

Ordonnance
sur le système de traitement des données
en matière de lutte contre le crime organisé
(Ordonnance ISOK)

du 19 novembre 1997 (Etat le 16 mai 2000)

Le Conseil fédéral suisse,

vu les articles 11, 1^{er} alinéa, 12, 2^e alinéa, 13, 1^{er} alinéa, et 15 de la loi fédérale du 7 octobre 1994¹ sur les Offices centraux de police criminelle de la Confédération (LOC),

arrête:

Section 1: Dispositions générales

Article premier **Objet**

La présente ordonnance règle la gestion et l'utilisation du système de traitement des données en matière de lutte contre le crime organisé (ISOK) par l'Office central de lutte contre le crime organisé (office central).

Art. 2 **But**

ISOK sert à faciliter:

- a. les tâches légales d'information, de coordination et d'analyse de l'office central;
- b. l'exécution des enquêtes préventives et des enquêtes de police judiciaire relatives aux cas de criminalité organisée;
- c. la coopération avec les autorités cantonales de poursuite pénale, par la mise en place d'un système permettant aux services de police criminelle des cantons qui participent à la lutte contre le crime organisé et qui coopèrent avec l'office central dans le cadre de leurs compétences d'accéder aux données qui peuvent être utiles dans la lutte contre le crime organisé;
- d. la collaboration à la lutte menée par d'autres Etats contre le crime organisé international.

Art. 3 **Champ d'application**

¹ Les données enregistrées dans ISOK concernent:

RO 1998 43

¹ RS 172.213.71

- a. les organisations que l'on peut raisonnablement soupçonner d'être des organisations criminelles au sens de l'article 260^{ter} du code pénal²;
- b. les personnes que l'on peut raisonnablement soupçonner de préparer, de commettre ou de faciliter des actes délictueux auxquels on présume que participe une organisation au sens de la lettre a;
- c. les personnes que l'on peut raisonnablement soupçonner d'appartenir à une organisation au sens de la lettre a ou de lui apporter leur soutien.

² Des informations concernant des tierces personnes ne sont enregistrées que si cela est nécessaire au sens de l'article 2.

Art. 4 Provenance des données

Les données enregistrées dans ISOK proviennent:

- a. d'investigations policières effectuées avant l'ouverture d'une enquête de police judiciaire;
- b. d'enquêtes de police judiciaire menées par les autorités cantonales de poursuite pénale et de police;
- c. d'enquêtes de police judiciaire menées par les autorités fédérales de poursuite pénale et de police;
- d. de renseignements communiqués conformément aux articles 4 et 8, 1^{er} alinéa, LOC;
- e. de vérifications effectuées dans le cadre de l'exécution de demandes d'entraide judiciaire avec recherche de preuves.

Art. 5 Sous-systèmes et essais

¹ ISOK se compose des sous-systèmes suivants:

- a. «Personnes et antécédents» (PV), où sont enregistrées des données sur des personnes et leurs antécédents recueillies dans le cadre d'enquêtes préventives ou d'enquêtes de police judiciaire;
- b. «Journaux» (JO), où sont enregistrées des données (observations, contrôles téléphoniques, etc.) recueillies sur toute affaire faisant l'objet d'une enquête préventive ou d'une enquête de police judiciaire;
- c. «Contrôle des affaires et des délais» (GT), où est enregistré le suivi des enquêtes en cours menées par l'office central (date d'ouverture, mesures ordonnées, etc.);
- d. «Renseignements généraux» (ER), où sont enregistrées des données utiles à la lutte contre le crime organisé (répertoires téléphoniques, extraits de presse, descriptif des compétences de diverses administrations, etc.);
- e. lexiques techniques, répertoires et méthodes d'action criminelle (DL);

² RS 311.0

- f. «Rapport de situation» (LA), où sont enregistrés des rapports décrivant la situation nationale et internationale en matière de crime organisé;
- g. «Représentation graphique» (VI), où sont enregistrés des graphiques relatifs aux structures des organisations criminelles.

² Le Département fédéral de justice et police (département) peut autoriser l'office central à effectuer des essais visant à évaluer de nouveaux outils informatiques et à exploiter et établir spécialement des graphiques représentant les connexions entre les personnes soupçonnées, sur la base de données extraites des sous-systèmes «Personnes et antécédents» et «Journaux». Les essais ne peuvent être effectués que par des spécialistes de l'office central autorisés à cet effet. Les résultats, enregistrés dans le sous-système «Représentation graphique», ne sont accessibles qu'à certains utilisateurs désignés. Les essais ont une durée maximale de trois ans.

Art. 6 Chiffrement

Lors de leur transmission, les données d'ISOK doivent faire l'objet d'un chiffrement de bout en bout.

Art. 7 Données traitées

¹ Seules les données énumérées à l'annexe 1 peuvent être traitées dans ISOK.

² Le sous-système «Personnes et antécédents» (PV) se compose:

- a. des données de base relatives à l'identité des personnes;
- b. des antécédents, soit les données relatives aux faits;
- c. des sous-champs dont l'utilisation permet, entre autres, de marquer les éléments de comparaison, notamment avec des tierces personnes, dans le texte d'un antécédent et de consulter des données d'après ces éléments de comparaison. La liste complète des sous-champs figure à l'annexe 1.

³ Le sous-système «Journaux» se compose:

- a. de l'en-tête, soit les données relatives aux journaux tenus dans le cadre d'une affaire;
- b. des inscriptions, soit les données relatives aux faits.

⁴ Constituent un bloc de données:

- a. les données de base et les antécédents qui s'y rapportent;
- b. l'en-tête des données et les inscriptions qui s'y rapportent.

⁵ Dans les sous-systèmes «Personnes et antécédents» et «Journaux», les données recueillies dans le cadre des enquêtes préventives et dans le cadre des enquêtes de police judiciaire font l'objet de catégories distinctes.

⁶ Dans le sous-système «Journaux», les données provenant de contrôles téléphoniques constituent une catégorie distincte.

⁷ Les données de base du système ISOK, celles du système DOSIS (ordonnance DOSIS du 26 juin 1996³) et celles du système FAMP (Ordonnance FAMP du 28 sept. 1998⁴) sont regroupées, dans un index commun.⁵

Section 2: Utilisateurs et accès

Art. 8 Accès aux données

¹ Sont raccordés à ISOK au moyen d'une procédure d'appel:

- a. l'office central;
- b. les brigades de police criminelle des corps de police des cantons qui prennent part à la lutte contre le crime organisé;
- c. le service de contrôle;
- d. le conseiller à la protection des données de l'Office fédéral de la police;
- e. le chef de projet et les gestionnaires du système.

² Les autorités de poursuite pénale spécialisées des cantons peuvent, sur demande, être raccordées à ISOK pour des procédures déterminées.

³ Les autorisations individuelles d'accès aux différentes données d'ISOK sont fixées à l'annexe 2.

⁴ Un seul sous-système peut être consulté à la fois.

Art. 9 Accès aux sous-systèmes «Personnes et antécédents» et «Journaux»

¹ Les organes ayant introduit les données dans le sous-système «Personnes et antécédents» peuvent, notamment pour les données recueillies dans le cadre d'enquêtes de police judiciaire, restreindre l'accès aux données qu'ils ont saisies, en déterminant les personnes autorisées à les traiter.

² Dans le cadre d'une enquête, seuls les services de police criminelle et les autorités de poursuite pénale des cantons qui mènent cette enquête, ainsi que les collaborateurs de l'office central, ont accès aux données du sous-système «Journaux».

³ Si un autre canton est concerné par l'enquête, l'office central ou le service cantonal compétent peut de même étendre l'accès aux données à l'autorité correspondante du canton concerné.

³ RS 812.121.7

⁴ RS 360.3

⁵ Nouvelle teneur selon le ch. 2 de l'annexe 3 à l'O FAMP du 28 sept. 1998, en vigueur depuis le 1^{er} nov. 1998 (RS 360.3).

Section 3: Traitement des données

Art. 10 Saisie des données et contrôle de qualité

¹ L'office central et les services de police criminelle des cantons participant à la lutte contre le crime organisé saisissent eux-mêmes dans ISOK les données concernant les antécédents qu'ils ont recueillis. Ce faisant, ils déterminent les catégories d'antécédents, fixent la durée de conservation conformément à l'article 16 et qualifient ces antécédents comme étant fiables ou peu fiables en fonction de leur provenance, de leur mode de transmission, de leur contenu et des données déjà disponibles.

² Les données destinées aux sous-systèmes «Personnes et antécédents» et «Journaux» sont saisies provisoirement jusqu'à ce qu'elles soient vérifiées par le service de contrôle.

³ Le service de contrôle de DOSIS/ISOK de l'Office fédéral de la police (service de contrôle) examine si les données saisies sont conformes aux dispositions de la présente ordonnance. Si tel n'est pas le cas, il les corrige ou les efface, après en avoir informé l'organe ayant effectué la saisie.

⁴ Le service de contrôle vérifie, au besoin en collaboration avec l'organe ayant effectué la saisie, les données saisies provisoirement, en particulier l'indication des sources, le degré d'exploitabilité technique et policière et de fiabilité de l'information, la légalité, la date de la prochaine appréciation générale et la durée de conservation. Il confirme la saisie définitive des données ou demande leur correction ou leur effacement. L'Office fédéral de la police précise les modalités de la vérification des données dans le règlement de traitement.

Art. 11 Communication de données à des autorités tenues de fournir des renseignements

¹ Si cela lui est nécessaire pour obtenir les renseignements dont il a besoin et motiver ses demandes d'entraide administrative, l'office central peut communiquer des données personnelles enregistrées dans ISOK aux autorités suivantes tenues de coopérer au sens de l'article 4 LOC:

- a. les autorités de poursuite pénale, notamment les ministères publics, les juges d'instruction, les autorités d'entraide judiciaire et les organes de police judiciaire de la Confédération et des cantons;
- b. les services de police, notamment les organes de la police de sûreté et de la police administrative de la Confédération et des cantons, ainsi que les autorités fédérales chargées de l'application de la loi fédérale du 21 mars 1997⁶ instituant des mesures visant au maintien de la sûreté intérieure;
- c. les organes de surveillance des frontières et les services douaniers;
- d. les autorités de la Confédération et des cantons assumant des tâches de police des étrangers compétentes en matière d'entrée et de séjour des étrangers,

⁶ RS 120

ou d'octroi du droit d'asile ou chargées de rendre les décisions d'admission provisoire;

- e. les contrôles des habitants et les autorités chargées en particulier de l'administration des registres du commerce, des registres d'état civil, des registres fiscaux, des registres de la circulation routière, des registres de l'aviation civile et des registres fonciers;
- f. les autorités compétentes en matière de relations diplomatiques et consulaires;
- g. les autres autorités chargées de délivrer les autorisations de circulation pour certains biens.

² Afin de les assister dans l'accomplissement de leurs tâches légales, l'office central peut en outre communiquer spontanément des données personnelles enregistrées dans ISOK aux autorités suivantes:

- a. les autorités mentionnées au 1^{er} alinéa, lettre a, dans le cadre de procédures pénales, d'enquêtes de police judiciaire et de procédures d'entraide judiciaire;
- b. les autorités mentionnées au 1^{er} alinéa, lettres b et c, dans le cadre d'enquêtes de police judiciaire, ainsi que pour l'accomplissement de tâches relatives à l'application de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure;
- c. les autorités mentionnées au 1^{er} alinéa, lettre d, chargées d'accomplir des tâches de police des étrangers, d'empêcher ou de réprimer les infractions aux dispositions relatives à l'entrée et au séjour des étrangers et à la législation en matière d'asile.

³ L'étendue du devoir de renseigner et les conditions auxquelles il est soumis sont régies par l'article 6, 2^e à 4^e alinéa, de l'ordonnance du 19 novembre 1997⁷ sur les Offices centraux de police criminelle près l'Office fédéral de la police (OOC).

Art. 12 Communication de données à d'autres destinataires

¹ Si cela lui est nécessaire pour obtenir les renseignements dont il a besoin et motiver ses demandes d'entraide administrative, l'office central peut communiquer des données personnelles enregistrées dans ISOK à d'autres destinataires, à savoir:

- a. les autres offices centraux de l'Office fédéral de la police;
- b. les autorités d'autres Etats exerçant des fonctions de poursuite pénale et de police, dans la mesure où les conditions énumérées à l'article 13, 2^e alinéa, LOC sont remplies;
- c. les organisations internationales exerçant des fonctions de poursuite pénale et de police (notamment EUROPOL et INTERPOL), dans la mesure où les conditions énumérées à l'article 13, 2^e alinéa, LOC sont remplies;
- d. les autorités financières de la Confédération et des cantons;

⁷ RS 360.1

- e. l'Administration fédérale des finances;
- f. la Commission fédérale des banques;
- g. l'autorité de contrôle en matière de lutte contre le blanchiment d'argent;
- h. l'Office fédéral des affaires économiques extérieures;
- i. les autorités fédérales chargées des contrôles de sécurité relatifs à des personnes et des mesures de protection au sens de l'article 2, 4^e alinéa, lettres c et d, de la loi fédérale du 21 mars 1997⁸ instituant des mesures visant au maintien de la sûreté intérieure;
- k. l'Office fédéral de l'aviation civile;
- l. les autorités compétentes en matière d'acquisition de terrains par des personnes résidant à l'étranger;
- m. les organisations non étatiques, qui œuvrent notamment en faveur de la lutte contre l'exploitation sexuelle à des fins commerciales, dans la mesure où il s'agit de prévenir et d'identifier des formes spécifiques de criminalité;
- n. les autorités de surveillance de la Confédération et des cantons.

² Afin de les assister dans l'accomplissement de leurs tâches légales, l'office central peut en outre communiquer spontanément des données personnelles enregistrées dans ISOK aux autorités suivantes:

- a. les autorités d'autres Etats exerçant des fonctions de poursuite pénale, pour leurs enquêtes de police judiciaire, dans la mesure où les conditions énumérées à l'article 13, 2^e alinéa, LOC sont remplies;
- b. les organisations internationales exerçant des fonctions de poursuite pénale et de police (notamment EUROPOL et INTERPOL), pour le traitement d'affaires déterminées, dans la mesure où les conditions énumérées à l'article 13, 2^e alinéa, LOC sont remplies;
- c. les autorités financières de la Confédération et des cantons, pour leurs enquêtes de police judiciaire dans le domaine fiscal;
- d. l'Administration fédérale des finances, dans le cadre des procédures pénales administratives qu'elle mène;
- e. la Commission fédérale des banques, pour l'assister dans son activité de surveillance découlant de la législation sur les banques, les bourses et les fonds de placement, s'il s'agit d'informations fiables qui sont nécessaires à une procédure ou susceptibles d'entraîner l'ouverture d'une procédure;
- f. l'autorité de contrôle en matière de lutte contre le blanchiment d'argent, pour l'assister dans son activité de surveillance découlant de la loi du 10 octobre 1997⁹ sur le blanchiment d'argent, s'il s'agit d'informations fiables qui sont nécessaires à une procédure ou susceptibles d'entraîner l'ouverture d'une procédure;

⁸ RS 120

⁹ RS 955.0

- g. les autorités fédérales chargées des contrôles de sécurité relatifs à des personnes et des mesures de protection au sens de l'article 2, 4^e alinéa, lettres c et d, de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure, pour leurs investigations, s'il s'agit d'informations fiables.

³ Toutes les données personnelles sont communiquées sur requête aux autorités de surveillance de la Confédération et des cantons, ainsi qu'au Préposé fédéral à la protection des données, pour leurs fonctions de contrôle.

Art. 13 Autres dispositions relatives à la communication de données

¹ Lors de la communication de données d'ISOK, les interdictions portant sur l'utilisation doivent être respectées. L'office central ne peut communiquer à des Etats étrangers des données concernant des demandeurs d'asile, des réfugiés ou des personnes provisoirement admises qu'après consultation de l'office fédéral compétent.

² L'office central refuse la communication de données d'ISOK si des intérêts prépondérants publics ou privés s'y opposent.

³ Dans le cadre d'une enquête de police judiciaire, les services de police criminelle des cantons participant à la lutte contre le crime organisé peuvent communiquer des données d'ISOK aux autres autorités de poursuite pénale et de police de leur canton. L'office central doit en être informé.

⁴ Lors de toute communication de données d'ISOK, le destinataire doit être informé de leur fiabilité et de leur actualité. Il ne peut les utiliser que dans le but en vue duquel elles lui ont été communiquées. Il doit être prévenu des restrictions d'emploi et du fait que l'office central se réserve le droit d'exiger des informations sur l'utilisation qui aura été faite de ces données.

⁵ La communication, ainsi que le destinataire, l'objet et le motif de la demande de renseignements doivent être enregistrés dans ISOK.

⁶ Afin d'éviter une double saisie, les données faisant l'objet d'une mention spéciale à l'annexe 1 de la présente ordonnance qui sont transmises par le canal d'INTERPOL peuvent être copiées dans l'Index central des dossiers (ZAN). Cette fonction n'est pas automatisée et l'Office fédéral de la police précise les modalités de cette opération dans le règlement sur le traitement des données.¹⁰

Art. 14 Traitement des demandes de renseignements présentées par des personnes concernées

Le traitement des demandes de renseignements concernant les données d'ISOK est régi par l'article 14 LOC.

¹⁰ Nouvelle teneur selon le ch. 2 de l'annexe 3 à l'O FAMP du 28 sept. 1998, en vigueur depuis le 1^{er} nov. 1998 (RS **360.3**).

Art. 15 Appréciation générale et périodique des données des sous-systèmes
«Personnes et antécédents» et «Journaux»

¹ Le service de contrôle procède à une appréciation générale de chaque bloc de données des sous-systèmes «Personnes et antécédents» et «Journaux» au plus tard trois ans après la saisie de la première donnée ou trois ans après la dernière appréciation générale.

² Lors de la saisie d'un fait nouveau, les données peu fiables sur les antécédents d'une personne qui sont déjà enregistrées dans le bloc de données afférent doivent faire l'objet d'une nouvelle appréciation.

Art. 16 Durée de conservation

¹ La durée de conservation des données relatives aux personnes contenues dans ISOK est de:

- a. deux ans depuis la saisie d'une donnée peu fiable recueillie avant l'ouverture d'une enquête de police judiciaire;
- b. dix ans depuis la saisie d'une donnée fiable recueillie avant l'ouverture d'une enquête de police judiciaire;
- c. en principe deux ans depuis la saisie d'une donnée peu fiable de police judiciaire;
- d. en principe dix ans depuis la saisie d'une donnée fiable de police criminelle, mais au plus tard jusqu'à ce que l'infraction visée soit prescrite.

² Toute donnée peu fiable de police criminelle peut continuer à être traitée pendant une année au plus:

- a. si elle est nécessaire à l'accomplissement de tâches légales; et
- b. si, sur proposition du chef du service de contrôle, le chef de l'office central donne son autorisation.

Art. 17 Effacement des données

¹ Tout bloc de données doit être effacé dans son intégralité en même temps que le dernier antécédent ou la dernière inscription.

² Les données recueillies sur des personnes sur lesquelles pesaient des soupçons au sens de l'article 3, 1^{er} alinéa, qui se sont définitivement révélés infondés doivent être immédiatement effacées.

³ Les données recueillies sur une tierce personne au sens de l'article 3, 2^e alinéa, doivent être immédiatement effacées dès qu'elles ne sont plus nécessaires à l'enquête, mais au plus tard lors de l'effacement des données relatives à la personne enregistrée à titre principal.

Art. 18 Communication de l'effacement des données aux cantons

Lorsque des données d'ISOK saisies par des services de police criminelle des cantons coopérant avec l'office central sont effacées, le service de contrôle doit en informer les services en question.

Art. 19 Remise de données et de documents aux Archives fédérales

¹ L'office central remet aux Archives fédérales, au plus tard lors de l'effacement d'un bloc de données, les données et documents qui s'y rapportent.

² Il remet également aux Archives fédérales les données et documents qui ne font pas partie d'un dossier personnel, au plus tard dès l'effacement dans ISOK du dernier antécédent ou de la dernière inscription qui s'y rapporte.

³ Les autres dispositions légales en matière de destruction de données sont réservées.

Section 4: Mesures organisationnelles**Art. 20** Sécurité des données et journalisation

¹ La sauvegarde de la sécurité des données est régie par l'ordonnance du 14 juin 1993¹¹ relative à la loi fédérale sur la protection des données et le chapitre 3 de l'ordonnance du 23 février 2000 sur l'informatique dans l'administration fédérale (OIAF)^{12,13}

² L'Office fédéral de la police décrit, dans le règlement sur le traitement des données, les mesures organisationnelles et techniques à prendre pour éviter le traitement non autorisé des données et pour assurer la journalisation automatique du traitement des données.

Art. 21 Surveillance et responsabilité

¹ L'Office fédéral de la police est responsable d'ISOK. Il arrête le règlement sur le traitement des données.

² Le service de contrôle veille à ce que les utilisateurs se conforment à la présente ordonnance, à ses annexes et au règlement sur le traitement des données.

³ Le centre de calcul du département est responsable de l'exploitation et de la sécurité d'ISOK.

Art. 22 Financement

¹ La Confédération finance la transmission des données jusqu'au distributeur principal sis dans les cantons.

¹¹ RS 235.11

¹² RS 172.010.58

¹³ Nouvelle teneur selon le ch. II 5 de l'annexe à l'O du 23 fév. 2000 sur l'informatique dans l'administration fédérale, en vigueur depuis le 1^{er} avril 2000 (RS 172.010.58).

² Les cantons assument:

- a. les frais d'acquisition et d'exploitation de leurs appareils;
- b. les frais d'installation et d'exploitation de leur réseau de distribution.

Art. 23 Exigences techniques

¹ Les terminaux utilisés par les cantons doivent répondre aux exigences techniques de la Confédération.

² L'Office fédéral de la police règle les détails dans le règlement sur le traitement des données.

Section 5: Entrée en vigueur

Art. 24

¹ La présente ordonnance entre en vigueur le 1^{er} janvier 1998, sous réserve des 2^e et 3^e alinéas.

² L'article 12, 2^e alinéa, lettre f, entre en vigueur en même temps que la loi du 10 octobre 1997¹⁴ sur le blanchiment d'argent.

³ Les dispositions de l'article 11, 1^{er} alinéa, lettre b, et 2^e alinéa, lettre b, concernant les autorités chargées de l'application de la loi fédérale du 21 mars 1997¹⁵ instituant des mesures visant au maintien de la sûreté intérieure, ainsi que l'article 12, 1^{er} alinéa, lettre i, et 2^e alinéa, lettre g, entrent en vigueur en même temps que ladite loi.

¹⁴ RS 955.0. Cette loi est entrée en vigueur le 1^{er} avril 1998.

¹⁵ RS 120. Cette loi est entrée en vigueur le 1^{er} juillet 1998.

Annexes 1 et 2¹⁶

¹⁶ Les annexes 1 et 2 ne sont publiées ni dans le RO, ni dans le RS. Des exemplaires tirés à part peuvent être obtenus auprès de l'Office central fédéral des imprimés et du matériel, 3000 Berne (Pour l'annexe 2, voir RS **360.3** annexe 3 ch. 2).