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

Modification du 30 juin 2004

Le Conseil fédéral suisse
arrête:

I

L'ordonnance ISIS du 30 novembre 2001[1] est modifiée comme suit:

Art. 2, al. 2, let. a, e et f

2 ISIS est utilisé pour:

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

e. l'exécution de travaux de documentation;

f. la gestion des affaires.

Art. 3 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;

1 RS **120.3**

j. factsheets: appréciations périodiques standardisées de l'analyse stratégique relative à un objet spécifique.

Art. 4 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»;

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)[2];

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;

2 RS **120.2**

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;

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. 5 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, al. 1

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

Art. 7 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 DPIO); 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.

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

Art. 8 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. 9

Abrogé

Art. 10, al. 2, 2bis, 3 et 4

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

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.

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

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»).

Art. 11 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, al. 1, 2 et 4

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.

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

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

Art. 13, al. 1, let. c, phrase introductive, let. e, p et t

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:

c. 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;

e. à l'Office fédéral de l'immigration, de l'intégration et de l'émigration (IMES), pour l'application de mesures contre des étrangers, notamment en vue de leur éloignement, ainsi que pour traiter des demandes de naturalisation;

p. 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 DPIO) ou aux services spécialisés des cantons;

t. 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.

Art. 16, al. 1 à 4

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.

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.

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.

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

Art. 17, al. 3

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

Art. 18, al. 1, 3 et 4

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.

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).

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.

Art. 19 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, al. 1 à 3

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

[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.

[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.

Art. 21, al. 1

[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)[3], l'ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale[4] 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.

Art. 22, al. 2

[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.

Art. 26

Abrogé

3 RS **235.11**
4 RS **172.010.58**

II

La présente modification entre en vigueur le 1er septembre 2004.

30 juin 2004 Au nom du Conseil fédéral suisse:

Le président de la Confédération, Josef Deiss
La chancelière de la Confédération, Annemarie Huber-Hotz