu d'une autre loi fédérale.

22 RS **510.10**

Art. 43 Répétition du contrôle

[1] Le contrôle de sécurité relatif aux personnes est répété comme suit:

a. contrôle de sécurité de base: au plus tôt après cinq ans, au plus tard après dix ans;

b. contrôle de sécurité élargi: au plus tôt après trois ans, au plus tard après cinq ans.

[2] Le Conseil fédéral peut prévoir qu'il n'est pas nécessaire de répéter le contrôle de sécurité de base pour les personnes exerçant certaines fonctions au sein de l'armée ou de la protection civile.

[3] Lorsque le service qui demande le contrôle ou l'instance décisionnelle ont des raisons de penser que de nouveaux risques sont apparus depuis le dernier contrôle, ils peuvent demander la répétition du contrôle de sécurité au service spécialisé CSP; ils motivent leur demande par écrit.

Art. 44 Voies de droit

[1] La personne contrôlée dispose d'un délai de 30 jours à compter de la réception d'une déclaration au sens de l'art. 39, al. 1, pour:

a. consulter le dossier du contrôle;

b. demander la rectification des données erronées ou la destruction des données obsolètes;

c. demander que l'on ajoute à une donnée la mention de son caractère litigieux.

[2] Les restrictions à la communication de renseignements sont régies par l'art. 26 LPD[23].[24]

[3] La déclaration constitue un acte matériel au sens de l'art. 25*a* de la loi fédérale du 20 décembre 1968 sur la procédure administrative[25]. La personne contrôlée peut recourir contre une déclaration au sens de l'art. 39, al. 1, let. b à d, auprès du Tribunal administratif fédéral dans un délai de 30 jours à compter de sa réception.

[4] Si l'instance décisionnelle est le Tribunal fédéral ou le Tribunal administratif fédéral, l'art. 36, al. 2 et 4, de la loi du 24 mars 2000 sur le personnel de la Confédération[26] s'applique par analogie.

[5] La procédure de recours est régie au surplus par les dispositions générales de la procédure fédérale.

23 RS **235.1**
24 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
25 RS **172.021**
26 RS **172.220.1**

Section 5 Traitement des données personnelles

Art. 45 Système d'information sur le contrôle de sécurité relatif aux personnes

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

a. des contrôles de sécurité relatifs aux personnes;

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

c. des contrôles de fiabilité;

d. des contrôles de loyauté.[27]

2 Chaque service spécialisé CSP est responsable de la licéité du traitement des données personnelles qu'il effectue dans le système d'information.

3 Les données sensibles au sens de l'art. 5, let. c, LPD[28] peuvent être traités dans le système d'information dans la mesure où elles sont nécessaires à l'évaluation du risque pour la sécurité.[29]

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

a. risque pour la sécurité;

b. potentiel d'abus et de dangerosité en ce qui concerne l'arme personnelle.[30]

4 Le système d'information contient les données suivantes:

a. les données d'identité des personnes à contrôler ou des personnes qui ont été contrôlées, y compris le numéro AVS et le numéro de passeport;

b. les données visées aux art. 34 et 35;

c. les données relatives à l'évaluation du risque pour la sécurité;

d. le résultat de l'évaluation visé à l'art. 39, al. 1;

e. la décision de l'instance décisionnelle;

f. les données et les dossiers relatifs aux procédures de recours;

g. des listes et statistiques contenant les données visées aux let. a à f.

5 Le traitement des données visées à l'al. 4 en dehors du système d'information doit être mentionné dans le système.

27 Nouvelle teneur selon le ch. II 2 de la LF du 17 juin 2022, en vigueur depuis le 1er janv. 2024 (RO **2023** 117, 650; FF **2021** 3046).
28 RS **235.1**
29 Nouvelle teneur selon l'annexe 2 ch. 5, en vigueur depuis le 1er janv. 2024 (RO **2022** 232; **2023** 650; FF **2017** 2465).
30 Introduit par le ch. II 2 de la LF du 17 juin 2022, en vigueur depuis le 1er janv. 2024 (RO **2023** 117, 650; FF **2021** 3046).

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

a.[31] casier judiciaire informatique au sens de la loi du 17 juin 2016 sur le casier judiciaire[32];

b. index national de police au sens de l'art. 17 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[33];

c. système d'indexation des données du SRC au sens de l'art. 51 de la loi fédérale du 25 septembre 2015 sur le renseignement[34];

d.[35] banques de données de l'Office central des armes visées à l'art. 32*a*, al. 1, de la loi du 20 juin 1997 sur les armes[36].

Art. 46 Consultation et communication des données

1 Les organes suivants peuvent consulter en ligne les données ci-après contenues dans le système d'information:

a. les services qui demandent le contrôle: les données visées à l'art. 45, al. 4, let. b, qu'ils ont saisies eux-mêmes lors de l'ouverture de la procédure de contrôle, ainsi que les données visées à l'art. 45, al. 4, let. a, d et e;

b. les instances décisionnelles: les données visées à l'art. 45, al. 4, let. a, d et e;

c. les préposés à la sécurité de l'information au sens de l'art. 81, pour l'exécution de leurs tâches de contrôle: les données visées à l'art. 45, al. 4, let. a, d et e;

d. les services de la Confédération et des cantons auprès desquels les données visées à l'art. 37 sont collectées: les données visées à l'art. 45, al. 4, let. a.

2 Les organes suivants peuvent consulter les données ci-après contenues dans le système d'information:

a. le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) au sens de l'art. 51, al. 2, par une interface liée au système d'information visé à l'art. 70, pour mener la procédure de sécurité relative aux entreprises au sens des art. 49 à 73: les données visées à l'art. 45, al. 4, let. a, d et e;

b. le Groupement Défense:

1. par une interface liée au système d'information visé à l'art. 12 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée (LSIA)[37], dans les buts définis à l'art. 13 LSIA: les données visées à l'art. 45, al. 4, let. a, d et e,

31 Nouvelle teneur selon l'annexe 2 ch. 4, en vigueur depuis le 1er janv. 2024 (RO **2022** 232; **2023** 650; FF **2017** 2465).
32 RS **330**
33 RS **361**
34 RS **121**
35 Introduite par le ch. II 2 de la LF du 17 juin 2022, en vigueur depuis le 1er janv. 2024 (RO **2023** 117, 650; FF **2021** 3046).
36 RS **514.54**
37 RS **510.91**

2. par une interface liée au système d'information visé à l'art. 18 LSIA, dans les buts définis à l'art. 19 LSIA: les données visées à l'art. 45, al. 4, let. a et e;
3. par une interface liée au système d'information visé à l'art. 156 LSIA, dans le but visé à l'art. 157 LSIA: les données visées à l'art. 45, al. 4, let. a et e,
4. par une interface liée au système d'information visé à l'art. 162 LSIA, dans le but visé à l'art. 163 LSIA: les données visées à l'art. 45, al. 4, let. a et e;

c. le service compétent pour délivrer des certificats internationaux de sécurité au sens de l'art. 48, let. c, par une interface: les données visées à l'art. 45, al. 4, let. a, d et e.

3 Les services spécialisés CSP peuvent au surplus communiquer électroniquement les données visées à l'art. 45, al. 4, let. a et e, à d'autres services de la Confédération dans la mesure où ces données sont nécessaires pour contrôler l'accès aux zones de sécurité.

4 Ils peuvent communiquer aux autorités et organisations soumises à la présente loi les listes et statistiques visées à l'art. 45, al. 1, let. g, dans la mesure où elles en ont besoin pour exécuter les tâches de contrôle prévues par la présente loi.

Art. 47 Conservation, archivage et destruction des données

1 Les services spécialisés CSP peuvent enregistrer les auditions visées à l'art. 34, al. 2, let. d, et 3, et conserver les enregistrements sur des supports.

2 Ils conservent les données aussi longtemps que la personne concernée exerce l'activité sensible, mais dix ans au plus.

3 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

4 Lorsque la procédure est classée ou que les services spécialisés CSP apprennent qu'une personne contrôlée n'occupe pas la fonction prévue ou a refusé d'exécuter le mandat prévu, ces services détruisent l'ensemble des données et dossiers relatifs à la procédure dans les trois mois.

Section 6 Dispositions édictées par le Conseil fédéral

Art. 48

Le Conseil fédéral règle:

a. les modalités de la procédure du contrôle de sécurité relatif aux personnes;
b. l'organisation des services spécialisés CSP;
c. les modalités de délivrance des certificats internationaux de sécurité;

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

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

Chapitre 4 Procédure de sécurité relative aux entreprises

Section 1 Dispositions générales

Art. 49 But de la procédure

La procédure de sécurité relative aux entreprises vise à préserver la sécurité de l'information lors de l'exécution de mandats publics par des entreprises, des parties d'entre elles ou des sous-contractants (entreprises), dans la mesure où ces mandats impliquent l'exercice d'une activité sensible (mandats sensibles).

Art. 50 Entreprises concernées

1 Les entreprises suivantes peuvent être soumises à la procédure de sécurité:

a. entreprises appelées à exécuter un mandat sensible pour le compte d'une autorité ou d'une organisation soumise à la présente loi;

b. entreprises dont le siège est en Suisse et qui soumissionnent pour des mandats dont l'exécution requiert un certificat international de sécurité au sens de l'art. 66.

2 La procédure ne peut être menée sans le consentement de l'entreprise concernée.

3 Les entreprises visées à l'al. 1, let. b, supportent les coûts de la procédure.

Art. 51 Classement de la procédure

1 La procédure de sécurité est classée dans les cas suivants:

a. l'entreprise concernée revient sur son consentement ou ne collabore pas à la procédure;

b. l'entreprise concernée retire son offre;

c. l'entreprise concernée n'entre plus en considération pour l'exécution du mandat.

2 Le service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) communique le classement de la procédure à l'entreprise et à l'autorité ou l'organisation qui attribue le mandat (adjudicateur).

Section 2 Ouverture de la procédure

Art. 52 Demande d'ouverture de la procédure

1 Lorsque les autorités et organisations soumises à la présente loi envisagent d'attribuer un mandat sensible, elles adressent au service spécialisé PSE une demande d'ouverture de la procédure.

2 Les autorités soumises à la présente loi désignent les services compétents pour demander l'ouverture de la procédure.

3 Les autorités étrangères ou organisations internationales doivent déposer elles-mêmes une demande pour les entreprises visées à l'art. 50, al. 1, let. b.

Art. 53 Examen de la demande

1 Le service spécialisé PSE examine la demande et ouvre la procédure.

2 Il peut renoncer, en accord avec l'adjudicateur, à ouvrir une procédure lorsque d'autres mesures permettent de ramener le risque pour la sécurité à un niveau acceptable. Il recommande les mesures à prendre.

Art. 54 Définition des exigences en matière de sécurité

Le service spécialisé PSE fixe, en accord avec l'adjudicateur, les exigences en matière de sécurité de l'information pour la procédure d'adjudication et la phase d'exécution du mandat.

Section 3 Évaluation des entreprises

Art. 55 Qualification

1 L'adjudicateur indique au service spécialisé PSE quelles entreprises entrent en considération pour l'exécution du mandat sensible.

2 Le service spécialisé PSE évalue si les entreprises concernées présentent les qualifications requises sous l'angle de la sécurité pour exécuter le mandat sensible ou s'il existe un risque pour la sécurité.

3 Il réalise l'évaluation sans aucune instruction.

Art. 56 Collecte des données

1 Pour évaluer la qualification d'une entreprise, le service spécialisé PSE peut collecter des données auprès des sources suivantes:

a. l'entreprise concernée;

b. le SRC;

c. toute source d'information publique.

2 Il peut demander à des services étrangers ou internationaux de lui transmettre des données. La demande est adressée par l'intermédiaire du SRC.

Art. 57 Évaluation du risque pour la sécurité

1 Il existe un risque pour la sécurité lorsque des indices concrets fondés sur les données collectées laissent supposer avec une probabilité élevée que l'entreprise exécutera le mandat sensible de manière inadéquate ou contraire aux prescriptions.

2 La probabilité d'une exécution inadéquate ou contraire aux prescriptions du mandat sensible peut être jugée élevée dans les cas suivants notamment:

a. l'entreprise manque d'intégrité ou de loyauté;

b. l'entreprise est contrôlée par des États étrangers ou des organisations étrangères de droit public ou privé ou se trouve sous leur influence, lorsque ce contrôle ou cette influence sont incompatibles avec les intérêts définis à l'art. 1, al. 2;

c. un service spécialisé CSP a rendu une déclaration de risque pour un membre du personnel de l'entreprise et cette personne est indispensable pour l'exécution du mandat.

3 L'évaluation doit se fonder sur des faits concernant la situation de l'entreprise, indépendamment de toute faute commise.

Art. 58 Notification de l'évaluation et exclusion de la procédure d'adjudication

1 Le service spécialisé PSE communique son évaluation à l'adjudicateur et la notifie formellement à l'entreprise.

2 Si le service spécialisé PSE conclut que l'exécution du mandat sensible par l'entreprise concernée pose un risque pour la sécurité, l'adjudicateur exclut l'entreprise de la procédure d'adjudication.

3 Si toutes les entreprises qui entrent en considération posent un risque pour la sécurité, l'adjudicateur peut néanmoins confier le mandat à l'une d'entre elles. Le service spécialisé PSE classe la procédure. L'adjudicateur applique par analogie les mesures visées aux art. 59, 60, 63 et 64.

Section 4 Plan de sécurité

Art. 59 Adjudication et plan de sécurité

1 L'adjudicateur indique au service spécialisé PSE quelle est l'entreprise adjudicataire.

2 L'entreprise établit un plan de sécurité en suivant les directives du service spécialisé PSE.

3 Le plan de sécurité est soumis au contrôle du service spécialisé PSE. Ce dernier peut collecter les données nécessaires par écrit ou inspecter les locaux de l'entreprise.

Art. 60 Contrôles de sécurité relatifs aux personnes

1 Les collaborateurs de l'entreprise qui sont appelés à exercer une activité sensible sont soumis à un contrôle de sécurité.

2 Le service spécialisé PSE est compétent pour la décision au sens de l'art. 41, al. 2. Si la procédure de sécurité relative aux entreprises est classée conformément à l'art. 58, al. 3, parce qu'aucune entreprise ne présente les qualifications requises pour exécuter le mandat, l'adjudicateur prend la décision.

Section 5 Déclaration de sécurité relative aux entreprises

Art. 61 Établissement de la déclaration de sécurité relative aux entreprises

1 Le service spécialisé PSE rend formellement une déclaration de sécurité lorsque l'entreprise apporte la preuve qu'elle a mis en œuvre le plan de sécurité.

2 Il refuse à l'entreprise la déclaration de sécurité et classe la procédure si l'entreprise ne met pas en œuvre le plan de sécurité. Il rend formellement une décision en conséquence.

3 Les décisions visées aux al. 1 et 2 sont communiquées à l'adjudicateur.

4 L'adjudicateur est lié par la décision du service spécialisé PSE, sous réserve de l'art. 58, al. 3.

5 La déclaration de sécurité est valable cinq ans.

Art. 62 Exécution d'un mandat sensible

L'adjudicateur ne peut laisser une entreprise exécuter un mandat sensible qu'une fois que celle-ci a obtenu une déclaration de sécurité.

Art. 63 Obligations de l'entreprise

1 Les entreprises qui ont obtenu une déclaration de sécurité doivent constamment appliquer les mesures prévues par le plan de sécurité.

2 Elles informent immédiatement le service spécialisé PSE et l'adjudicateur de tout changement et de tout incident dans le domaine de la sécurité.

Art. 64 Contrôles et mesures de protection

1 Le service spécialisé PSE peut:

a. inspecter inopinément les secteurs où le mandat sensible est exécuté;
b. consulter les documents relatifs au mandat.

2 Lorsque des indices concrets donnent à penser que la sécurité de l'information est menacée dans une entreprise, le service spécialisé PSE peut prendre immédiatement les mesures de protection qui s'imposent, notamment mettre les documents et le matériel en lieu sûr.

Art. 65 Procédure simplifiée en cas d'adjudication d'autres mandats sensibles

Les entreprises qui ont obtenu une déclaration de sécurité sont réputées qualifiées en cas d'adjudication d'autres mandats sensibles. Le service spécialisé PSE examine la nécessité d'adapter le plan de sécurité.

Art. 66 Certificat international de sécurité

Le service spécialisé PSE établit à la demande de l'entreprise un certificat international de sécurité.

Art. 67 Révocation de la déclaration de sécurité

1 Le service spécialisé PSE révoque la déclaration de sécurité dans les cas suivants:

a. l'entreprise n'a pas rempli ses obligations au sens de l'art. 63;

b. une répétition de la procédure a permis d'identifier un risque pour la sécurité.

2 Il notifie sa décision à l'entreprise et à l'adjudicateur.

3 En cas de révocation de la déclaration de sécurité, l'adjudicateur retire immédiatement le mandat à l'entreprise, sous réserve de l'art. 58, al. 3. L'entreprise n'a droit à aucune indemnisation.

Section 6 Répétition de la procédure et voies de droit

Art. 68 Répétition de la procédure

La procédure de sécurité est répétée dans les cas suivants:

a. la déclaration de sécurité de l'entreprise échoit alors que l'entreprise exécute un mandat sensible;

b. des changements importants sont intervenus au sein de l'entreprise et des indices concrets donnent à penser que ces changements ont fait apparaître de nouveaux risques pour la sécurité.

Art. 69 Voies de droit

1 L'entreprise a 30 jours à compter de la notification de la décision du service spécialisé PSE pour:

a. consulter le dossier du contrôle;

b. demander la rectification des données erronées ou la destruction des données obsolètes;

c. demander que l'on ajoute à une donnée la mention de son caractère litigieux;

d. faire recours devant le Tribunal administratif fédéral.

2 Les restrictions à la communication de renseignements sont régies par l'art. 26 LPD[38].[39]

Section 7 Traitement des données personnelles

Art. 70 Système d'information sur la procédure de sécurité relative aux entreprises

1 Le service spécialisé PSE exploite un système d'information pour réaliser et gérer les procédures de sécurité relatives aux entreprises.

2 Les données sensibles et au sens de l'art. 5, let. c, LPD[40] peuvent être traitées dans le système d'information dans la mesure où elles sont nécessaires à l'exécution de la procédure.[41]

3 Le système d'information contient les données suivantes:

a. les données visées aux art. 56 et 59, al. 3;

b. le résultat de l'évaluation visée à l'art. 55, al. 2;

c. le résultat des contrôles de sécurité relatifs aux personnes visés à l'art. 60, al. 1;

d. la décision du service spécialisé PSE visée à l'art. 60, al. 2;

e. la raison sociale des entreprises qui ont obtenu une déclaration de sécurité;

f. les mesures de protection visées à l'art. 64;

g. les données et les dossiers relatifs aux procédures de recours.

4 Le service spécialisé PSE est responsable de la sécurité du système d'information et de la licéité du traitement des données personnelles.

Art. 71 Consultation et communication des données

1 Les organes suivants peuvent consulter en ligne les données ci-après:

a. les adjudicateurs: les données visées à l'art. 70, al. 3, let. b et d à g;

38 RS **235.1**

39 Nouvelle teneur selon l'annexe 2 ch. 5, en vigueur depuis le 1er janv. 2024 (RO **2022** 232; **2023** 650; FF **2017** 2465).

40 RS **235.1**

41 Nouvelle teneur selon l'annexe 2 ch. 5, en vigueur depuis le 1er janv. 2024 (RO **2022** 232; **2023** 650; FF **2017** 2465).

b. les entreprises qui sont habilitées par le Conseil fédéral, en vertu de l'art. 31, al. 1, let. a, à ouvrir des procédures de contrôle de sécurité relatifs aux personnes dans leur domaine de compétence: les données visées à l'art. 70, al. 3, let. d.

2 Le service spécialisé PSE peut au surplus communiquer les données visées à l'art. 70, al. 3, let. b à d, à d'autres services de la Confédération dans la mesure où ces données sont nécessaires à la sécurité de l'information.

Art. 72 Conservation, archivage et destruction des données

1 Le service spécialisé PSE conserve les données aussi longtemps que l'entreprise concernée dispose d'une déclaration de sécurité, mais dix ans au plus.

2 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

3 Lorsque la procédure est classée, le service spécialisé PSE détruit l'ensemble des données et dossiers relatifs à la procédure dans les trois mois.

Section 8 Dispositions édictées par le Conseil fédéral

Art. 73

Le Conseil fédéral règle:

a. les modalités de la procédure de sécurité relative aux entreprises;

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

c. l'organisation du service spécialisé PSE;

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

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

Chapitre 5
Mesures de la Confédération afin de protéger la Suisse contre les cybermenaces[42]

Section 1 Dispositions générales[43]

Art. 73*a*[44] Principe

[1] Afin de protéger la Suisse contre les cybermenaces, l'OFCS réalise des analyses techniques pour évaluer et contrer les cyberincidents et les cybermenaces, ainsi que pour identifier et éliminer les vulnérabilités.

[2] Sur la base de ces analyses, l'OFCS assume notamment les tâches suivantes:

a. sensibiliser le public aux cybermenaces et l'alerter sur de telles menaces;

b. alerter les autorités, les organisations et les personnes concernées en cas de cybermenace immédiate ou de cyberattaque en cours;

c. publier des informations sur la cybersécurité et des recommandations sur les mesures préventives et réactives à prendre contre les cyberincidents;

d. réceptionner et traiter les signalements concernant les cyberincidents et les cybermenaces;

e. soutenir les exploitants d'infrastructures critiques.

Art. 73*b*[45] Signalements

[1] L'OFCS reçoit des signalements concernant des cyberincidents et des cybermenaces. Les signalements peuvent être anonymes.

[2] L'OFCS analyse les signalements au regard de leur importance pour la protection de la Suisse contre les cybermenaces. Sur demande, il émet une recommandation quant aux mesures à prendre, pour autant qu'aucune analyse ou clarification supplémentaire ne soit nécessaire à cet effet.

[3] Si l'OFCS prend connaissance d'une vulnérabilité, il en informe immédiatement le fabricant du matériel informatique ou du logiciel concerné et lui fixe un délai approprié pour l'éliminer. Il lui indique que tout manquement pourra être sanctionné en vertu du droit des marchés publics (art. 44, al. 1, let. f[bis], de la loi fédérale du 21 juin

42 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

43 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

44 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

45 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

2019 sur les marchés publics[46]) et qu'à l'expiration du délai, il pourra rendre publique la vulnérabilité en vertu de l'art. 73*c*, al. 2.

Art. 73*c*[47] Publication d'informations provenant de signalements

[1] L'OFCS peut publier des informations relatives à des cyberincidents pour autant que cela serve à la protection contre les cybermenaces. Ces informations ne peuvent contenir de données relatives aux personnes physiques ou morales concernées que si ces dernières y consentent et que ces données sont des caractères d'identification et des ressources d'adressage utilisés de manière abusive.

[2] L'OFCS peut publier des informations relatives à des vulnérabilités en indiquant le matériel informatique ou le logiciel concerné, à condition que le fabricant y consente ou qu'il n'ait pas éliminé la vulnérabilité dans le délai visé à l'art. 73*b*, al. 3.

Art. 73*d*[48] Transmission d'informations

[1] L'OFCS peut transmettre des informations provenant de signalements aux autorités et aux organisations actives dans le domaine de la cybersécurité. Ces informations ne peuvent contenir de données personnelles que si la personne concernée y consent.

[2] Si le signalement d'un cyberincident ou son analyse révèle que des informations sont nécessaires pour déceler à temps et prévenir des menaces pour la sûreté intérieure ou extérieure, pour apprécier la menace ou pour assurer un service d'alerte précoce en vue de protéger les infrastructures critiques conformément à l'art. 6, al. 1, let. a, 2 et 5, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[49], l'OFCS transmet ces informations au SRC.

[3] En dérogation à l'art. 22*a*, al. 1, de la loi du 24 mars 2000 sur le personnel de la Confédération[50], les collaborateurs de l'OFCS qui, dans le cadre d'un signalement ou de son analyse, obtiennent des informations sur une possible infraction la rapportent exclusivement au directeur de l'OFCS. Celui-ci peut dénoncer cette possible infraction aux autorités de poursuite pénale si la gravité de cette dernière le justifie.

[4] La transmission par l'OFCS de secrets protégés par le droit pénal doit obéir aux exigences prévues à l'art. 320 du code pénal[51].

46 RS **172.056.1**
47 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
48 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
49 RS **121**
50 RS **172.220.1**
51 RS **311.0**

Art. 74[52] Soutien aux exploitants d'infrastructures critiques

[1] L'OFCS aide les exploitants d'infrastructures critiques à se protéger contre les cybermenaces.

[2] Il met notamment à leur disposition, à titre gratuit et pour une utilisation sur une base volontaire, les outils suivants:

a. un système de communication permettant l'échange sécurisé d'informations;

b. des informations techniques sur les cybermenaces en cours et des recommandations sur les mesures préventives et réactives à prendre contre les cyberincidents;

c. des instruments techniques et des instructions de détection des cyberincidents visant à répondre aux besoins accrus de protection des infrastructures critiques.

[3] Il peut les conseiller et les soutenir dans la gestion des cyberincidents et l'élimination des vulnérabilités lorsque le fonctionnement de l'infrastructure critique concernée est mis en péril et, s'il s'agit d'exploitants privés, qu'il n'est pas possible d'obtenir en temps voulu un soutien équivalent sur le marché.

[4] Avec l'accord de l'exploitant concerné, il peut accéder aux informations et aux moyens informatiques de celui-ci pour analyser un cyberincident.

Section 2[53] Obligation de signaler les cyberattaques

Art. 74*a* Principes

[1] Les autorités et les organisations énumérées à l'art. 74*b* veillent à ce que les cyberattaques visant leurs moyens informatiques soient signalées à l'OFCS.

[2] L'OFCS renseigne les autorités et les organisations intéressées sur leur éventuel assujettissement à l'obligation de signaler et, sur demande, rend une décision sur ce point.

[3] Lorsqu'elles signalent une cyberattaque, les autorités et les organisations assujetties ont droit, dans la gestion de l'incident, au soutien de l'OFCS prévu à l'art. 74, al. 3.

[4] L'obligation de signaler vise uniquement à permettre à l'OFCS de détecter à un stade précoce les modes opératoires utilisés lors des attaques visant les infrastructures critiques et, ainsi, d'avertir les victimes potentielles et de leur recommander les mesures préventives et réactives qui s'imposent.

52 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

53 Introduite par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

Art. 74*b* Autorités et organisations assujetties à l'obligation de signaler

[1] L'obligation de signaler s'applique:

a. aux hautes écoles au sens de l'art. 2, al. 2, de la loi du 30 septembre 2011 sur l'encouragement et la coordination des hautes écoles[54];

b. aux autorités fédérales, cantonales et communales ainsi qu'aux organisations intercantonales, cantonales et intercommunales, à l'exception du Groupement Défense lorsque l'armée accomplit un service d'appui ou un service actif au sens des art. 67 et 76 de la loi du 3 février 1995 sur l'armée[55];

c. aux organisations chargées de tâches de droit public dans les domaines de la sécurité et du sauvetage, de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets;

d. aux entreprises œuvrant dans les domaines de l'approvisionnement énergétique au sens de l'art. 6, al. 1, de la loi du 30 septembre 2016 sur l'énergie[56] ainsi que du commerce, de la mesure et de la gestion de l'énergie, à l'exception des détenteurs d'une autorisation au sens de la loi du 21 mars 2003 sur l'énergie nucléaire[57] si une cyberattaque est lancée contre une installation nucléaire;

e. aux entreprises soumises à la loi du 8 novembre 1934 sur les banques[58], à la loi du 17 décembre 2004 sur la surveillance des assurances[59] ou à la loi du 19 juin 2015 sur l'infrastructure des marchés financiers[60];

f. aux établissements de santé figurant sur la liste hospitalière cantonale conformément à l'art. 39, al. 1, let. e, de la loi fédérale du 18 mars 1994 sur l'assurance-maladie[61];

g. aux laboratoires médicaux titulaires d'une autorisation conformément à l'art. 16, al. 1, de la loi du 28 septembre 2012 sur les épidémies[62];

h. aux entreprises titulaires d'une autorisation de fabriquer, de mettre sur le marché ou d'importer des médicaments conformément à la loi du 15 décembre 2000 sur les produits thérapeutiques[63];

i. aux organisations qui fournissent des prestations destinées à couvrir les conséquences de la maladie, des accidents, de l'incapacité de travail et de gain, de la vieillesse, de l'invalidité et de l'impotence;

j. à la Société suisse de radiodiffusion et télévision;

k. aux agences de presse d'importance nationale;

54 RS **414.20**
55 RS **510.10**
56 RS **730.0**
57 RS **732.1**
58 RS **952.0**
59 RS **961.01**
60 RS **958.1**
61 RS **832.10**
62 RS **818.101**
63 RS **812.21**

l. aux prestataires de services postaux enregistrés auprès de la Commission de la poste conformément à l'art. 4, al. 1, de la loi du 17 décembre 2010 sur la poste[64];

m. aux entreprises ferroviaires visées à l'art. 5 ou 8*c* de la loi fédérale du 20 décembre 1957 sur les chemins de fer[65] ainsi qu'aux entreprises d'installations à câbles, de trolleybus, d'autobus et de navigation concessionnaires au sens de l'art. 6 de la loi du 20 mars 2009 sur le transport de voyageurs[66];

n. aux entreprises de l'aviation civile disposant d'une autorisation délivrée par l'Office fédéral de l'aviation civile et aux aéroports nationaux figurant dans le Plan sectoriel de l'infrastructure aéronautique;

o. aux entreprises qui transportent des marchandises sur le Rhin conformément à la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse[67] et aux entreprises qui effectuent l'enregistrement, le chargement ou le déchargement de marchandises dans le port de Bâle;

p. aux entreprises qui approvisionnent la population en biens d'usage quotidien indispensables et dont la défaillance partielle ou complète entraînerait de graves difficultés d'approvisionnement;

q. aux fournisseurs de services de télécommunication enregistrés auprès de l'Office fédéral de la communication conformément à l'art. 4, al. 1, LTC[68];

r. aux registres et aux registraires de domaines Internet au sens de l'art. 28*b* LTC;

s. aux fournisseurs et aux exploitants de services et d'infrastructures servant à l'exercice des droits politiques;

t. aux fournisseurs et aux exploitants d'informatique en nuage, de moteurs de recherche, de services numériques de sécurité ou de confiance ainsi que de centres de calcul, pour autant qu'ils aient un siège en Suisse;

u. aux fabricants de matériel informatique ou de logiciels dont les produits sont utilisés par des infrastructures critiques, si le matériel ou les logiciels concernés disposent d'un accès de télémaintenance ou sont utilisés à l'une des fins suivantes:

1. commande et surveillance de systèmes et de processus techniques,
2. garantie de la sécurité publique.

2 Les autorités et les organisations qui exercent également des activités ne relevant pas de l'al. 1 n'ont pas l'obligation de signaler les cyberattaques qui ont un effet uniquement sur ces activités.

3 L'obligation de signaler visée à l'al. 1 s'applique aux cyberattaques qui ont un effet en Suisse, même si les moyens informatiques concernés se trouvent à l'étranger.

64 RS **783.0**
65 RS **742.101**
66 RS **745.1**
67 RS **747.30**
68 RS **784.10**

Art. 74*c* Exceptions à l'obligation de signaler

Le Conseil fédéral exempte les autorités et les organisations de l'obligation de signaler visée à l'art. 74*b* lorsque les perturbations provoquées par les cyberattaques n'ont qu'un effet limité sur le fonctionnement de l'économie ou sur le bien-être de la population.

Art. 74*d* Cyberattaques à signaler

Une cyberattaque doit être signalée lorsqu'elle:

a. met en péril le fonctionnement de l'infrastructure critique concernée;

b. a entraîné une manipulation ou une fuite d'informations;

c. n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou

d. s'accompagne d'actes de chantage, de menaces ou de contrainte.

Art. 74*e* Délai et contenu du signalement

1 Le signalement doit être fait dans les 24 heures suivant la détection de la cyberattaque.

2 Il doit contenir des informations sur l'autorité ou l'organisation assujetties à l'obligation de signaler, sur le type et l'exécution de la cyberattaque sur ses effets, sur les mesures prises et, si elles sont connues, sur les mesures prévues.

3 Si toutes les informations requises ne sont pas connues au moment du signalement, l'autorité ou l'organisation assujettie complète le signalement dès qu'elle dispose de nouvelles informations.

4 Celui qui assume l'obligation de signaler pour une autorité ou une organisation n'est pas tenu, dans le cadre du signalement, de fournir des informations qui l'exposent à des poursuites pénales.

5 L'OFCS informe l'autorité ou l'organisation assujettie dès que toutes les données permettant de satisfaire à l'obligation de signaler sont disponibles.

Art. 74*f* Communication du signalement

1 L'OFCS met à disposition un système sécurisé qui permet de lui communiquer le signalement des cyberattaques par voie électronique.

2 Le système doit permettre aux autorités ou aux organisations assujetties de communiquer simultanément à d'autres autorités tout ou partie du signalement de la cyberattaque ou de ses effets.

3 Si des informations dépassant le cadre prévu à l'art. 74*e* sont nécessaires à l'exécution d'une obligation de signaler vis-à-vis d'autres autorités, le système doit permettre aux autorités ou aux organisations assujetties de les communiquer directement aux autorités concernées, sans que l'OFCS y ait accès.

Section 3 Protection des données et échange d'informations[69]

Art. 75[70] Traitement des données personnelles

[1] Pour accomplir ses tâches, l'OFCS peut traiter des données personnelles, y compris les ressources d'adressage au sens de l'art. 3, let. f, LTC[71] et les données sensibles qui s'y rapportent, qui contiennent des informations relatives:

a. à des opinions religieuses, philosophiques ou politiques; le traitement des données n'est admissible que dans la mesure où il est nécessaire à l'évaluation de menaces et de dangers concrets en matière de cybersécurité;

b. à des poursuites ou à des sanctions pénales ou administratives.

[2] Lors du traitement de données personnelles ou en cas de soupçon fondé d'usurpation d'identité ou d'utilisation abusive de ressources d'adressage, l'OFCS en informe les personnes concernées si cela n'entraîne pas des efforts disproportionnés et qu'aucun intérêt public prépondérant ne s'y oppose.

Art. 76[72] Collaboration sur le plan national

[1] L'OFCS et les exploitants d'infrastructures peuvent communiquer entre eux des données personnelles dans la mesure où cela est nécessaire à la protection contre des cybermenaces.

[2] L'OFCS et les fournisseurs de services de télécommunication peuvent communiquer entre eux des ressources d'adressage et les données personnelles qui s'y rapportent dans la mesure où cela est nécessaire à la protection contre des cybermenaces.

Art. 76*a*[73] Soutien aux autorités

[1] L'OFCS apporte son soutien au SRC en lui fournissant des évaluations périodiques du nombre, du type et de l'ampleur des cyberattaques ainsi que, sur demande, des analyses techniques des cybermenaces.

[2] Il octroie au SRC l'accès à des informations concernant l'identité ou le mode opératoire des auteurs de cyberattaques dans le but de déceler à temps et de prévenir les menaces pour la sûreté intérieure ou extérieure, d'apprécier la menace ou d'assurer un

69 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

70 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

71 RS **784.10**

72 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

73 Introduit par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

service d'alerte précoce en vue de protéger les infrastructures critiques au sens de l'art. 6, al. 1, let. a, 2 et 5, LRens[74].

3 Il octroie aux autorités de poursuite pénale l'accès à des informations concernant l'identité et le mode opératoire des auteurs de cyberattaques.

4 Il octroie aux services cantonaux chargés de la cybersécurité l'accès aux informations nécessaires à la protection contre les cybermenaces.

Art. 77[75] Coopération internationale

1 L'OFCS peut échanger avec des services étrangers ou internationaux chargés de la cybersécurité des informations permettant de connaître l'identité ou le mode opératoire des auteurs de cyberattaques s'ils en ont besoin pour accomplir des tâches qui correspondent à celles de l'OFCS. Si l'échange d'informations comprend également des données personnelles, les art. 16 et 17 LPD[76] sont applicables.

2 L'échange d'informations au sens de l'al. 1 n'est autorisé que si les services étrangers ou internationaux garantissent que les données seront utilisées conformément aux fins prévues.

Art. 78[77]

Art. 79 Conservation et archivage des données

1 L'OFCS conserve les données personnelles aussi longtemps que celles-ci sont utiles pour détecter des cybermenaces ou gérer des cyberincidents, mais durant cinq ans au plus à compter de leur dernière utilisation à cette fin. Pour les données sensibles, le délai est de deux ans.[78]

2 L'archivage des données est régi par les dispositions de la législation relative à l'archivage.

Art. 80[79]

74 RS **121**
75 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
76 RS **235.1**
77 Abrogé par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), avec effet au 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
78 Nouvelle teneur selon le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), en vigueur depuis le 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).
79 Abrogé par le ch. I de la LF du 29 sept. 2023 (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), avec effet au 1er avr. 2025 (RO **2024** 257; **2025** 173; FF **2023** 84).

Chapitre 6 Organisation et exécution
Section 1 Organisation

Art. 81 Préposés à la sécurité de l'information

1 Les autorités et organisations suivantes désignent, chacune dans son domaine de compétence, un préposé à la sécurité de l'information et un suppléant:

a. le Conseil fédéral;

b. la Délégation administrative de l'Assemblée fédérale;

c. les tribunaux de la Confédération;

d. le Ministère public de la Confédération;

e. la Banque nationale suisse;

f. les départements et la Chancellerie fédérale.

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

a. conseiller et aider dans leur domaine les services compétents dans l'accomplissement des tâches et l'exécution des obligations qui leur incombent en vertu de la présente loi;

b. diriger, sur mandat de l'autorité ou de l'organisation à laquelle ils sont subordonnés, l'organisation spécialisée chargée de la sécurité de l'information et la gestion des risques;

c. vérifier, sur mandat de l'autorité ou de l'organisation à laquelle ils sont subordonnés, le respect des prescriptions relatives à la sécurité de l'information, en rendre compte et proposer les mesures qui s'imposent;

d. signaler, sur une base volontaire, les incidents dans le domaine de la sécurité de l'information au service spécialisé de la Confédération pour la sécurité de l'information et aux services visés à l'art. 74, al. 5.

3 Aucune tâche susceptible d'entrer en conflit avec l'une des tâches visées à l'al. 2 ne peut être confiée aux préposés à la sécurité de l'information.

Art. 82 Conférence des préposés à la sécurité de l'information

1 La Conférence des préposés à la sécurité de l'information se compose des préposés à la sécurité de l'information au sens de l'art. 81, al. 1, de deux représentants des cantons et du Préposé fédéral à la protection des données et à la transparence.

2 Elle accomplit les tâches suivantes:

a. promouvoir l'exécution uniforme de la présente loi;

b. contribuer à la normalisation des exigences et mesures visées à l'art. 85;

c. conseiller le service spécialisé de la Confédération pour la sécurité de l'information sur tous les aspects de la coordination de l'exécution et sur tous les points d'importance stratégique;

d. veiller à l'échange d'informations, notamment sur la gestion des risques et sur les problèmes et les incidents dans le domaine de la sécurité de l'information;

e. assurer la coordination avec les autres services qui accomplissent des tâches dans le domaine de la sécurité de l'information.

3 Elle édicte son règlement interne.

Art. 83 Service spécialisé de la Confédération pour la sécurité de l'information

1 Le service spécialisé de la Confédération pour la sécurité de l'information:

a. conseille et soutient les autorités soumises à la présente loi, leurs préposés à la sécurité de l'information et les cantons dans l'exécution de la présente loi;

b. peut recommander des mesures si la sécurité de l'information de la Confédération est menacée;

c. peut mener des contrôles à la demande des autorités soumises à la présente loi;

d. peut évaluer, à la demande des autorités soumises à la présente loi, les risques liés à l'utilisation de nouvelles technologies;

e. peut examiner, à la demande des autorités et organisations soumises à la présente loi, l'adéquation de leurs processus, moyens, installations, objets et prestations par rapport aux exigences en matière de sécurité de l'information;

f. peut gérer et coordonner, à la demande des autorités soumises à la présente loi, les questions liées à la sécurité de l'information lorsque des projets importants impliquent plusieurs autorités;

g. sert d'interlocuteur pour les contacts spécialisés avec des services nationaux, étrangers ou internationaux;

h. rend compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération.

2 Le préposé du Conseil fédéral à la sécurité de l'information dirige le service spécialisé de la Confédération pour la sécurité de l'information.

3 Le Conseil fédéral règle l'organisation du service spécialisé de la Confédération pour la sécurité de l'information. Il peut le charger d'autres tâches pour le compte de l'administration fédérale ou de l'armée.

Section 2 Exécution

Art. 84 Dispositions d'exécution

1 Les autorités soumises à la présente loi édictent les dispositions d'exécution. Le Conseil fédéral peut charger la Chancellerie fédérale d'édicter des dispositions d'exécution pour les affaires du Conseil fédéral.

2 Les compétences que la présente loi donne aux autorités soumises à la présente loi sont exercées, pour l'Assemblée fédérale, par la Délégation administrative de l'Assemblée fédérale.

3 Les dispositions d'exécution du Conseil fédéral s'appliquent par analogie aux autorités soumises à la présente loi si elles n'édictent pas leurs propres dispositions d'exécution.

Art. 85 Exigences et mesures standard

1 Le Conseil fédéral fixe des exigences standard en matière de sécurité et définit des mesures standard en matière d'organisation, de personnel et de construction, de même que sur le plan technique, pour assurer la sécurité de l'information; il suit à cet effet l'avancement des connaissances et de la technique.

2 Il peut déléguer cette tâche.

3 Les exigences et mesures standard du Conseil fédéral ont valeur de recommandations, sauf si les autorités soumises à la présente loi les déclarent obligatoires.

Art. 86 Cantons

1 Les cantons veillent au contrôle périodique de la mise en œuvre et de l'efficacité de la sécurité de l'information visée à l'art. 3.

2 Ils informent le service spécialisé de la Confédération pour la sécurité de l'information des résultats des contrôles visés à l'al. 1.

3 Ils désignent le service qui est l'interlocuteur des autorités soumises à la présente loi en matière de sécurité de l'information.

4 Le Conseil fédéral définit les cas dans lesquels les cantons peuvent recourir aux prestations des services spécialisés visés par la présente loi afin d'assurer leur propre sécurité de l'information. Ces prestations sont soumises à des émoluments. Leur montant est fixé par le Conseil fédéral.

Art. 87 Traités internationaux

Le Conseil fédéral peut conclure des traités internationaux en matière de sécurité de l'information portant sur les objets suivants:

a. l'échange d'informations sur des menaces, des vulnérabilités et des incidents dans le domaine de la sécurité de l'information, en particulier dans les infrastructures critiques;

b. l'échange d'informations classifiées;

c. l'exécution des contrôles de sécurité relatifs aux personnes et des procédures de sécurité relatives aux entreprises;

d. la reconnaissance des déclarations de sécurité;

e. l'exécution de contrôles.

Art. 88 Évaluation

[1] Le Conseil fédéral veille à ce que l'exécution, l'adéquation, l'efficacité et l'économicité de la présente loi soient contrôlés périodiquement par un service indépendant, en particulier par le Contrôle fédéral des finances.

[2] Il en rend compte régulièrement aux commissions compétentes de l'Assemblée fédérale.

Chapitre 7 Dispositions finales

Art. 89 Modification d'autres actes

La modification d'autres actes est réglée en annexe 1.

Art. 90 Dispositions transitoires

[1] Les informations classifiées selon l'ancien droit sont adaptées aux règles de classification du nouveau droit dès leur premier traitement faisant suite à l'entrée en vigueur de la présente loi.

[2] Les moyens informatiques doivent être classés dans un délai de deux ans à compter de l'entrée en vigueur de la présente loi. Les mesures techniques visant à assurer la sécurité de l'information doivent être mises en place dans un délai de six ans à compter de l'entrée en vigueur de la présente loi.

[3] Les déclarations relatives à la sécurité des personnes et les déclarations relatives à la sécurité des entreprises rendues selon l'ancien droit sont valables cinq ans à compter de leur établissement.

Art. 91 Dispositions de coordination

La coordination de la présente loi avec d'autres actes est réglée dans l'annexe 2.

Art. 92 Référendum et entrée en vigueur

[1] La présente loi est sujette au référendum.

[2] Le Conseil fédéral fixe la date de l'entrée en vigueur.

Date de l'entrée en vigueur:
Art. 87: 1er mai 2022[80]
Autres dispositions: 1er janvier 2024[81]

80 ACF du 6 avr. 2022
81 O du 8 nov. 2023 (RO **2023** 650)

Annexe 1
(art. 89)

Modification d'autres actes

Les actes mentionnés ci-après sont modifiés comme suit:

…[82]

82 Les mod. peuvent être consultées au RO **2022** 232.

Annexe 2
(art. 91)

Dispositions de coordination

…[83]

83 Les disp. de coordination peuvent être consultées au RO **2022** 232.