

Ordonnance sur le système de traitement des données relatives à la protection de l'Etat (Ordonnance ISIS)

du 30 novembre 2001 (Etat le 28 mars 2006)

Le Conseil fédéral suisse,

vu les art. 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 (LM SI)¹,
vu l'art. 39, al. 3, de la loi fédérale du 20 juin 1997 sur les armes, les accessoires d'armes et les munitions (LArm)²,

arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance règle l'exploitation, le contenu des données et l'utilisation du système de traitement des données relatives à la protection de l'Etat (ISIS).

Art. 2 Buts

¹ ISIS a pour but de faciliter:

- a. la mise en œuvre de mesures préventives dans le domaine de la protection fédérale de l'Etat;
- b. les tâches de police de sécurité et de police administrative;
- c. l'exécution de la législation sur les armes;

² ISIS est utilisé pour:

- a.³ 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;

RO 2001 3173

¹ RS 120

² RS 514.54

³ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

- d. le classement et la gestion de dossiers;
- e.⁴ l'exécution de travaux de documentation;
- f.⁵ la gestion des affaires.

Art. 3⁶ Définitions

Dans la présente ordonnance, on entend par:

- a. données: informations mémorisées dans ISIS;
- b. objets: regroupements de données se rapportant à une ou plusieurs personnes, faits ou événements;
- c. communications: nouvelles informations relatives à un ou plusieurs objets;
- d. relations: liens entre des objets et des communications spécifiques;
- e. blocs de données: communications et relations relatives à un objet;
- f. données OCR: données de dossiers saisies de telle manière qu'une recherche dans l'ensemble du texte est possible;
- g. données d'image: documents consultés sous forme d'image;
- h. consultations ponctuelles: consultations en ligne pour déterminer si une personne figure dans ISIS;
- i. tiers: personnes ou organisations revêtant une importance du point de vue de la protection de l'Etat uniquement de par leur lien avec un objet;
- j. factsheets: appréciations périodiques standardisées de l'analyse stratégique relative à un objet spécifique.

Art. 4⁷ Systèmes et banques de données

¹ ISIS se compose des systèmes et banques de données suivants:

- a. «ISIS00 Général» avec classement des dossiers, gestion des mandats, analyse des risques, statistique et module d'archivage;
- b. «ISIS01 Protection de l'Etat» avec les banques de données «Protection de l'Etat», «Police administrative», «Documentation» et «Système numérique»;
- c. «ISIS02 Administration» avec la banque de données «Administration»;
- d. «ISIS03 Armes» avec les banques de données «Acquisition d'armes par des étrangers» et «Révocation d'autorisations et mise sous séquestre d'armes»;

⁴ Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁵ Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁶ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁷ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

- e. «ISIS04 Explosifs» avec la banque de données «BARBARA»;
 - f. «ISIS05 News» avec les banques de données «NEWS», «Portail interactif pour Open Sources», «ELIS», «IPIS», «Infopress» et «ISIS-Info»;
 - g. «ISIS06 Contrôles de sécurité relatifs aux personnes» avec la banque de données «Contrôles de sécurité relatifs aux personnes».
- ² Les banques de données contiennent les informations suivantes:
- a. «Protection de l'Etat» (ST): informations relatives aux personnes et aux événements, tirées des activités préventives déployées dans le domaine de la protection de l'Etat;
 - b. «Police administrative» (VP): informations relatives aux personnes et aux événements relevant du domaine des offices centraux de police administrative du Service d'analyse et de prévention (SAP);
 - c. «Documentation» (DO): informations documentaires relevant de l'ensemble du domaine d'activité du SAP, conformément à l'art. 11 de l'ordonnance du 27 juin 2001 sur les mesures visant au maintien de la sûreté intérieure (OMSI)⁸;
 - d. «Système numérique» (NU): informations relatives aux événements, tirées de programmes déterminés de recherches;
 - e. «Administration» (VE): informations nécessaires au contrôle des affaires;
 - f. «Acquisition d'armes par des étrangers» (DEWA): informations personnelles concernant l'acquisition d'armes par des ressortissants étrangers non titulaires d'un permis d'établissement en Suisse;
 - g. «Révocation d'autorisations et mise sous séquestre d'armes» (DEBBWA): informations personnelles concernant la révocation d'autorisations et la mise sous séquestre d'armes en Suisse;
 - h. «BARBARA»: informations relatives aux événements, tirées du domaine d'activité de l'Office central pour les explosifs et la pyrotechnie;
 - i. «NEWS»: communiqués de presse relevant de la protection de l'Etat, tirés d'Internet;
 - j. «Portail interactif pour Open Sources» (IPOS): portail personnalisé permettant d'utiliser des sources d'information accessibles au public;
 - k. «ELIS»: représentation électronique de la situation en matière de sécurité intérieure;
 - l. «IPIS»: communiqués des agences de presse relevant de la protection de l'Etat;
 - m. «Infopress»: revue de presse quotidienne établie par le SAP;
 - n. «ISIS-Info»: plate-forme d'information destinée aux utilisateurs d'ISIS;

⁸ RS 120.2

- o. «Contrôles de sécurité relatifs aux personnes» (PSP): informations nécessaires au contrôle des affaires dans le domaine des contrôles de sécurité relatifs aux personnes.

Art. 5⁹ Données traitées

¹ Les données enregistrées dans les banques de données d'ISIS sont classées en catégories en fonction des domaines spécialisés, dans la mesure où cette classification est judicieuse pour la gestion des accès.

² Les banques de données d'ISIS sont structurées selon les critères ci-après: communications, objets et relations. Les différents champs de données sont réglés par le Département fédéral de justice et police (département).

Art. 6 Intranet

¹ L'«Intranet ISIS» est un système de communication codé au sein d'ISIS.¹⁰

² Le SAP ne met ce système qu'à la disposition des utilisateurs d'ISIS.

Section 2 Utilisateurs, raccordement et accès aux données

Art. 7¹¹ Utilisateurs

¹ Les utilisateurs d'ISIS sont les suivants:

- a. les agents du SAP et ceux des organes cantonaux chargés du maintien de la sûreté intérieure; ils sont raccordés au système par une procédure d'appel;
- b. les collaborateurs du Service fédéral de sécurité (SFS), de la Police judiciaire fédérale (PJF) et du Service fédéral chargé des contrôles de sécurité relatifs aux personnes (intégré à la Division de la protection des informations et des objets); ils peuvent effectuer des consultations ponctuelles par une procédure d'appel.

² Les utilisateurs d'ISIS ont accès aux données nécessaires à l'accomplissement de leurs tâches légales.

³ Les organes cantonaux chargés du maintien de la sûreté intérieure ne peuvent pas consulter les données classifiées issues des contacts directs avec les autorités de sécurité étrangères.

⁴ Les droits d'accès sont réglés par le département. Le chef du SAP, ou l'un de ses suppléants, statue sur les demandes individuelles.

⁹ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹⁰ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹¹ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁵ La Section Assurance qualité du SAP est responsable de l'application des droits d'accès.

Art. 8¹² Raccordement des cantons

Le département fixe les conditions du raccordement des organes cantonaux chargés du maintien de la sûreté intérieure, lesquels ne sont raccordés à ISIS qu'une fois ces conditions remplies.

Art. 9¹³

Section 3 Traitement des données

Art. 10 Saisie des données et contrôle de qualité

¹ Seules peuvent être traitées dans ISIS des informations qui répondent aux buts définis à l'art. 2.

² La Section Analyse préliminaire du SAP introduit les données dans ISIS et détermine la catégorie de communications.¹⁴

^{2bis} Les personnes suivantes peuvent également introduire des données et déterminer les catégories de communications:

- a. les collaborateurs de la Section Service des étrangers du SAP: données issues du contrôle des photos d'identité;
- b. les collaborateurs de l'Office central des armes du SAP: données issues des banques de données DEWA et DEBBWA;
- c. les collaborateurs de l'Office central pour les explosifs et la pyrotechnie du SAP: données issues des banques de données BARBARA et VP;
- d. les collaborateurs de la Division Analyse du SAP: factsheets;
- e. les collaborateurs du Domaine Contrôles de sécurité relatifs aux personnes: données issues de la banque de données PSP;
- f. les collaborateurs des organes cantonaux chargés du maintien de la sécurité intérieure: données issues de la banque de données NU.¹⁵

³ Les données destinées aux banques ST et VP sont, dans un premier temps, saisies provisoirement (code «p»). Leur fiabilité est appréciée en fonction de la provenance,

¹² Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹³ Abrogé par le ch. I de l'O du 30 juin 2004, avec effet au 1^{er} sept. 2004 (RO 2004 3495).

¹⁴ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹⁵ Introduit par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

du mode de transmission, du contenu et des informations déjà disponibles (code «g» pour les communications fiables et code «u» pour celles qui ne le sont pas).¹⁶

⁴ La Section Assurance qualité du SAP vérifie les saisies provisoires, notamment l'indication des sources, l'appréciation de la fiabilité et la date de la prochaine appréciation globale; enfin, elle confirme l'enregistrement définitif des données (code «k»).¹⁷

⁵ Le chef du SAP ou l'un de ses remplaçants peuvent charger l'Assurance qualité d'apprécier le contenu des autres banques de données.

Art. 11¹⁸ Classement des dossiers

¹ Le classement des dossiers doit garantir leur gestion et leur archivage conformément aux instructions.

² Les informations à l'origine des objets et des communications peuvent être saisies comme données OCR, sauf dans les banques de données ST, BARBARA et PSP, où elles sont saisies uniquement comme données d'image.

³ Il est possible de renoncer au classement-papier des dossiers dans la mesure où les informations à l'origine des objets et des communications sont saisies comme données d'image.

Art. 12 Consultation des banques de données

¹ Les données peuvent être consultées suivant les critères ci-après: objets, relations, communications, mandats et recherche dans l'ensemble du texte. Les données d'image ne peuvent pas être consultées séparément.¹⁹

² La consultation des communications n'est possible que dans un seul système à la fois.²⁰

³ Les agents du SAP spécialement formés peuvent procéder à des appréciations dans le cadre de leur domaine d'activité.

⁴ Les objets et leurs relations peuvent être représentés et enregistrés visuellement.²¹

¹⁶ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹⁷ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹⁸ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

¹⁹ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

²⁰ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

²¹ Introduit par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

Art. 13 Communication de données

¹ Dans des cas déterminés, le SAP peut communiquer des données personnelles traitées dans ISIS, à l'exception des données contenues dans les banques DEWA et DEBBWA et des données prélevées dans le cadre de contrôles de sécurité relatifs aux personnes:

- a. aux autorités pénales cantonales, aux fins de prévenir et de poursuivre les actes punissables;
- b. au Département fédéral des affaires étrangères (DFAE), pour l'appréciation des demandes d'accréditation et du droit de séjourner en Suisse de ressortissants d'Etats étrangers ou de membres d'organisations internationales, en vue du respect des engagements de protection découlant du droit international public ainsi que dans le cadre du droit de coopérer du DFAE dans le domaine de la législation régissant les échanges extérieurs;
- c.²² aux autres unités administratives de l'Office fédéral de la police (fedpol):
 1. pour soutenir les enquêtes de police judiciaire, ainsi que dans le cadre de recherches préliminaires utiles à l'établissement de faits dans le domaine de la lutte contre le crime organisé et le trafic illicite des stupéfiants;
 2. dans le cadre de l'entraide administrative internationale liée à des affaires pénales (INTERPOL);
 3. pour saisir des informations dans le système de recherches informatisées de police RIPOL;
 4. pour apprécier les risques sur le plan sécuritaire lors de la mise en œuvre de mesures de protection en faveur de personnes ou de bâtiments;
- d. à l'Office fédéral de la justice, pour compléter ou exécuter une requête d'entraide judiciaire en matière pénale;
- e.²³ à l'Office fédéral des migrations pour l'application de mesures contre des étrangers, notamment en vue de leur éloignement, ainsi que pour traiter des demandes de naturalisation et pour apprécier des demandes d'asile;
- f. ...²⁴
- g. au Département fédéral de la défense, de la protection de la population et des sports, pour l'exercice de son droit de coopérer dans le domaine de la législation régissant les échanges extérieurs;
- h. au Service de sécurité militaire pour:
 1. apprécier la situation militaire en matière de sécurité,
 2. protéger des informations et des ouvrages militaires,

²² Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

²³ Nouvelle teneur selon le ch. 2 de l'annexe à l'O du 3 nov. 2004, en vigueur depuis le 1^{er} janv. 2005 (RO 2004 4813).

²⁴ Abrogée par le ch. 2 de l'annexe à l'O du 3 nov. 2004, avec effet au 1^{er} janv. 2005 (RO 2004 4813).

3. exécuter, dans le domaine de l'armée, des tâches en matière de police criminelle et de police de sécurité,

et, lorsque les membres du service sont mis sur pied pour un service actif, pour:

 4. garantir la sécurité préventive de l'armée à l'égard de l'espionnage, du sabotage et d'autres activités illicites,
 5. rechercher des renseignements,
 6. veiller à la protection de personnes occupant des postes de représentants de l'Etat;
- i. au Service de renseignements du Département fédéral de la défense, de la protection de la population et des sports, dans le contexte d'informations importantes pour la politique de sécurité;
- j. à la justice militaire, pour l'exécution de tâches de police judiciaire et de police de sécurité;
- k. aux organes des gardes-frontière et de la douane, pour localiser des personnes, opérer des contrôles douaniers et effectuer des enquêtes pénales administratives;
- l. au Secrétariat d'Etat à l'économie, pour l'application de la loi fédérale du 13 décembre 1996 sur le matériel de guerre²⁵, et pour l'exécution de mesures dans le domaine de la législation régissant les échanges extérieurs;
- m. à l'Office fédéral de la formation professionnelle et de la technologie, pour l'octroi de permis d'emploi de substances explosibles;
- n. à l'Office fédéral de l'aviation civile et à La Poste Suisse, pour l'exécution des mesures en matière de police de sécurité;
- o. à l'Office fédéral de l'énergie, pour l'application de la loi du 23 décembre 1959 sur l'énergie atomique²⁶ et pour l'exercice de son droit de coopérer dans le domaine de la législation régissant les échanges extérieurs;
- p.²⁷ aux services de la Confédération et des cantons compétents pour initier des contrôles de sécurité relatifs aux personnes (services requérants), au service fédéral chargé de la mise en œuvre de ces contrôles (intégré à la DPPO) ou aux services spécialisés des cantons;
- q. aux organes administratifs concernés, pour assurer leur sécurité;
- r. à des organes administratifs et à des particuliers, pour leur permettre de motiver une demande de renseignements;
- s. à des particuliers, pour écarter un danger considérable;

²⁵ RS 514.51

²⁶ [RO 1960 585, 1983 1886 art. 36 ch. 2, 1987 544, 1993 901 annexe ch. 9, 1994 1933 art. 48 ch. 1, 1995 4954, 2002 3673 art. 17 ch. 3, 2004 3503 annexe ch. 4. RO 2004 4719 annexe ch. I 1]. Voir actuellement la loi du 21 mars 2003 sur l'énergie nucléaire (RS 732.1).

²⁷ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

t.²⁸ à des autorités de sécurité étrangères, dans le cadre des demandes de clearing (demandes de conformité); les données qui ne sont pas dans l'intérêt de la personne concernée ne peuvent être transmises qu'avec l'accord exprès de celle-ci;

u.²⁹ à l'Office européen de police (Europol), aux fins de la coopération prévue par l'Accord du 24 septembre 2004 entre la Confédération suisse et l'Office européen de police³⁰.

² Pour la communication à l'étranger, sont applicables les art. 17, al. 3 à 5, et 7 LMSI.

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

⁴ Lors de toute communication, le destinataire doit être renseigné sur la fiabilité et l'actualité des données (art. 10). Il ne peut utiliser les données que dans le but pour lequel elles lui ont été transmises. Il doit être rendu attentif aux restrictions d'emploi et au fait que l'autorité qui communique les données se réserve le droit de se renseigner sur l'utilisation qui en aura été faite.

⁵ La communication, ainsi que ses destinataires, son objet et ses motifs, doivent être enregistrés.

⁶ La communication des données issues des banques DEWA et DEBBWA est régie par l'art. 43 de l'ordonnance du 21 septembre 1998 sur les armes, les accessoires d'armes et les munitions (OArm)³¹.

Art. 14 Copie de données

¹ Les données d'ISIS ne peuvent être reportées dans d'autres fichiers ni par le biais d'installations de communication ni au moyen de supports de données. L'archivage électronique des données d'ISIS aux Archives fédérales n'est pas soumis à la présente disposition.

² Des données d'ISIS peuvent être passagèrement transférées dans des banques de données de travail aux fins de travaux d'exploitation particuliers. Ceux-ci terminés, les données doivent être effacées.

Art. 15 Droit d'être renseigné

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

² Le droit d'être renseigné sur les banques de données DEWA et DEBBWA est régi par les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données³².

²⁸ Introduite par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO **2004** 3495).

²⁹ Introduite par le ch. I de l'O du 10 mars 2006 (RO **2006** 921).

³⁰ RS **0.360.268.2**

³¹ RS **514.541**

³² RS **235.1**

Art. 16 Appréciation générale périodique des données de la banque ST

¹ La Section Assurance qualité du SAP procède à une appréciation générale de chaque bloc de données au plus tard cinq ans après la saisie de la première communication et trois ans après la dernière appréciation générale.³³

² Elle vérifie, à la lumière des dangers et des risques qui menacent la sécurité du pays, si les communications et les objets saisis dans un bloc présentent un degré de vraisemblance élevé s'agissant du risque pour la sécurité intérieure, en vue d'une appréciation administrative, et si les données sont nécessaires pour d'autres tâches de protection de l'Etat.³⁴

³ Les communications et les relations qui figurent dans la banque de données depuis plus de trois ans, avec l'appréciation «peu fiables», ne peuvent continuer d'être traitées comme telles (code «u») jusqu'à la prochaine appréciation générale que si elles sont nécessaires à l'accomplissement de tâches légales et si le chef du SAP ou l'un de ses suppléants en a autorisé le traitement.³⁵

⁴ Les objets identifiés depuis plus de trois ans comme des données relatives à des tiers sont effacés lors de l'appréciation générale.³⁶

⁵ L'Assurance qualité efface les données devenues inutiles. En cas de traitement ultérieur de données encore nécessaires, la date de la dernière appréciation générale doit être enregistrée.

Art. 17 Durée de conservation des données

¹ Les données de police préventive peuvent être mémorisées dans ISIS pendant une durée maximum de quinze ans.

² Pour les données ci-après, la durée de conservation maximale est la suivante:

- a. 20 ans pour les données relatives à des programmes de recherches de police préventive en cours;
- b. dix ans au plus pour les données relatives à des interdictions d'entrée, à compter de leur expiration;
- c. cinq ans pour les données recueillies dans le cadre de procédures de contrôles de sécurité relatifs aux personnes;
- d. 30 et 10 ans respectivement pour les données relevant de la correspondance avec des organes administratifs et des particuliers.

³³ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

³⁴ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

³⁵ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

³⁶ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

³ Les données des banques DO, BARBARA, IPOS, NEWS, IPIS, Infopress et ISIS-Info peuvent être conservées pendant une durée illimitée.³⁷

⁴ La conservation des données dans les banques DEWA et DEBBWA est régie par l'art. 45 OArm³⁸.

Art. 18 Effacement des données

¹ A l'expiration de leur durée de conservation, les données sont effacées dans un délai de trois mois, à moins que le chef du SAP ou l'un de ses suppléants ne décide, à la lumière des dangers et des risques existants, qu'elles sont indispensables à l'accomplissement de tâches légales.³⁹

² Dans les cas visés à l'al. 1, la durée de conservation ultérieure des données s'élève à trois ans. Elle ne peut être prolongée qu'une fois.

³ Tout le bloc de données ainsi que toute factsheet éventuelle sont supprimés avec l'effacement de la dernière communication (y compris les relations, données d'image et mandats correspondants).⁴⁰

⁴ Les données destinées à être supprimées, à l'exception des informations définies à l'art. 20, al. 2, sont transférées dans le module d'archivage.⁴¹

Art. 19⁴² Données et dossiers des organes cantonaux chargés de la protection de l'Etat

¹ Les organes cantonaux chargés du maintien de la sécurité intérieure peuvent conserver cinq ans au plus après la première saisie 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 doivent être effacées et les dossiers détruits.

Art. 20 Obligation de proposer les documents aux Archives fédérales

¹ Les données et les dossiers devenus inutiles ou destinés à être effacés ou détruits sont proposés aux Archives fédérales aux fins d'archivage.⁴³

³⁷ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

³⁸ RS 514.541

³⁹ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴⁰ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴¹ Introduit par le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴² Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴³ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

² Les documents classifiés (données et dossiers) émanant des relations avec les autorités de sécurité étrangères et de la recherche opérative ne sont pas proposés aux fins d'archivage, mais conservés en interne d'entente avec les Archives fédérales.⁴⁴

³ Les données que les Archives fédérales jugent sans valeur archivistique sont effacées du module d'archivage. Les autres dispositions légales en matière de destruction de données sont réservées.⁴⁵

⁴ Avant la remise des documents d'un dossier personnel aux Archives fédérales, le SAP introduit dans la banque de données VE la date de livraison, le numéro d'enregistrement, ainsi que les données établissant l'identité de la personne concernée; ces informations sont conservées pendant dix ans, puis effacées.

Section 4 Dispositions relatives à l'organisation

Art. 21 Sécurité des données et journalisation

¹ Pour assurer la sécurité des données, sont applicables l'art. 20 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)⁴⁶, l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale⁴⁷ ainsi que les conditions fixées par le département selon l'art. 8 de la présente ordonnance pour le raccordement des organes cantonaux chargés du maintien de la sécurité intérieure.⁴⁸

² Le SAP précise dans un règlement ISIS les mesures organisationnelles et techniques contre le traitement non autorisé des données et les modalités de la journalisation automatique des données.

³ Les données ISIS ne peuvent être transmises que sous forme chiffrée durant toute l'opération de transmission.

Art. 22 Responsabilités et compétences

¹ Le SAP assume la responsabilité d'ISIS. Il en édicte le règlement.

² La Section Assurance qualité du SAP est chargée de la formation et de l'assistance aux utilisateurs et elle veille à la mise en œuvre du règlement ISIS.⁴⁹

³ Le Centre de service informatique du département veille à l'exploitation et à la sécurité d'ISIS.

⁴⁴ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴⁵ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴⁶ RS 235.11

⁴⁷ RS 172.010.58

⁴⁸ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴⁹ Nouvelle teneur selon le ch. I de l'O du 30 juin 2004, en vigueur depuis le 1^{er} sept. 2004 (RO 2004 3495).

⁴ Le conseiller à la protection des données de la fedpol peut vérifier au cas par cas que le traitement de données dans ISIS se fait bien conformément aux dispositions relatives à la protection des données.

Art. 23 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.

Art. 24 Exigences techniques

¹ Le département détermine les exigences techniques auxquelles doivent satisfaire les terminaux des cantons.

² Les détails sont fixés dans le règlement ISIS.

Section 5 Dispositions finales

Art. 25 Abrogation du droit en vigueur

L'ordonnance du 1^{er} décembre 1999 sur le système de traitement des données relatives à la protection de l'Etat⁵⁰ est abrogée.

Art. 26⁵¹

Art. 27 Entrée en vigueur

La présente ordonnance entre en vigueur le 1^{er} janvier 2002.

⁵⁰ [RO 1999 3461, 2000 1227 annexe ch. II 1 2027]

⁵¹ Abrogé par le ch. I de l'O du 30 juin 2004, avec effet au 1^{er} sept. 2004 (RO 2004 3495).

