

Système d'information Schengen de deuxième génération (SIS II): établissement, fonctionnement et utilisation

2005/0103(CNS) - 12/06/2007 - Acte final

OBJECTIF : établir un système d'information Schengen de 2^{ème} génération ou SIS II (volet relevant de la coopération policière et judiciaire en matière pénale).

ACTE LÉGISLATIF : Décision 2007/533/JAI du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de 2^{ème} génération (SIS II).

CONTEXTE : le SIS est un système d'information commun permettant aux autorités compétentes des États membres d'échanger des informations en vue de faciliter la mise en place d'un espace européen sans contrôles aux frontières intérieures dans l'Union. Conçu comme une mesure compensatoire permettant aux États membres de maintenir un niveau élevé de sécurité dans un espace commun de libre circulation, le SIS avait été institué en 1990 dans un cadre intergouvernemental avec la Convention de Schengen. Depuis, les dispositions fondamentales de la Convention ont été intégrées dans le cadre de l'UE.

Après plusieurs années d'utilisation, il est apparu nécessaire de remodeler le SIS afin de répondre aux nouveaux défis posés par l'élargissement de l'Union et par la lutte contre le terrorisme. C'est dans ce contexte que le Conseil a jeté les bases d'un SIS dit de 2^{ème} génération en prévoyant dès 2001 son développement technique et son financement par le budget communautaire (voir règlement (CE) n° 2424/2001 - [CNS/2001/0818](#) et décision 2001/886/JAI – [CNS/2001/0819](#)).

La présente décision et le règlement « pilier I » parallèle (règlement (CE) n° 2006/1987, voir [COD/2005/0106](#)) qui constituent ensemble la base légale du SIS II, marquent la 2^{ème} étape de la mise en place du SIS et prévoit l'établissement, les modalités de fonctionnement et d'utilisation du SIS II.

À noter parallèlement, l'adoption d'un 3^{ème} instrument destiné à étendre l'accès du SIS (et sous certaines conditions), aux services nationaux de délivrance des certificats d'immatriculation des véhicules (voir [COD/2005/0104](#)).

CONTENU : Avec le règlement (CE) n° 2006/1987 du Parlement et du Conseil, la présente décision fixe les objectifs généraux du SIS II, son architecture technique et de financement, ses règles de fonctionnement et d'utilisation. Le cadre législatif régissant le SIS II définit également les catégories de données à introduire dans le système, les finalités et les critères de leur introduction, les autorités qui sont autorisées à y avoir accès ainsi que les règles complémentaires à observer en matière de traitement et de protection des données à caractère personnel.

Architecture technique et mode de fonctionnement du SIS II : le SIS II se compose:

1. d'un système central (le "SIS II central") comprenant une fonction de support technique (le "CS-CIS") contenant la base de données du SIS II ainsi qu'une interface nationale uniforme (le "NI-SIS") ;
2. d'un système national (le "N.SIS II") dans chaque État membre, constitué des systèmes de données nationaux reliés au SIS II central ;

3. d'une infrastructure de communication entre le CS-SIS et la NI-SIS, fournissant un réseau virtuel crypté consacré aux données du SIS II et à l'échange de données entre les instances chargée de l'échange de toutes les informations supplémentaires (bureaux SIRENE).

Les données du SIS II sont introduites, mises à jour, supprimées et consultées par le biais des systèmes nationaux. Le CS-SIS, qui assure le contrôle et la gestion techniques, est installé à Strasbourg et un CS-SIS de secours, capable d'assurer l'ensemble des fonctionnalités du CS-SIS principal en cas de défaillance, est installé à Sankt Johann im Pongau (Autriche). Il assure les services nécessaires à l'introduction et au traitement des données du SIS II.

Les coûts de mise en place, d'exploitation et de maintenance du SIS II central et de l'infrastructure de communication sont à la charge du budget de l'UE.

Autorités responsables de la gestion des données du SIS II : des dispositions sont prévues pour déterminer les responsabilités incombant aux États membres ou à l'instance gestionnaire qui sera mise en place pour assurer, avec les États membres, à la gestion opérationnelle du SIS II central :

- **responsabilité des États membres :** chaque État membre sera chargé de mettre en place et d'exploiter son N.SIS II, d'en assurer la maintenance et de le connecter au système central. Les États membres sont responsables de tout dommage causé à une personne du fait de l'exploitation du N.SIS II et devront veiller à une utilisation correcte des données introduites dans le SIS II de sorte que tout échange d'informations contraires à la décision fasse l'objet de sanctions ;
- **responsabilité de l'instance gestionnaire** l'instance gestionnaire assurera, après une période transitoire, les tâches de supervision, de sécurité et de coordination des relations entre les États membres et avec le fournisseur de l'infrastructure de communication

Types de données introduites dans le SIS II :

- **Signalements « pilier I » :** comme le règlement parallèle, la décision prévoit que le SIS II se cantonne à un certain nombre de données strictement spécifiées, fournies par chacun des États membres. Ces données sont celles qui sont nécessaires aux signalements de personnes non-admissibles ou dans une situation d'interdiction de séjour. Les renseignements concernent au maximum les éléments suivants: les nom(s), prénom(s), nom(s) à la naissance, pseudonymes, signes physiques particuliers, le lieu et la date de naissance, le sexe, les photographies, les empreintes digitales, la ou les nationalités, l'indication que la personne concernée est armée, violente ou en fuite, le motif du signalement, l'État membre signalant, une référence à la décision qui est à l'origine du signalement, et le(s) lien(s) vers d'autres signalements introduits dans le SIS II ;
- **Signalements « pilier III » :** outre les ressortissants de pays tiers faisant l'objet d'une interdiction d'entrée ou de séjour concernés par le règlement, la décision prévoit que le SIS II contienne également des signalements concernant : i) des personnes recherchées aux fins de remise ou d'extradition, ii) des personnes disparues (dans l'intérêt de leur propre protection ou pour la prévention de menaces), iii) des personnes recherchées dans le cadre de procédures judiciaires (ex. : témoin d'une affaire, personnes citées à comparaître, ...), iv) des personnes qui font l'objet de surveillance discrète ou d'un contrôle spécifique.

Parallèlement, le SIS II permettra d'échanger des *informations supplémentaires* non stockées dans le SIS mais nécessaires à l'identification d'une personne. Ces informations pourront notamment concerner la conduite à observer vis-à-vis d'une personne signalée. Elles ne pourront être échangées que par des autorités spécifiques appelées « autorités SIRENE » spécifiquement désignées par les États membres. Des *informations complémentaires* pourront également être introduites dans le SIS II sous réserve du consentement des personnes concernées, en vue de mieux vérifier l'identité d'une personne et d'éviter que son identité ne soit usurpée.

Signalements d'objets : la décision prévoit également le signalement d'objets aux fins de saisie ou de preuve dans le cadre d'une procédure pénale : il s'agit des véhicules à moteurs, des embarcations, aéronefs, armes à feu, documents officiels ou d'identité, certificats et plaques d'immatriculation, billets de banque et titres et moyens de paiement. En cas de découverte du signalement, l'autorité doit prendre contact avec l'État membre signalant afin de convenir des mesures à suivre.

Procédure à suivre suite à un signalement : la décision fixe la procédure à suivre en cas de signalement:

- d'une personne recherchée : dans ce cas, l'autorité compétente doit procéder à l'arrestation et à la remise de la personne conformément aux mécanismes du mandat d'arrêt européen, ou procéder à son arrestation provisoire ;
- d'une personne disparue : l'autorité compétente doit communiquer la découverte de la personne en question et si cette dernière accepte une protection, elle pourra être mise en sécurité ;
- d'une personne citée à comparaître : l'autorité compétente devra suivre les informations spécifiques communiquées par les bureaux SIRENE ;
- d'une personne sous le coup d'une mesure de répression pour infraction pénale grave ou recherchée à titre de prévention contre une menace pour la sécurité publique : l'autorité compétente devra procéder à un contrôle soit discret, soit spécifique.

Si une autorité nationale ne peut assurer l'une des mesures ci-avant prévue après un signalement, elle devra dûment en informer l'État membre qui signale l'information.

La décision prévoit également la possibilité pour un État membre d'apposer sur certains signalements un « indicateur de validité » tendant à préciser que la conduite à tenir vis-à-vis des personnes signalées (ex. : arrestation) ne doit pas être exécutée sur son territoire ou que le signalement est incompatible avec son droit ou ses intérêts nationaux.

Évolution du SIS II : lorsque cela sera possible d'un point de vue technique, les empreintes digitales pourront également être utilisées pour identifier un ressortissant d'un pays tiers sur la base de ses identificateurs biométriques. Avant que cette fonctionnalité ne soit introduite dans le SIS II, la Commission devra toutefois présenter un rapport précisant si la technique requise est disponible et prête à être employée.

Accès et conservation des données dans le SIS II : les autorités disposant d'un droit d'accès aux signalements sont celles chargées des contrôles aux frontières, et des autres vérifications de police et de douane effectuées à l'intérieur de l'État membre concerné. Par extension, le droit d'accès peut également être exercé par les autorités judiciaires nationales, dans l'exercice de leurs fonctions. En tous les cas, les utilisateurs ne peuvent accéder qu'aux données qui sont nécessaires à l'accomplissement de leurs missions. Des dispositions sont également prévues pour ouvrir l'accès du SIS II à EUROPOL et EUROJUST.

Les signalements ne sont **conservés** que pendant le temps nécessaire à la réalisation des objectifs pour lesquels ils ont été introduits. Dans les **3 ans** à compter de l'introduction d'un tel signalement dans le SIS II, l'État membre signalant examine la nécessité de le maintenir.

Les signalements relatifs aux objets, introduits aux fins de contrôle discret ou spécifique sont conservés pendant **5 ans**. Les signalements relatifs aux objets, introduits aux fins d'une saisie ou de la preuve dans une procédure pénale, seront automatiquement effacés du SIS II après **10 ans**.

Les données ne peuvent être copiées qu'à des fins techniques. Ces **copies** ne peuvent être conservées que pour une durée inférieure à **48 heures**.

Règles générales à observer en matière de traitement des données : la décision fixe les règles applicables en matière i) de qualité, d'exactitude et de licéité des données introduites dans le SIS, ii) de

modification, rectification, tenue à jour et effacement des données introduites, iii) de mise en relation des signalements introduits dans le SIS II, opérée par un État membre vers une autre autorité responsable lorsque cela répond à un besoin opérationnel manifeste, iv) de conduite à tenir en cas d'erreur ou d'usurpation d'identité avec une personne signalée dans le SIS.

À noter que les données traitées dans le SIS II ne peuvent être transférées à des pays tiers ou à des organisations internationales, ni mises à leur disposition. Des mesures sont toutefois prévues pour renforcer la coopération avec Interpol.

Protection des données : des dispositions très strictes sont prévues en matière de protection des données afin de clairement limiter et encadrer l'utilisation et le traitement des données à la mission du SIS II. Seules sont autorisées à introduire et à consulter les informations pertinentes du SIS, les autorités strictement identifiées à la décision et selon les modalités prévues. Le traitement des catégories de données « sensibles » est interdit. Toute personne peut accéder aux données la concernant et a le droit de faire rectifier ses données si elles sont inexactes ou stockées illégalement. Elle peut également intentier une action devant les juridictions compétentes pour faire respecter sa décision de rectification ou d'effacement de ses données.

Toutes les autorités responsables dans le cadre de la gestion et de l'introduction des données doivent respecter les principes des textes pertinents en matière de protection des données (en particulier, le règlement 45/2001/CE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel). Pour sa part, le contrôleur européen des données sera chargé de vérifier la légalité du traitement des données par l'instance gestionnaire.

Des sanctions sont prévues en cas d'utilisation frauduleuse du SIS par toute autorité responsable.

Période transitoire : pendant une période transitoire, la Commission sera chargée de la gestion du SIS avant la mise en place de l'instance gestionnaire qui sera chargée des tâches de gestion opérationnelle, organisationnelle et financière du SIS II. Elle pourra néanmoins assurer une transition en douceur vers le SIS II en déléguant les responsabilités à des organismes publics nationaux. La période transitoire ne devra pas dépasser 5 ans à compter de l'entrée en vigueur de la décision.

Durant la période transitoire, les signalements sont transférés du SIS 1+ (version révisée du SIS de 1^{ère} génération) au SIS II. Le SIS II s'applique aux États membres participant au SIS 1+ à compter des dates à arrêter par le Conseil. Trois ans après la mise en service du SIS II (puis tous les 4 ans), la Commission présentera un rapport d'évaluation globale du SIS II et transmettra ce rapport au Parlement européen et au Conseil.

Dispositions territoriales : la décision s'applique au Royaume-Uni et à l'Irlande conformément aux dispositions pertinentes du traité. Sont également associés à la décision, conformément à des accords conclus bilatéralement avec ces pays, la Suisse, la Norvège et l'Islande.

ENTRÉE EN VIGUEUR : 27 août 2007.