Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC)

du 4 décembre 2009 (Etat le 1er janvier 2014)

Le Conseil fédéral suisse,

vu l'art. 5, al. 4, de la loi fédérale du 3 octobre 2008 sur le renseignement civil (LFRC)[1],
vu les art. 10*a*, al. 5, 15, al. 3 et 5, et 30 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[2],
vu l'art. 17*a* de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[3],[4]

arrête:

Section 1 Objet et définitions

Art. 1[5] Objet

La présente ordonnance règle l'exploitation, le contenu des données et l'utilisation des systèmes d'information suivants du Service de renseignement de la Confédération (SRC):

a. Système d'information sécurité extérieure (ISAS);

b. Système d'information sécurité intérieure (ISIS);

c. Présentation électronique de la situation (PES);

d. Module informatique P4 (module P4);

e. Système de gestion électronique des affaires du SRC (GEVER SRC).

Art. 2[6] Définitions

Dans la présente ordonnance, on entend par:

a. *données:* informations enregistrées dans les systèmes d'information du SRC;

RO **2009** 7041

1 RS **121**
2 RS **120**
3 RS **235.1**
4 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
5 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
6 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

b. *objet:* regroupement de données se rapportant à une personne, une organisation, une chose ou un événement;

c. *source documentaire:* produit de la saisie structurée de données;

d. *relation:* lien entre un objet et une source documentaire;

e. *bloc de données:* ensemble des sources documentaires relatives à un objet;

f. *technique OCR:* reconnaissance optique de caractères;

g. *document original:* entrée d'information d'origine et isolée;

h. *tiers:* personne ou organisation n'ayant une importance du point de vue de la protection de l'Etat que par son lien avec un objet;

i. *consultation brève:* consultation en ligne limitée d'ISIS et d'ISAS par des services externes via l'index pour déterminer si une personne ou une organisation y figure;

j. *consultation SRC:* consultation en ligne illimitée d'ISIS et d'ISAS par les collaborateurs du SRC;

k. *consultation des services de renseignement cantonaux:* consultation en ligne limitée d'ISIS et d'ISAS par des services externes via l'index pour déterminer si une personne ou une organisation y figure et pour lire les sources documentaires saisies sur la base de documents originaux établis par les organes de sûreté des cantons en application de la LMSI.

Section 2
Dispositions générales concernant les systèmes d'information du SRC

Art. 3 But des systèmes d'information du SRC

1 Les systèmes d'information du SRC ont pour but de faciliter l'accomplissement des tâches qui incombent à ce dernier en vertu de l'art. 1 LFRC.

2 Ils sont utilisés pour:

a. l'exécution de travaux de recherche et d'analyse des données saisies;

b. l'élaboration de rapports de situation;

c. l'exécution de travaux administratifs;

d. le classement et la gestion de dossiers;

e. l'exécution de travaux de documentation;

f. la gestion des affaires.

Art. 4 Droits de consultation

1 Les utilisateurs des systèmes d'information du SRC ont accès aux données nécessaires à l'accomplissement de leurs tâches légales.

2 Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) règle les droits de consultation.

3 Le directeur du SRC ou son suppléant rend une décision sur les demandes individuelles.

4 La Gestion de l'information du SRC est chargée de la mise en œuvre des droits de consultation.

Art. 5[7] Représentation visuelle

Les objets et les sources documentaires peuvent être représentés visuellement et les représentations peuvent être enregistrées.

Art. 6[8] Recherches sur plusieurs systèmes

Les utilisateurs des systèmes d'information du SRC peuvent consulter simultanément tous les systèmes d'information du SRC, dans les limites de leur droit d'accès. Ils disposent à cet effet d'une fonction de recherche et de distribution adéquate.

Art. 7[9] Réseau SiLAN

1 Le SRC exploite un réseau informatique sécurisé (réseau SiLAN) séparé des autres réseaux informatiques.

2 Le réseau SiLAN est destiné au traitement de données classifiées.

3 Seuls les collaborateurs du SRC, de la Surveillance des services de renseignement du DDPS, du Service de renseignement de l'armée et du prestataire de services TED au sens de l'art. 15, al. 5, qui sont titulaires des droits correspondants ont accès au réseau SiLAN. Le droit d'utilisation s'applique par analogie aux mandataires auxquels les services susmentionnés ont donné le droit d'accès correspondant.

Art. 8[10] Intranet du SRC

1 L'intranet du SRC est exploité au sein du réseau SiLAN. Il est destiné à l'information des collaborateurs du SRC.

2 Seuls les collaborateurs du SRC et de la Surveillance des services de renseignement du DDPS y ont accès.

7 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
8 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
9 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
10 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Art. 8*a*[11] Index

[1] Le SRC exploite à l'extérieur du réseau SiLAN une plate-forme d'informations sécurisée (index) contenant des données classifiées jusqu'à «CONFIDENTIEL».

[2] Le SRC s'assure que toutes les personnes et organisations pertinentes pour l'exécution des tâches des utilisateurs externes d'ISIS et d'ISAS sont représentées dans l'index pour autant que la protection des sources le permette.

[3] Les utilisateurs externes d'ISIS et d'ISAS peuvent consulter l'index dans les limites de leur droit d'accès.

Art. 9 Documentation générale

[1] Le SRC gère dans ses systèmes d'information une documentation provenant de sources d'information accessibles au public contenant:

a. des informations sur des personnes, des organisations et des faits relevant de la LFRC;

b. des informations sur des personnes et des organisations dont la sécurité pourrait être menacée en Suisse;

c. des informations sur des pays et sur des contextes sociaux et politiques pouvant influer sur l'appréciation de la situation;

d. des informations scientifiques et techniques relevant du domaine d'activité des autorités de sécurité.

[2] Il exploite un portail personnalisé permettant d'utiliser des sources d'information accessibles au public (Portail interactif pour Open Sources; IPOS).

[3] Il gère un service de documentation sur le matériel propageant le racisme ou la violence. Ce service appuie les procédures pénales ou administratives qui traitent de cas impliquant ce genre de matériel.

Art. 10 Communication de données personnelles

[1] Le SRC peut communiquer les données personnelles traitées dans ses systèmes d'information aux autorités et organes officiels aux fins et aux conditions définies dans l'annexe 3 de l'ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération (OSRC)[12].

[2] Pour la communication à l'étranger, sont applicables:

a. pour les informations concernant l'étranger: les art. 5, al. 3, LFRC, et 14 OSRC;

b. pour les informations concernant la Suisse: l'art. 17, al. 3 à 5, LMSI.

[3] La communication de données n'est pas autorisée lorsque des intérêts prépondérants publics ou privés s'y opposent.

11 Introduit par le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
12 RS **121.1**

4 Lors de toute communication, le SRC renseigne le destinataire sur la fiabilité et l'actualité des données.

5 Il signale au destinataire:

a. qu'il ne peut utiliser les données que dans le but pour lequel elles lui ont été transmises; et

b. que le SRC se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

6 …[13]

Art. 11 Copie de données

1 Les données des systèmes d'information du SRC ne peuvent être copiées dans d'autres fichiers ni par le biais d'installations de communication ni au moyen de supports de données.

2 Des données des systèmes d'information du SRC peuvent être temporairement transférées dans des banques de données de travail aux fins de travaux d'analyse particuliers. Ceux-ci terminés, les données doivent être détruites.

Art. 12[14] Effacement des données

1 A l'expiration de leur durée de conservation fixée aux art. 24, 33, 35*f*, 35*k* et 35*q*, les données sont effacées dans un délai de trois mois.

2 Le bloc de données est effacé dans sa totalité lors de la suppression de la dernière source documentaire.

3 Les données destinées à être effacées sont transférées dans le module d'archivage, sous réserve de l'art. 13, al. 2.

Art. 13 Archivage

1 Le SRC propose les données et les dossiers devenus inutiles ou destinés à être détruits aux Archives fédérales aux fins d'archivage.

2 Il ne propose pas d'archiver les documents classifiés (données et dossiers) émanant des relations avec les autorités de sécurité étrangères et de la recherche opérative. Il les conserve en interne, d'entente avec les Archives fédérales, et les détruit après 45 ans.

3 Il détruit les données du module d'archivage et les dossiers correspondants que les Archives fédérales jugent sans valeur archivistique. Les autres dispositions légales en matière de destruction de données sont réservées.

13 Abrogé par le ch. I de l'O du 29 nov. 2013, avec effet au 1er janv. 2014 (RO **2013** 4359).
14 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Art. 14 Sécurité des données et journalisation

1 Pour assurer la sécurité des données, sont applicables:

a. l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[15];

b. l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale[16];

c. les conditions fixées par le DDPS selon l'art. 28 de la présente ordonnance pour le raccordement des organes cantonaux chargés du maintien de la sécurité intérieure.

2 Le SRC précise dans un règlement de traitement:

a. les mesures organisationnelles et techniques contre le traitement non autorisé des données;

b. les modalités de la journalisation automatique des données.

3 Lorsque des données du SRC sont transmises à l'extérieur du réseau SiLAN, l'ensemble de l'opération doit être réalisée sous une forme chiffrée.[17]

Art. 15 Responsabilités et compétences

1 Le SRC assume la responsabilité de ses systèmes d'information.

2 Il édicte les règlements de traitement.

3 La Gestion de l'information du SRC est chargée de la formation et de l'assistance aux utilisateurs et veille à la mise en œuvre des règlements de traitement.

4 La responsabilité technique intégrale des systèmes d'information du SRC incombe au DDPS.

5 Le prestataire de services TED veille à l'exploitation, à l'entretien et à la sécurité.

6 Les conseillers à la protection des données du SRC peuvent vérifier au cas par cas que le traitement des données dans ses systèmes d'information est bien conforme aux dispositions relatives à la protection des données.

Art. 16 Exigences techniques

1 Le DDPS détermine les exigences techniques auxquelles doivent satisfaire les terminaux des utilisateurs.

2 Les règlements de traitement déterminent les particularités pour chaque système d'information.

15 RS **235.11**

16 [RO **2003** 3687, **2007** 3401 art. 22 al. 2, **2010** 635 annexe ch. 2, **2011** 4491. RO **2011** 6093 art. 29 al. 1]. Voir actuellement l'O du 9 déc. 2011 (RS **172.010.58**).

17 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Section 3[18] Système d'information sécurité extérieure (ISAS)

Art. 17 Phase d'essai d'ISAS

[1] ISAS est exploité dans le cadre d'un essai pilote de durée déterminée au sens de l'art. 17*a* LPD.[19]

[2] Le SRC présente, dans les deux ans qui suivent la mise en exploitation d'ISAS, un rapport d'évaluation au Conseil fédéral.

[3] Le Conseil fédéral décide de la fin de l'essai pilote d'ISAS et du début de son exploitation régulière.

[4] Les dispositions des sections 1 et 2 (art. 1 à 16) sont applicables dans le cadre de l'essai pilote d'ISAS.

Art. 17*a*[20] Structure d'ISAS

[1] ISAS comprend:

a. un système de classement pour la saisie et la consultation des données visées à l'art. 18, al. 1;

b. un système d'analyse et de suivi de la situation pour la saisie et pour le traitement et l'analyse des données dans plusieurs systèmes (IASA SRC);

c. un index pour déterminer si le SRC traite des données au sens de l'art. 1, let. a, LFRC sur une personne ou une organisation.

[2] Le DDPS fixe les champs de données.

Art. 18[21] Données contenues dans ISAS

[1] ISAS contient des données pertinentes du point de vue de la politique de sécurité sur l'étranger.

[2] Il permet de traiter les données suivantes:

a. données sur l'identité des personnes ou des organisations enregistrées;

b. enregistrements sonores ou visuels;

c. données alphanumériques relatives à des événements ou à des personnes, telles que l'immatriculation de véhicules, et données concernant des raccordements de télécommunication.

[3] Les données sont classées en objet, source documentaire ou document original.

18 La durée de validité est limitée au 31 déc. 2014.
19 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
20 Introduit par le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
21 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

4 Les données de l'ancien Service de renseignement stratégique sur les thèmes du terrorisme et de la non-prolifération qui sont disponibles sous forme électronique sont transférées dans ISAS.**Art. 19**[22]

Art. 20[23] Droits d'accès

1 Les collaborateurs du SRC chargés de mener à bien l'essai pilote d'ISAS ont accès en ligne à ISAS et aux données de l'index pour autant que l'accomplissement de leurs tâches légales le requiert.

2 Ont accès en ligne à l'index les collaborateurs des autorités suivantes chargés de mener à bien l'essai pilote d'ISAS:

a. l'organe de sûreté cantonal désigné par le chef du DDPS pour accomplir les tâches que lui assigne la LMSI;

b. les services fédéraux compétents pour les contrôles de sécurité relatifs aux personnes en vue d'exécuter ces contrôles.

Art. 21[24] Saisie des données et contrôle de la qualité

1 Seules les informations qui répondent aux buts définis à l'art. 3 peuvent être traitées dans ISAS.

2 Les collaborateurs du SRC chargés du triage versent les documents originaux dans le système de classement.

3 Les collaborateurs du SRC chargés de mener à bien l'essai pilote d'ISAS saisissent les données dans ISAS en se fondant sur les documents originaux.

4 Le directeur du SRC ou son suppléant peut charger le service responsable du contrôle de la qualité du SRC (service d'assurance de la qualité) de vérifier les données enregistrées dans ISAS.

5 Le service d'assurance de la qualité efface les données devenues inutiles.

Art. 22[25] Classement des dossiers

1 Le classement des dossiers vise à garantir la gestion et l'archivage en bonne et due forme des dossiers.

2 Les documents originaux peuvent être saisis à l'aide de la technique OCR.

3 Il n'est pas nécessaire de classer les documents originaux sur papier lorsqu'ils ont été saisis sous forme électronique.

22 Abrogé par le ch. I de l'O du 9 déc. 2011, avec effet au 1er janv. 2012 (RO **2011** 6081).
23 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
24 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
25 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Art. 23[26] Droit d'être renseigné

Le droit d'être renseigné est régi par la LPD.

Art. 24[27] Durée de conservation

[1] Les objets et les documents originaux peuvent être conservés pendant 30 ans au maximum à compter de leur dernier traitement. Est considéré comme traitement toute modification ou tout complément apporté à un bloc de données.

[2] La durée maximale de conservation des données contenues dans ISAS est de 45 ans.

Section 4 Système d'information sécurité intérieure (ISIS)

Art. 25[28] Structure d'ISIS

[1] ISIS comprend:

a. un système de classement pour la saisie et la consultation des données visées à l'art. 26, al. 1;

b. un système d'analyse et de suivi de la situation pour la saisie et pour le traitement et l'analyse des données dans plusieurs systèmes;

c. un index pour déterminer si le SRC traite des données au sens de l'art. 1, let. b, LFRC relatives à une personne ou à une organisation.

[2] Le DDPS fixe les champs de données.

Art. 26[29] Données contenues dans ISIS

[1] ISIS contient des données relatives à des personnes et des événements ainsi que des données documentaires sur la Suisse tirées des activités préventives déployées dans le domaine de la protection de l'Etat et des données provenant de sources d'information accessibles au public au sens de l'art. 9.

[2] Il permet de traiter les données suivantes:

a. données sur l'identité des personnes ou des organisations enregistrées;

b. enregistrements sonores ou visuels;

26 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
27 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
28 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
29 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

c. données alphanumériques relatives à des événements ou à des personnes, telles que l'immatriculation de véhicules, et données concernant des raccordements de télécommunication.

3 Les données sont classées en objet, source documentaire ou document original.

4 Elles peuvent être rattachées à un domaine spécifique et être classées en catégories pour les besoins de la gestion des accès.

Art. 27[30] Contrôle de la qualité

1 Le service d'assurance de la qualité vérifie les données marquées du code «p», en particulier l'indication des sources, l'appréciation de la fiabilité de l'information et la date de la prochaine appréciation globale.

2 Il confirme l'enregistrement définitif des données en les marquant du code «k».

3 Il efface les données devenues inutiles.

Art. 27*a*[31] Droits d'accès

1 Les collaborateurs du SRC ont accès en ligne à ISIS et aux données de l'index.

2 Les autorités suivantes ont accès en ligne à l'index:

a. les organes de sûreté des cantons pour accomplir les tâches que leur assigne la LMSI;

b. fedpol pour accomplir des tâches de police judiciaire et de police de sûreté et pour vérifier des cas de soupçon de blanchiment d'argent ou de financement du terrorisme lors de communications d'instituts financiers suisses (consultation brève);

c. les services fédéraux compétents pour exécuter les contrôles de sécurité relatifs aux personnes (consultation brève).

3 Les organes de sûreté des cantons ont au surplus accès en ligne à l'index pour consulter les sources documentaires saisies sur la base de documents originaux établis par ces organes dans le cadre de l'exécution de la LMSI, pour autant que l'accomplissement des tâches que la LMSI leur assigne le requiert.

Art. 28[32] Exigences techniques pour le raccordement des autorités externes

1 Le DDPS fixe les exigences techniques pour le raccordement des autorités externes.

2 Les autorités externes ne peuvent se raccorder à l'index qu'après avoir satisfait à ces exigences techniques.

30 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
31 Introduit par le ch. I de l'O du 15 juin 2012 (RO **2012** 3773). Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
32 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Art. 29[33] Traitement des données

1 Seules les informations qui répondent aux buts définis à l'art. 3 peuvent être traitées dans ISIS.

2 Les collaborateurs chargés de la saisie des données examinent si une information permet de déduire la pertinence pour la protection de l'Etat de la personne ou de l'organisation à laquelle cette information se rapporte. Dans ce cas, ils saisissent les données dans ISIS.

3 Les données sont saisies provisoirement et marquées du code «p».

4 Les collaborateurs chargés de la saisie des données apprécient la fiabilité des sources documentaires en fonction de la provenance, du mode de transmission, du contenu et des informations disponibles.

5 Ils marquent du code «g» les sources documentaires fiables et du code «u» les communications qui ne le sont pas.

6 Les données concernant des personnes et des organisations figurant dans des documents originaux ne peuvent être utilisées qu'une fois qu'un objet correspondant a été créé.

7 Les sources documentaires marquées du code «u» depuis plus de trois ans après leur saisie ne peuvent être utilisées que si elles sont nécessaires à l'accomplissement des tâches légales et que le directeur du SRC ou son suppléant en a autorisé l'utilisation. Cette autorisation est valable jusqu'à la prochaine appréciation globale.

Art. 30[34] Classement des dossiers

1 Le classement des dossiers vise à garantir la gestion et l'archivage en bonne et due forme des dossiers.

2 Les documents originaux peuvent être saisis au moyen de la technique OCR.

3 Il n'est pas nécessaire de classer les documents originaux sur papier lorsqu'ils ont été saisis sous forme électronique.

Art. 31 Droit d'être renseigné

1 Le droit d'être renseigné est régi par l'art. 18 LMSI.[35]

2 …[36]

33 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
34 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).
35 Nouvelle teneur selon le ch. I de l'O du 9 déc. 2011, en vigueur depuis le 1er janv. 2012 (RO **2011** 6081).
36 Introduit par le ch. I de l'O du 9 déc. 2011 (RO **2011** 6081). Abrogé par le ch. I de l'O du 29 nov. 2013, avec effet au 1er janv. 2014 (RO **2013** 4359).

Art. 32[37] Appréciation globale périodique des données contenues dans ISIS

1 Le service d'assurance de la qualité procède à une appréciation globale de chaque bloc de données au plus tard cinq ans après la saisie de la première source documentaire. Il procède ensuite à une appréciation globale de chaque bloc de données tous les trois ans au minimum.

2 Il vérifie, à la lumière des dangers et des risques existants, si les informations saisies dans un bloc de données sont encore nécessaires pour évaluer les risques relatifs à la sécurité intérieure et pour d'autres tâches de protection de l'Etat. Il efface les données devenues inutiles.

3 Les sources documentaires marquées du code «u» depuis plus de trois ans ne peuvent être utilisées jusqu'à la prochaine appréciation globale que si les conditions suivantes sont réunies:

a. elles sont nécessaires pour l'accomplissement des tâches légales;

b. le directeur du SRC ou son suppléant en a autorisé l'utilisation.

4 Le service d'assurance de la qualité note son appréciation globale sur les blocs de données qui peuvent continuer d'être utilisés.

5 Les objets identifiés depuis plus de trois ans comme des données relatives à des tiers sont effacés lors de l'appréciation globale.

Art. 33[38] Durée de conservation

1 La durée de conservation maximale des données enregistrées dans ISIS est la suivante:

a. pour les données préventives, quinze ans;

b. pour les données relatives à des programmes de recherches préventives en cours, 20 ans;

c. pour les données relatives aux interdictions d'entrée, jusqu'à dix ans après la date de l'expiration de l'interdiction, mais 35 ans au maximum;

d. pour les données relevant du domaine de l'espionnage, 45 ans;

e. pour les données documentaires provenant d'activités préventives déployées dans le domaine de la protection de l'Etat et des données provenant de sources d'information accessibles au public, 45 ans.

2 La durée de conservation maximale des documents originaux est de 45 ans.

37 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

38 Nouvelle teneur selon le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

Art. 34 Données et dossiers des organes cantonaux chargés du maintien de la sécurité intérieure

1 Les organes cantonaux chargés du maintien de la sécurité intérieure peuvent conserver cinq ans au plus les données et les dossiers établis dans le cadre des tâches de protection de l'Etat qu'ils effectuent pour la Confédération.

2 A l'expiration de leur durée de conservation, les données et les dossiers doivent être détruits.

Art. 35 Financement

1 La Confédération finance le transport des données jusqu'aux centraux de raccordement des cantons.

2 Les cantons prennent en charge:

a. les frais d'acquisition et de maintenance de leurs appareils;

b. les frais d'installation et d'exploitation de leur réseau de distribution.

Section 4*a*[39] Présentation électronique de la situation

Art. 35*a* Système et contenu de la PES

1 La Présentation électronique de la situation (PES) est un système d'information en ligne.

2 Il contient des données sur des personnes et des événements en vue de présenter, d'évaluer et d'analyser la situation de la sécurité intérieure et les mesures de politique de sécurité.

3 Il permet de traiter les données suivantes:

a. données décrivant un événement;

b. informations pour la mise en œuvre et l'application de mesures de politique de sécurité et de mesures visant au maintien de la sûreté intérieure et extérieure.

Art. 35*b* Structure de la PES

La PES se compose de registres qui contiennent les données suivantes:

a. «Evénements»: données relatives à des événements traités par des réseaux d'information;

b. «Centre fédéral de situation»: rapports périodiques sur la situation, suivi de la situation et documentation;

39 Introduite par le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

c. «SRC»: données provenant du journal tenu par les services de permanence du SRC.

Art. 35*c* Droits d'accès

[1] Les autorités et offices mentionnés à l'annexe 3 de l'OSRC[40] ont accès à la PES pour autant que les buts fixés dans ladite annexe l'exigent et que les conditions citées soient remplies.

[2] En cas d'événement impliquant un risque accru pour la sécurité, le directeur du SRC peut accorder pour une durée limitée à des services privés et à des autorités de sécurité et de police étrangères un accès à certains contenus de la PES pour autant qu'ils remplissent l'une des conditions suivantes:

a. ils sont directement ou indirectement touchés par l'événement;

b. leurs informations ou leurs connaissances peuvent contribuer à une meilleure présentation et évaluation de la situation;

c. ils participent à la mise en œuvre et à l'application de mesures de politique de sécurité.

[3] Le SRC peut demander aux autorités et offices visés à l'al. 1 qu'ils l'informent de l'utilisation des données.

Art. 35*d* Contrôle de la qualité

Le service d'assurance de la qualité contrôle par sondages la légalité, l'utilité, l'efficacité et l'exactitude des traitements de données dans la PES.

Art. 35*e* Droit d'accès des personnes concernées

Le droit d'accès des personnes concernées est régi par la LPD.

Art. 35*f* Durée de conservation

La durée de conservation maximale des données et des documents originaux qui s'y rapportent est de trois ans.

Section 4*b*[41] Module informatique P4

Art. 35*g* Contenu, but et structure du module P4

[1] Le module informatique P4 (module P4) contient les données suivantes relatives à des personnes et à des événements pour le traitement et l'analyse d'informations sur l'entrée en Suisse de ressortissants étrangers provenant de pays déterminés:

40 RS **121.1**
41 Introduite par le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

a. l'identité des personnes concernées;

b. la photo et d'autres données figurant sur la pièce d'identité;

c. les données provenant des contrôles douaniers.

2 Le module P4 comprend un système de classement pour la saisie et la consultation des données transmises au SRC par les organes de contrôle à la frontière.

Art. 35*h* Droits d'accès

1 Les collaborateurs du SRC chargés du programme de recherche P4, qui vise à traiter et à analyser le franchissement des frontières de ressortissants étrangers de pays déterminés, peuvent accéder en ligne aux données enregistrées dans le module P4 et y saisir, modifier ou effacer des données.

2 Les collaborateurs du SRC peuvent consulter les données enregistrées dans le module P4 pour autant que l'accomplissement de leurs tâches légales le requiert.

Art. 35*i* Contrôle de la qualité

Le service d'assurance de la qualité contrôle par sondages la légalité, l'utilité, l'efficacité et l'exactitude des traitements de données dans le module P4.

Art. 35*j* Droit d'accès des personnes concernées

Le droit d'accès des personnes concernées est régi par la LPD.

Art. 35*k* Durée de conservation

La durée de conservation maximale des données et des documents originaux qui s'y rapportent est de cinq ans.

Section 4*c*[42] Système de gestion électronique des affaires

Art. 35*l* Exploitation et but de GEVER SRC

1 Le SRC exploite dans SiLAN un système de gestion, de traitement et de contrôle des affaires (GEVER SRC).

2 En dérogation à l'art. 12, al. 2, de l'ordonnance GEVER du 30 novembre 2012[43], les données classifiées «CONFIDENTIEL» sont enregistrées dans GEVER SRC sans être chiffrées.

3 En dérogation à l'art. 12, al. 3, de l'ordonnance GEVER, les données classifiées «SECRET» peuvent être enregistrées dans GEVER SRC.

42 Introduite par le ch. I de l'O du 29 nov. 2013, en vigueur depuis le 1er janv. 2014 (RO **2013** 4359).

43 RS **172.010.441**

Art. 35*m* Contenu de GEVER SRC

GEVER SRC contient:

a. des données pour la gestion administrative des affaires;

b. des informations nécessaires pour le contrôle des affaires dans le domaine des contrôles de sécurité relatifs aux personnes;

c. tous les produits du renseignement sortant du SRC;

d. les données utilisées pour établir les contenus visés aux let. a à c pour autant que la protection des sources soit assurée.

Art. 35*n* Droits d'accès

Les collaborateurs du SRC peuvent accéder en ligne aux données enregistrées dans GEVER SRC et y saisir, modifier ou effacer des données pour autant que l'accomplissement de leurs tâches légales le requiert.

Art. 35*o* Contrôle de la qualité

Le service d'assurance de la qualité contrôle par sondages la légalité, l'utilité, l'efficacité et l'exactitude des traitements de données dans GEVER SRC.

Art. 35*p* Droit d'accès des personnes concernées

Le droit d'accès des personnes concernées est régi par la LPD.

Art. 35*q* Durée de conservation

La durée de conservation maximale des données enregistrées est de 45 ans.

Section 5 Dispositions finales

Art. 36 Abrogation du droit en vigueur

L'ordonnance ISIS du 30 novembre 2001[44] est abrogée.

Art. 37 Entrée en vigueur et durée de validité

1 La présente ordonnance entre en vigueur le 1er janvier 2010.

2 La durée de validité des dispositions de la section 3 (art. 17 à 24) est limitée au 31 décembre 2014.

44 [RO **2001** 3173, **2004** 3495 4813 annexe ch. 2, **2006** 921, **2008** 4943 ch. I 2 5525 annexe 4 ch. II 1 6305 annexe ch. 3]