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

du 8 octobre 2014

Le Conseil fédéral suisse,

vu les art. 5, al. 4, et 6*l* 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],

arrête:

Section 1 Objet et définitions

Art. 1 Objet

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

a. système d'information pour la sécurité extérieure (ISAS);
b. système d'information pour la sécurité intérieure (ISIS);
c. système de présentation électronique de la situation (PES);
d. module informatique P4 (module P4);
e. système de gestion des affaires du SRC (GEVER SRC);
f. espace de stockage intermédiaire ROSO.

Art. 2 Définitions

Dans la présente ordonnance, on entend par:

a. *données:* informations enregistrées sous forme écrite, visuelle ou sonore dans les systèmes d'information du SRC;
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 documents originaux dans ISAS ou ISIS;
d. *relation:* lien entre des objets ou entre un objet et une source documentaire;

RS **121.2**
1 RS **121**
2 RS **120**

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

f. *document original*: document disponible sous forme électronique en mode lecture uniquement;

g. *tiers:* personne ou organisation n'ayant une importance pour les tâches que la LMSI confie au SRC que par son lien à un objet et marquée comme telle dans ISIS;

h. *consultation brève:* consultation en ligne limitée d'ISAS ou d'ISIS par les services externes via l'index pour déterminer si une personne ou une organisation figure dans l'un de ces systèmes d'information;

i. *SRCant:* services de renseignement des cantons;

j. *consultation SRCant:* consultation en ligne limitée d'ISAS ou d'ISIS par les SRCant chargés de l'exécution de la LMSI via l'index pour déterminer si une personne ou une organisation figure dans l'un de ces systèmes d'information ou pour lire les données saisies sur la base de documents originaux saisis par les SRCant dans ISAS ou ISIS.

Section 2 Dispositions générales

Art. 3 Droits d'accès

1 L'utilisateur qui a le droit de consulter un système d'information du SRC a uniquement accès aux données dont il a besoin pour accomplir les tâches que la loi lui assigne.

2 Le chef de domaine de direction compétent du SRC ou son suppléant décide des demandes individuelles de droits d'accès.

3 Le SRC répond de l'exécution des droits d'accès.

Art. 4 Accès et analyse sur plusieurs systèmes

1 Les utilisateurs des systèmes d'information du SRC peuvent accéder simultanément à tous les systèmes d'information du SRC dans les limites de leurs droits d'accès. Ils disposent à cet effet d'une fonction de recherche et de distribution adéquate.

2 Les utilisateurs peuvent établir une relation entre les sources documentaires d'ISAS et d'ISIS et un objet individuel pour permettre des analyses sur plusieurs systèmes.

Art. 5 Saisie des données

1 Les documents originaux peuvent être saisis par reconnaissance optique de caractères.

2 Les documents originaux saisis sous forme électronique n'ont pas besoin d'être conservés sur papier.

Art. 6 Transmission de données personnelles

1 Le SRC peut transmettre les données personnelles qui sont traitées dans ses systèmes d'information aux autorités et offices visées à l'annexe 3 de l'ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération (OSRC)[3] pour les buts et aux conditions qui y sont prévus.

2 Les dispositions suivantes régissent la transmission de données personnelles à un service étranger:

a. les art. 6*h* et 6*i* LFRC pour les informations sur l'étranger;

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

3 Il est interdit de transmettre des données lorsque des intérêts publics ou privés prépondérants s'y opposent.

4 Lors de chaque transmission, le SRC informe le destinataire de l'évaluation et de l'actualité des données transmises.

5 Il signale au destinataire:

a. dans quel but il peut utiliser les données et que toute autre utilisation est exclue;

b. qu'il se réserve le droit de lui demander qu'il l'informe de l'utilisation des données.

Art. 7 Effacement des données

1 Les données sont effacées dans un délai de trois mois à compter de l'expiration de leur durée de conservation fixée aux art. 19, 26, 31, 36, 40 et 44.

2 Dans ISAS et ISIS, l'effacement de la dernière source documentaire référencée entraîne l'effacement de l'objet concerné.

3 Dans ISAS, le document original est effacé au plus tard à l'expiration de la durée de conservation.

4 Dans ISIS, l'effacement de la dernière source documentaire entraîne l'effacement du document original référencé.

5 Les données effacées sont transférées dans un module d'archivage.

Art. 8 Sécurité des données

1 Les dispositions suivantes régissent la sécurité des données:

a. l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[4];

b. l'ordonnance du 9 décembre 2011 sur l'informatique dans l'administration fédérale[5];

3 RS **121.1**
4 RS **235.11**
5 RS **172.010.58**

c. l'ordonnance du 4 juillet 2007 concernant la protection des informations[6];

d. les directives du Conseil fédéral du 14 août 2013 concernant la sécurité des TIC dans l'administration fédérale[7].

2 Le SRC précise dans des règlements de traitement:

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

b. les modalités de la journalisation automatique du traitement des données.

Art. 9 Portail ROSO

Le SRC exploite un portail qui compile les données provenant de sources d'informations accessibles au public (portail d'accès aux renseignements de source ouverte, portail ROSO).

Art. 10 Réseau SiLAN

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

2 Il exploite ses systèmes d'information, gère le classement des dossiers et exploite le système intranet du SRC dans le réseau SiLAN; l'index d'ISAS et l'index d'ISIS, de même que le PES, ne sont pas exploités dans le réseau SiLAN pour garantir l'accès des autorités externes.

3 Toutes les données classifiées peuvent être traitées dans le réseau SiLAN, quel que soit leur échelon de classification.

4 Seuls les collaborateurs du SRC, de la Surveillance des services de renseignement du Département fédéral de la défense, de la protection de la population et des sports (DDPS), du Service de renseignement de l'armée et du prestataire de services d'information et de communication (prestataire TIC) du SRC qui se sont vu attribuer les droits nécessaires ont accès au réseau SiLAN. Les mandataires auxquels les services susmentionnés ont donné un droit d'accès sont soumis par analogie aux mêmes conditions d'utilisation.

Art. 11 Transmission de données hors du réseau SiLAN

1 La transmission de données hors du réseau SiLAN est régie par l'ordonnance du 4 juillet 2007 concernant la protection des informations[8].

2 La Confédération finance la transmission des données jusqu'à un point de raccordement central pour les cantons.

6 RS **510.411**

7 Les directives peuvent être consultées sur le site de l'Unité de pilotage informatique de la Confédération à l'adresse suivante: www.upic.admin.ch > Thèmes > Sécurité > Bases de sécurité > Directives de la sécurité informatique.

8 RS **510.411**

3 Les cantons prennent à leur charge:

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

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

Art. 12 Exigences techniques

1 Le DDPS détermine les exigences techniques auxquelles les terminaux des utilisateurs doivent satisfaire. Les autorités externes ne sont raccordées au réseau que lorsque leurs terminaux satisfont à ces exigences.

2 Le SRC fixe les modalités pour chaque système d'information dans des règlements de traitement.

Art. 13 Responsabilités et compétences

1 Le SRC répond de ses systèmes d'information.

2 Les services du SRC chargés de la gestion des applications et de l'assurance qualité répondent de la formation et du soutien technique des utilisateurs des systèmes d'information du SRC. Ces services veillent à la mise en œuvre des règlements de traitement.

3 Le prestataire TIC du SRC répond de l'exploitation technique, de la maintenance et de la sécurité des systèmes d'information visés à l'art. 1, let. a, b et d à f. Le prestataire TIC de la Centrale nationale d'alarme répond de l'exploitation technique, de la maintenance et de la sécurité du PES.

4 Le service chargé d'assurer la qualité contrôle par sondage la légalité du traitement des données saisies dans les systèmes d'information visés à l'art. 1, let. c à f, son adéquation, son efficacité et son exactitude. Il effectue ce contrôle au moins une fois par an pour chaque système d'information selon un plan de contrôle.

Art. 14 Droit d'accéder aux données qui concernent sa propre personne

Les dispositions suivantes régissent le droit des personnes d'accéder aux données qui les concernent:

a. pour les données enregistrées dans ISAS, dans le PES, dans le module P4, dans GEVER SRC ou dans l'espace de stockage intermédiaire ROSO, les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données[9];

b. pour les données enregistrées dans ISIS, l'art. 18 LMSI.

9 RS **235.1**

Section 3 Dispositions particulières applicables à ISAS

Art. 15 Structure

La structure d'ISAS se fonde sur l'art. 6*e* LFRC.

Art. 16 Données

1 Le contenu d'ISAS se fonde sur l'art. 6*c* LFRC.

2 Les objets et les sources documentaires peuvent être présentés visuellement et cette présentation visuelle peut être enregistrée.

3 L'annexe 1 énumère le catalogue des données personnelles.

4 Le DDPS définit les champs de données.

5 L'index contient les données relatives à toutes les personnes et organisations pertinentes pour les tâches que doivent accomplir les utilisateurs externes d'ISAS, sous réserve des données qui ne peuvent être enregistrées pour des raisons de protection des sources.

6 L'index contient des données classifiées allant jusqu'à l'échelon CONFIDENTIEL.

Art. 17 Saisie des données

Les collaborateurs du SRC chargés de saisir les données apprécient la pertinence et l'exactitude des données personnelles à saisir.

Art. 18 Contrôle périodique des données personnelles

1 Les collaborateurs du SRC chargés de saisir les données contrôlent périodiquement les blocs de données contenues dans ISAS qui comportent des objets relatifs à des personnes ou à des organisations.

2 A cet effet, ils assument les tâches suivantes:

a. ils apprécient au vu de la situation actuelle si les blocs de données sont encore utiles à l'accomplissement des tâches que l'art. 1, let. a, LFRC assigne au SRC;

b. ils effacent les données dont le SRC n'a plus besoin;

c. ils rectifient, marquent ou effacent les données qui s'avèrent inexactes;

d. ils consignent l'exécution et le résultat du contrôle.

3 Le contrôle périodique a lieu chaque fois qu'un bloc de données est complété. Les délais maximaux ci-après s'appliquent aux données provenant des domaines suivants:

a. terrorisme international: 10 ans au plus après la saisie de l'objet ou le dernier contrôle périodique;

b. activités d'espionnage ou de dissémination d'armes de destruction massive: 15 ans au plus après la saisie de l'objet ou du dernier contrôle périodique;

c. autres informations importantes en matière de politique de sécurité: 20 ans au plus après la saisie de l'objet ou du dernier contrôle périodique.

4 Le service chargé d'assurer la qualité veille au respect des al. 2 et 3 en donnant des formations internes et en procédant à des contrôles réguliers. Il effectue ces contrôles au moins une fois par an selon un plan de contrôle.

Art. 19 Durée de conservation

1 Les durées de conservation suivantes sont applicables aux sources documentaires enregistrées dans ISAS:

a. pour les données provenant du domaine du terrorisme international: 30 ans au plus;

b. pour les données provenant des activités d'espionnage et de dissémination d'armes de destruction massive: 45 ans au plus;

c. pour les autres informations importantes en matière de politique de sécurité: 45 ans au plus.

2 La durée de conservation de documents originaux est de 45 ans au plus.

Art. 20 Droits d'accès

1 Les droits d'accès sont régis par l'art. 6*f* LFRC.

2 Les organes de sûreté des cantons ont accès en ligne à l'index au moyen de la consultation SRCant pour accomplir les tâches que la LMSI leur assigne.

3 L'annexe 2 règle les droits d'accès individuels.

Section 4 Dispositions particulières applicables à ISIS

Art. 21 Structure

1 ISIS comprend:

a. un système de classement pour la saisie et la consultation des données visées à l'art. 22, 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 relatives à une personne ou à une organisation dans ce système d'information.

2 Le DDPS définit les champs de données.

Art. 22 Données

1 ISIS contient des données nécessaires pour assurer les tâches de renseignement dans le domaine de la sûreté intérieure en vertu de la LMSI.

2 Il contient des données concernant des personnes physiques et morales, des organisations, des objets et des événements.

3 Il peut également contenir des données sensibles et des profils de la personnalité.

4 L'annexe 1 énumère le catalogue des données personnelles.

5 L'index contient les données relatives à toutes les personnes et organisations pertinentes pour les tâches que les utilisateurs externes d'ISIS doivent accomplir , sous réserve des données qui ne peuvent être enregistrées dans l'index pour des raisons de protection des sources.

6 L'index contient des données classifiées allant jusqu'à l'échelon CONFIDENTIEL.

Art. 23 Saisie des données

1 Les collaborateurs du SRC chargés de saisir les données introduisent les informations dans ISIS. Avant la saisie d'une nouvelle information, ils sont tenus d'apprécier si cette information confirme ou infirme la pertinence de la personne ou de l'organisation concernée pour l'accomplissement des tâches de renseignement que la LMSI assigne au SRC.

2 Les collaborateurs évaluent sur la base de la provenance, du genre de transmission, du contenu et des renseignements disponibles si les données sont sûres ou incertaines et ils les marquent en conséquence.

3 Les données sont saisies provisoirement et sont marquées en conséquence.

4 Les objets et les sources documentaires peuvent être présentés visuellement et cette présentation visuelle peut être enregistrée.

5 Les données relatives à des personnes ou à des organisations contenues dans les documents originaux ne peuvent être réutilisées que lorsqu'un objet concernant la personne ou l'organisation en question a été établi.

Art. 24 Contrôle de la saisie

1 Le service chargé d'assurer la qualité vérifie que les données ont été saisies légalement. A cet effet, il apprécie en particulier si leur pertinence est suffisante, si les restrictions de traitement visées à l'art. 3 LMSI ont été respectées et si l'évaluation des données est exacte.

2 Il confirme la saisie définitive de ces données en les marquant en conséquence.

3 Il efface les données qu'il n'a pas confirmées.

Art. 25 Appréciation globale périodique des données

1 Le service chargé d'assurer la qualité procède à une appréciation globale du bloc de données cinq ans au plus après la saisie de l'objet qui s'y rapporte. Il procède ensuite à une appréciation globale du bloc de données tous les trois ans au moins.

2 Il vérifie, au vu des dangers et des risques existants, si le bloc de données est encore nécessaire pour maintenir la sûreté intérieure et pour accomplir d'autres tâches de renseignement que la LMSI assigne au SRC. Il efface les données dont le SRC n'a plus besoin.

3 Les données marquées comme incertaines depuis plus de trois ans ne peuvent continuer à être utilisées jusqu'à la prochaine appréciation globale que si les conditions suivantes sont réunies:

a. elles sont nécessaires pour l'accomplissement des tâches que la loi assigne au SRC;

b. le directeur du SRC ou son suppléant en donne l'autorisation.

4 Le service chargé d'assurer la qualité note sur les blocs de données qui peuvent continuer d'être utilisés qu'il a procédé à leur appréciation globale.

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

Art. 26 Durée de conservation

1 Les sources documentaires enregistrées dans ISIS peuvent être conservée pendant 15 ans au plus, sous réserve de l'al. 2.

2 Les durées de conservation ci-après s'appliquent aux sources documentaires suivantes enregistrées dans ISIS:

a. pour les sources documentaires comportant des données relatives à des programmes de recherches préventives en cours: 20 ans au plus;

b. pour les sources documentaires comportant des données relatives aux interdictions d'entrée: 10 ans au plus après l'expiration de l'interdiction, mais 35 ans au plus;

c. pour les sources documentaires comportant des données relevant du domaine de l'espionnage: 45 ans au plus;

d. pour les sources documentaires comportant des données provenant de sources accessibles au public: 45 ans au plus.

Art. 27 Durée de conservation des données provenant des SRCant

1 Les SRCant peuvent conserver pendant cinq ans au plus les données qu'ils ont saisies en vertu de la LMSI dans l'exercice de leurs tâches de renseignement pour la Confédération.

2 A l'expiration de ce délai, ils sont tenus de détruire ces données.

Art. 28 Droits d'accès

1 Les collaborateurs du SRC ont accès en ligne aux données contenues dans ISIS.

2 Les autorités suivantes ont accès en ligne à l'index selon les modalités ci-après:

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

b. l'Office fédéral de la police pour accomplir des tâches de sécurité, de police judiciaire et administrative et pour vérifier des soupçons 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 succincte.

3 L'annexe 2 règle les droits d'accès individuels.

Section 5 Dispositions particulières applicables au PES

Art. 29 But et structure

1 Le PES est un système d'information en ligne qui permet de présenter, d'évaluer et d'analyser la situation en matière de sûreté intérieure ou extérieure et les mesures de politique de sécurité.

2 Il se compose des registres suivants, qui contiennent les données ci-après:

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

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

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

Art. 30 Données

1 Le PES contient:

a. les données décrivant un événement;

b. les informations concernant le pilotage et la mise en œuvre de mesures de politique de sécurité et concernant les mesures prises en vue de maintenir la sécurité intérieure ou extérieure.

2 L'annexe 3 énumère le catalogue des données personnelles.

Art. 31 Durée de conservation

La durée de conservation des données contenues dans le PES et des documents originaux qui s'y rapportent est de trois ans au plus.

Art. 32 Droits d'accès

1 Les autorités et offices visés à l'annexe 3 OSRC[10] ont accès au PES pour les buts et aux conditions qui y sont prévus.

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 du PES si l'une des conditions suivantes est remplie:

a. ces autorités ou services sont touchés directement ou indirectement par l'événement;

b. les informations ou les connaissances de ces autorités ou services peuvent contribuer à une meilleure présentation et évaluation de la situation;

c. ces autorités ou services participent au pilotage ou à la mise en œuvre de mesures de politique de sécurité.

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

4 L'annexe 4 règle les droits d'accès individuels.

Section 6 Dispositions particulières applicables au module P4

Art. 33 But et structure

1 Le module P4 est un système d'information qui permet de traiter et d'analyser des informations sur l'entrée en Suisse ou la sortie du territoire suisse de ressortissants de certains pays étrangers.

2 Il consiste en un système de classement pour la saisie et la consultation des données transmises au SRC par les organes de contrôle douaniers.

Art. 34 Données

1 Le module P4 contient les données suivantes:

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 L'annexe 5 énumère le catalogue des données personnelles.

Art. 35 Droits d'accès

1 Les collaborateurs du SRC ont accès en ligne aux données contenues dans le module P4.

10 RS **121.1**

2 Les collaborateurs du SRC chargés du programme de recherche visant à traiter et à analyser l'entrée en Suisse et la sortie du territoire suisse de ressortissants de certains pays étrangers peuvent au surplus saisir, modifier ou effacer des données dans le module P4, pour autant que l'accomplissement des tâches que la loi leur assigne le requiert.

3 Les collaborateurs de la surveillance du service de renseignement du DDPS ont accès en ligne aux données contenues dans le module P4 pour la durée de leurs inspections.

4 L'annexe 6 règle les droits d'accès individuels.

Art. 36 Durée de conservation

La durée de conservation des données contenues dans le module P4 et des documents originaux qui s'y rapportent est de cinq ans au plus.

Section 7 Dispositions particulières applicables à GEVER SRC

Art. 37 Exploitation et but

1 Le SRC exploite dans le réseau SiLAN le système d'information GEVER SRC, qui permet de gérer, de traiter et de contrôler les mandats et les affaires.

2 En dérogation à l'art. 12, al. 2 et 3, de l'ordonnance GEVER du 30 novembre 2012[11], les données classifiées CONFIDENTIEL et SECRET peuvent être enregistrées dans GEVER SRC sans être chiffrées.

Art. 38 Données

1 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 transmis à l'extérieur par le SRC en matière de renseignement;

d. des données au sujet du matériel qui prône le racisme ou la violence, pour le contrôle des affaires par le service de documentation;

e. des données pour le contrôle des affaires en matière d'exploration radio.

2 Dans la mesure où la protection des sources est garantie, les données utilisées pour établir les contenus visés à l'al. 1, let. a à c, peuvent également être traitées pendant cinq ans dans GEVER SRC.

11 RS **172.010.441**

Art. 39 Droits d'accès

1 Les collaborateurs du SRC peuvent consulter, saisir, modifier et effacer des données dans GEVER SRC, pour autant que l'accomplissement des tâches que la loi leur assigne le requiert.

2 L'annexe 7 règle les droits d'accès individuels.

Art. 40 Durée de conservation

Les durées de conservation ci-après s'appliquent aux données contenues dans GEVER SRC:

a. 15 ans au plus pour les données destinées au contrôle des affaires en matière d'exploration radio;

b. 45 ans au plus pour les autres données.

Section 8
Dispositions particulières applicables à l'espace de stockage intermédiaire ROSO

Art. 41 But

L'espace de stockage intermédiaire ROSO est un système d'information qui permet d'évaluer de grandes quantités de données.

Art. 42 Données

1 L'espace de stockage intermédiaire ROSO contient des données provenant de sources d'informations accessibles au public.

2 L'annexe 8 énumère le catalogue des données personnelles.

Art. 43 Droits d'accès

1 Les collaborateurs du SRC peuvent accéder en ligne aux données enregistrées dans l'espace de stockage intermédiaire ROSO et y consulter, saisir, modifier ou effacer des données, pour autant que l'accomplissement des tâches que la loi leur assigne le requiert.

2 Les collaborateurs de la surveillance du service de renseignement du DDPS ont accès en ligne aux données contenues dans l'espace de stockage intermédiaire ROSO pour la durée de leurs inspections.

3 L'annexe 9 règle les droits d'accès individuels.

Art. 44 Durée de conservation

Les données contenues dans l'espace de stockage intermédiaire ROSO peuvent être conservées aussi longtemps que leur évaluation le requiert, mais pendant six mois au plus.

Section 9 Dispositions finales

Art. 45 Abrogation d'un autre acte

L'ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération[12] est abrogée.

Art. 46 Modification d'un autre acte

L'OSRC[13] est modifiée comme suit:

Art. 13, al. 1

1 Le SRC peut transmettre des informations à des services étrangers aux conditions prévues aux art. 6*h* et 6*i* LFRC et 17, al. 3 à 5, LMSI.

Art. 19, al. 3

3 Les documents originaux du système d'information pour la sécurité extérieure (ISAS) et ceux du système d'information pour la sécurité intérieure (ISIS) doivent être enregistrés séparément sur le plan logique en fonction de leur lien matériel avec la Suisse.

Art. 28 Archivage

Le SRC propose les données dont il n'a plus besoin ou qui sont destinées à être détruites aux Archives fédérales en vue de leur archivage (art. 7*a* LFRC).

Art. 47 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er novembre 2014.

8 octobre 2014 Au nom du Conseil fédéral suisse:

Le président de la Confédération, Didier Burkhalter
La chancelière de la Confédération, Corina Casanova

12 RO **2009** 7041**, 2011** 6081**, 2013** 4359
13 RS **121.1**

Annexe 1
(art. 16, al. 3, et 22, al. 4)

Catalogue des données personnelles contenues dans ISAS et ISIS

1. Nom
2. Prénom
3. Date de naissance
4. Nationalité
5. Sexe
6. Etat civil
7. Lieu d'origine
8. Signalement (signes particuliers, taille, couleur des yeux, de la peau et des cheveux)
9. Photographie
10. Appartenance ethnique
11. Religion
12. Orientation politique/idéologique
13. Profession/formation/activités
14. Adresse
15. Pièces d'identité et numéros des pièces d'identité
16. Identité de personnes de référence/membres de la famille
17. Moyens de locomotion et numéros des plaques minéralogiques
18. Moyens de communication et données sur les raccordements de télécommunication
19. Informations géographiques (GIS, coordonnées géographiques)
20. Evénement (description)
21. Objet (description, numéros)
22. Données multimédia (enregistrements visuels et sonores)
23. Données médicales

Annexe 2
(art. 20, al. 3, et 28, al. 3)

Droits d'accès à ISAS et à ISIS

Fonction	ISIS/ISAS	ISIS-/ISAS-Index
Responsable d'application SRC (sur le plan technique)	A	A
Administrateur (technique) SRC	A	A
Archiviste SRC	E	L
Responsable de domaine SRC	X	L
Responsable des données SRC	S	L
Personne saisissant des données/ triage et ComCenter SRC	X	L
Personnes saisissant des données à l'évaluation SRC	X	L
Personnes saisissant des données cyber/collaborateurs pour le contrôle DJIMON SRC	X	L
Personnes saisissant des données relatives à la recherche d'informations	X	L
Personne saisissant des données au Centre fédéral de situation	X	L
Collaborateur au service chargé de la qualité du SRC	Z	L
Autres collaborateurs du SRC ayant besoin de ces données pour accomplir les tâches que la loi leur assigne	L	L
Collaborateur au service de la sécurité du SRC	S	L
SRCant	–	L
Sécurité de l'information et des objets, Chancellerie fédérale, Office fédéral de la police	–	L

Légendes

A = droits d'administrateur

E = lire, muter, saisir

L = lire

S = lire, statistique, audit

X = lire, muter, saisir, effacer

Z = lire, muter, saisir, effacer, statistique, audit

Annexe 3
(art. 30, al. 2)

Catalogue des données personnelles du PES

1. Description de l'événement (qui, quoi, quand et où).
2. Identité (nom, prénom, date de naissance, nationalité) des personnes ayant participé à l'événement.
3. Description (qui, quoi, quand et où) des mesures prévues et des mesures mises en œuvre pour maîtriser l'événement.
4. Identité (nom, prénom, date de naissance, nationalité) des personnes ayant participé à la mesure.

Annexe 4
(art. 32, al. 4)

Droits d'accès au PES

	Evénements	Rapports sur la situation	PES SRC
Personne saisissant des données au Centre fédéral de situation	X	X	X
Autres collaborateurs du SRC	E	E	E
Autorités selon l'annexe 3 OSRC[14]	E	E	–
Administrateur SRC	A	A	A
Collaborateur au service chargé de la qualité du SRC	Z	Z	Z
Collaborateur au service de la sécurité du SRC	S	S	S
Archiviste SRC	X	X	X

Légendes

A = droits d'administrateur
E = lire, muter, saisir
L = lire
S = lire, statistique, audit
X = lire, muter, saisir, effacer
Z = lire, muter, saisir, effacer, statistique, audit

14 RS **121.1**

Annexe 5
(art. 34, al. 2)

Catalogue des données personnelles contenues dans le module P4

1. Nom, prénom, date de naissance, nationalité
2. Numéro de la pièce d'identité, numéro de visa, date de validité
3. Photographie figurant sur la pièce d'identité
4. Lieu, date et description du contrôle douanier

Annexe 6
(art. 35, al. 4)

Droits d'accès au module P4

Administrateur SRC	A
Collaborateur du service spécialisé du module P4 SRC	X
Collaborateur du service des étrangers SRC	L
Collaborateur recherches sécurité intérieure et extérieure SRC	L
Analyste SRC	L
Collaborateur du Centre fédéral de situation	L
Collaborateur au service de la sécurité du SRC	S
Collaborateur au service de la surveillance du DDPS	L*
Archiviste SRC	X

Légendes

A = droits d'administrateur

X = lire, muter, saisir, effacer

L = lire

S = lire, statistique, audit

* seulement pour la durée de l'inspection

Annexe 7
(art. 39, al. 2)

Droits d'accès à GEVER SRC

Administrateur SRC	A
Personnel du SRC	X
Collaborateur au service de la sécurité du SRC	S
Archiviste SRC	X

Légendes
A = droits d'administrateur
X = lire, muter, saisir, effacer
S = lire, statistique, audit

Annexe 8
(art. 42, al. 2)

Catalogue des données personnelles contenues dans l'espace de stockage intermédiaire ROSO

1. Données d'identité (nom, prénom, date de naissance, nationalité, sexe, profession)
2. Données personnelles de tout type publiées sur Internet

Annexe 9
(art. 43, al. 3)

Droit d'accès à l'espace de stockage intermédiaire ROSO

Administrateur SRC	A
Archiviste SRC	X
Collaborateur SRC	X
Collaborateur au service de la sécurité du SRC	S
Collaborateur au service de la surveillance du DDPS	S*

Légendes

A = droits d'administrateur

X = lire, muter, saisir, effacer

S = lire, statistique, audit

* seulement pour la durée de l'inspection