

SCHENGEN

SYSTÈME D'INFORMATION SCHENGEN GUIDE POUR L'EXERCICE DU DROIT D'ACCES

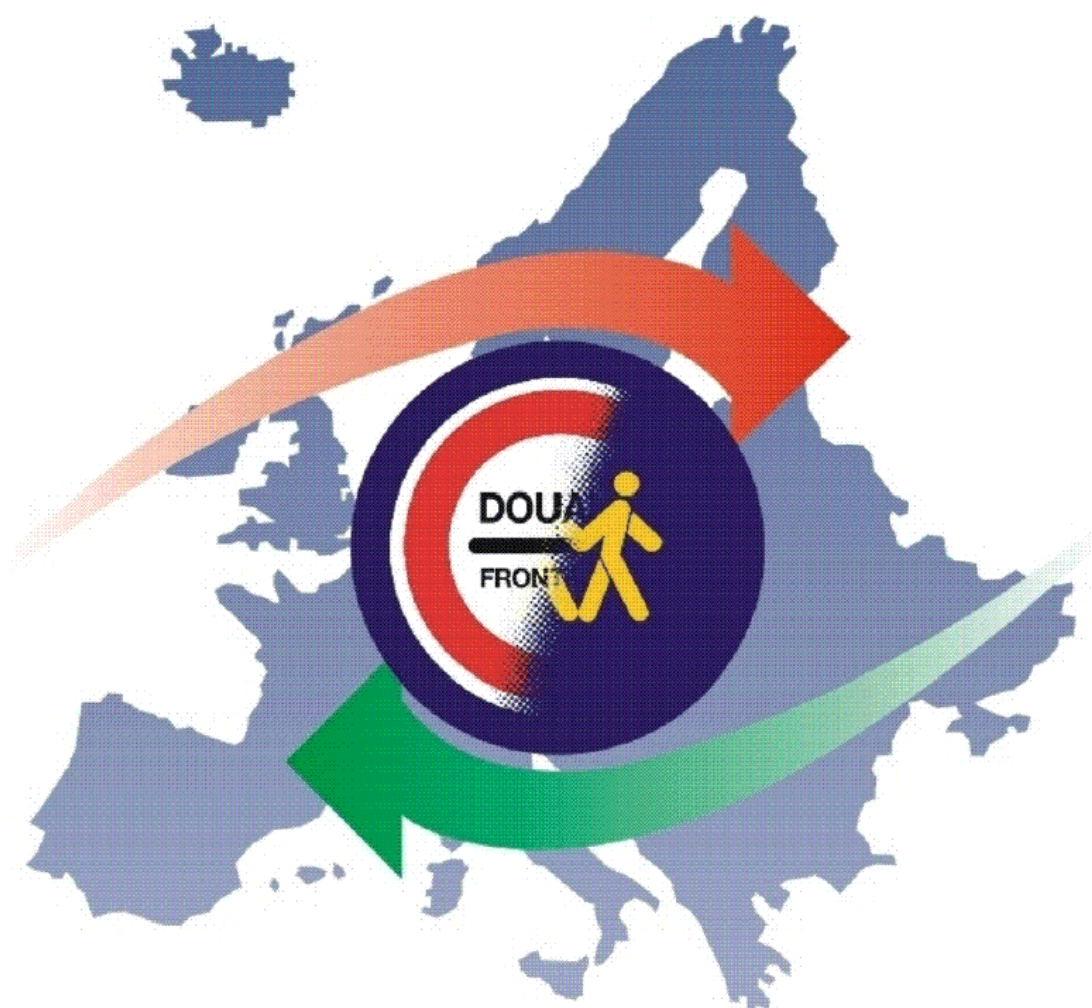


TABLE DES MATIÈRES

I.	Rappel des principes généraux	3
II.	Description de la procédure de droit d'accès dans chacun des pays de l'espace Schengen	5
III.	Situations particulières nécessitant une procédure spécifique	6
IV.	Autriche	11
V.	Belgique	16
VI.	Danemark	18
VII.	Finlande	21
VIII.	France	23
IX.	Allemagne	27
X.	Grèce	29
XI.	Islande	32
XII.	Italie	35
XIII.	Luxembourg	37
XIV.	Pays-Bas	39
XV.	Norvège	41
XVI.	Portugal	43
XVII.	Espagne	44
XVIII.	Suède	46

Ce mémento a pour objet de décrire les modalités d'exercice du droit d'accès au système d'information Schengen (SIS).

Destiné principalement aux personnes confrontées à titre professionnel à l'exercice du droit d'accès (autorités de protection des données, services de police, services des étrangers, avocats, etc.), ce document se veut un outil pratique, pouvant également être consulté par toute personne intéressée par cette question.

Ce mémento comporte trois volets: un rappel des principes généraux et des définitions essentielles concernant le SIS, une description de la procédure d'exercice du droit d'accès dans chacun des pays concernés et, enfin, une présentation de quelques situations particulières nécessitant une procédure spécifique.

I. Rappel des principes généraux

I.A Le système d'information Schengen (SIS)

L'accord de Schengen du 14 juin 1985 et sa convention d'application du 19 juin 1990 ont créé un espace de libre circulation des personnes en supprimant les contrôles aux frontières intérieures des États membres et en instaurant le principe d'un contrôle d'entrée sur le territoire Schengen unique.

Pour maintenir un niveau de sécurité satisfaisant, il est apparu nécessaire, entre autres mesures (renforcement de la coopération policière et judiciaire, harmonisation des politiques de visa et d'asile), de créer le système d'information Schengen (SIS).

Le SIS est un fichier commun à l'ensemble des États membres de l'espace Schengen. Il centralise deux grandes catégories d'informations concernant, l'une, des personnes recherchées ou disparues et des personnes placées sous surveillance, l'autre, des véhicules et des objets recherchés tels que, notamment, des documents d'identité.

Par exemple, peuvent être fichées dans le système d'information Schengen:

- les personnes recherchées ou surveillées par les services de police,
- les personnes disparues ou qui doivent être placées sous protection, en particulier les mineurs,
- les personnes, non ressortissantes d'un État membre de l'espace Schengen, qui sont interdites d'entrée sur le territoire Schengen.

L'exécution d'une demande est soumise au droit national de l'État Schengen qui procède à l'exécution. Si la mesure ne peut pas être exécutée conformément au droit national, l'État Schengen requis en informe sans délai l'État Schengen signalant.

En application des principes de la protection des données, des droits particuliers sont reconnus par la convention Schengen aux personnes, qu'elles soient ou non ressortissantes d'un État membre de l'espace Schengen.

Il s'agit essentiellement:

- d'un droit d'accès aux informations les concernant, enregistrées dans le SIS,
- d'un droit de rectification lorsque les données sont enregistrées sur la base d'une erreur de droit ou de fait,
- du droit d'engager une action devant les juridictions ou les instances compétentes pour obtenir la rectification ou l'effacement des informations erronées, ou une indemnisation.

I.B Le droit d'accès:

Le droit d'accès est la possibilité pour toute personne qui le demande d'accéder aux informations la concernant enregistrées dans un fichier tel que visé dans le droit national. Il s'agit d'un principe fondamental de protection des données, qui permet aux personnes concernées d'exercer un contrôle sur les données à caractère personnel détenues par des tiers.

Ce droit est expressément prévu par la convention d'application de l'accord de Schengen du 19 juin 1990. Aux termes de l'article 109 de la convention, toute personne a le droit d'accéder aux données la concernant enregistrées dans le système d'information Schengen (SIS). Ce droit est complété par un droit de rectification, lorsque les données sont entachées d'erreur de fait, et par un droit d'effacement, lorsque les données sont entachées d'erreur de droit (article 110).

Le droit d'accès est refusé s'il peut nuire à l'exécution de la tâche légale consignée dans le signalement, ou pour la protection des droits et libertés d'autrui. Il est refusé dans tous les cas durant la période de signalement aux fins de surveillance discrète. (Article 109, paragraphe 2, de la convention).

Toute personne qui exerce son droit d'accès peut s'adresser aux autorités compétentes du pays Schengen ¹ de son choix. Cette faculté de choix résulte de ce que chacune des bases nationales (N-SIS) est identique au système central (C-SIS), installé à Strasbourg (cf. Article 92, paragraphe 2, de la convention). Le droit d'accès porte donc sur des données identiques, quel que soit l'État auprès duquel la demande est formée.

Cependant, le droit d'accès s'exerce conformément au droit national de l'État saisi. Or, les règles de procédures applicables diffèrent d'un pays à l'autre, dans la mesure où deux régimes de droit d'accès aux fichiers de police - et donc, au SIS - sont actuellement en vigueur. Dans certains pays, le droit d'accès est direct, dans d'autres, le droit d'accès est indirect.

Toute personne qui le souhaite peut obtenir des informations sur le système de droit d'accès et de rectification applicable auprès de l'autorité nationale de protection des données des différents États Schengen.

I.B.1 Le droit d'accès direct

Dans ce cas, la personne adresse sa demande de droit d'accès directement aux autorités gestionnaires des données (services de police, de gendarmerie, de douanes, etc.). Si le droit national le prévoit, le demandeur peut se voir communiquer les informations qui le concernent.

I.B.2 Le droit d'accès indirect

Dans ce cas, la personne adresse sa demande de droit d'accès à l'autorité nationale de protection des données de l'État auprès duquel elle forme sa demande. La vérification des informations enregistrées dans le SIS est effectuée, par l'autorité de protection des données, de la même façon que pour les fichiers de police qui intéressent la sûreté de l'État, la défense ou la sécurité publique.

¹ Belgique, Pays-Bas, Luxembourg, France, Allemagne, Italie, Portugal, Espagne, Autriche, Grèce, Danemark, Suède, Finlande, Norvège et Islande (situation au 1^{er} juin 2001).

Les modalités de communication des données sont différentes selon le pays concerné (cf. infra), et peuvent dans certains cas être extrêmement limitées.

I.C Le principe de la rectification ou de l'effacement des données

Aux termes de la convention Schengen, seul l'État à l'origine d'un signalement enregistré dans le SIS peut le modifier ou l'effacer (article 106).

Lorsqu'un pays de droit d'accès direct est saisi d'une demande de droit d'accès pour un signalement qu'il n'a pas lui-même effectué, cet État doit donner au pays signalant l'occasion de prendre position quant à la possibilité de communiquer les données au demandeur.

Lorsqu'il s'agit d'un pays de droit d'accès indirect, une coopération doit s'instaurer entre autorités nationales de protection des données, sur la base de l'article 114, paragraphe 2, de la convention Schengen (cf. infra).

II. Description de la procédure de droit d'accès dans chacun des pays de l'espace Schengen

La procédure à suivre dans chaque pays appliquant l'acquis de Schengen pour exercer son droit d'accès est indiquée dans les fiches nationales figurant aux chapitres IV à XVIII.

III. Situations particulières nécessitant une procédure spécifique

III.A La coopération entre autorités nationales de protection des données

Lorsqu'une personne adresse une demande de droit d'accès aux données la concernant à l'autorité nationale de protection des données de l'un des États membres de l'espace Schengen et qu'il apparaît, lors de la vérification, que les données ont été introduites par un autre État Schengen, une coopération étroite doit s'instaurer entre les autorités de contrôle des deux États concernés: celui auprès duquel la demande d'accès est introduite et celui qui est à l'origine du signalement.

Compte tenu du nombre élevé de demandes de droit d'accès impliquant plusieurs États et des conséquences que peut avoir un signalement dans le SIS au regard des libertés individuelles, en particulier de la liberté d'aller et venir, une coopération efficace et rapide entre autorités de contrôle s'impose. Les principes suivants devraient s'appliquer dans le respect des législations nationales:

- L'autorité de contrôle nationale saisie d'une demande de droit d'accès doit, lorsque les données à caractère personnel ont été introduites par un autre État, agir en étroite coopération avec l'autorité de contrôle nationale de cet autre État .
En aucun cas, une demande de coopération ne dessaisit l'autorité de contrôle initialement saisie.
- L'autorité de contrôle initialement saisie fournit à l'autorité requise tous les éléments en sa possession utiles à l'exercice des vérifications. L'autorité de contrôle nationale requise procède avec diligence aux vérifications qui lui sont demandées.

En particulier, l'autorité de contrôle vérifie le bien-fondé du signalement dans le SIS, ce qui nécessite parfois d'étendre les vérifications aux données enregistrées dans des fichiers nationaux.

- Une priorité particulière doit être accordée au traitement de ces demandes, afin de ne pas prolonger excessivement le délai de réponse au demandeur.

Si le demandeur est, en vertu du droit national applicable, en mesure d'exercer son droit d'accès directement auprès des autorités gestionnaires des fichiers nationaux, cette possibilité doit lui être communiquée dans les meilleurs délais.

- À l'issue des vérifications, l'autorité de contrôle requise transmet à l'autorité de contrôle initialement saisie l'ensemble des informations recueillies au cours de ses investigations et émet un avis. Lorsqu'elle communique son avis à l'autorité de contrôle nationale requérante, l'autorité de contrôle nationale lui précise les implications de sa législation nationale pour le droit d'accès. Elle peut indiquer quelle serait la décision prise sur la demande d'accès en vertu de son droit national. Elle indique, s'il s'agit d'une autorité de droit d'accès direct, alors que l'autorité requérante est de droit d'accès indirect, si elle est d'accord pour transmettre au demandeur les informations en question.

III.B L'enregistrement des alias

Il arrive fréquemment qu'une personne dont l'identité a été usurpée (par exemple, à la suite du vol et de l'utilisation de ses documents d'identité par un tiers) soit signalée dans le SIS. En effet, on enregistre la personne réellement recherchée sous les différentes identités qu'elle est susceptible d'utiliser.

Le signalement dans le SIS de personnes dont l'identité est usurpée pose de sérieux problèmes juridiques et pratiques.

Le SIS contient un signalement assorti d'une identité qui ne correspond ni en droit ni en fait à une personne répondant aux critères prévus par les articles 95 à 100 de la convention Schengen. Ce signalement se heurte aux principes de pertinence et d'exactitude des données, essentiels en matière de protection des données.

En outre, l'expérience des autorités de contrôle nationales montre que les personnes dont l'identité est usurpée peuvent se retrouver dans une situation extrêmement désavantageuse et éprouver de grandes difficultés à faire valoir leurs droits.

Face à cette situation, l'autorité de contrôle commune (ACC Schengen) a émis deux avis (avis 98/2 du 3 février 1998 et avis complémentaire du 15 février 2000) dans lesquels elle souligne l'importance du respect des principes de protection des données figurant dans la convention, et où elle préconise l'adoption d'une solution technique dans le cadre du SIS I+ et du SIS II.

Sans préjudice des solutions techniques envisagées à plus long terme, les principes qui figurent ci-après devraient être appliqués lors du traitement des demandes de droit d'accès présentées par des personnes victimes d'une usurpation d'identité.

- Compte tenu de l'obligation qui pèse sur les États participant au SIS de garantir que les données enregistrées sont exactes et mises à jour, le stockage du signalement de personnes dont l'identité a été usurpée ne peut être admis que de manière très restrictive, c'est-à-dire uniquement dans les cas dont la gravité justifie le traitement de ces données et dans les conditions visées aux articles 95 à 100.
Il faut en effet mettre en balance les droits de la personne victime de l'usurpation d'identité - en particulier le droit de demander l'effacement d'un signalement qui lui porte préjudice - et le risque qu'entraînerait l'effacement de ce signalement.
- Lorsque la personne dont l'identité a été usurpée exerce son droit d'accès aux données, l'État signalant devrait accéder à une demande de "désignalement" avec la plus grande célérité dans la majorité des cas, en particulier lorsque le signalement a été effectué sur la base de l'article 96 et non de l'article 95, par exemple.
- Enfin, il peut arriver qu'une personne, dont l'identité est enregistrée dans le SIS en tant que "identité établie", soutienne que son nom a été usurpé et utilisé à des fins frauduleuses. Cette situation délicate peut se produire lorsque l'auteur du délit a été interpellé et s'est présenté sous l'identité de la victime de l'usurpation d'identité. L'ACC Schengen considère que, dans ce cas, la personne qui estime être victime d'une usurpation d'identité doit être en mesure de prouver par tout moyen qu'elle n'est pas l'auteur des faits qui lui sont reprochés et de faire valoir ses droits.

III.C Le signalement d'un étranger titulaire d'un titre de séjour délivré par un État membre

L'article 25, paragraphe 2, de la convention Schengen prévoit dans ce cas la procédure suivante:

"Lorsqu'il apparaît qu'un étranger titulaire d'un titre de séjour en cours de validité délivré par l'une des parties contractantes est signalé aux fins de non-admission, la partie contractante signalante consulte la partie qui a délivré le titre de séjour afin de déterminer s'il y a des motifs suffisants pour retirer le titre de séjour.

Si le titre de séjour n'est pas retiré, la partie contractante signalante procède au retrait du signalement, mais peut cependant inscrire cet étranger sur sa liste nationale de signalement".

Or, il peut arriver qu'un ressortissant étranger soit signalé par un État membre de l'espace Schengen dans le SIS sur la base de l'article 96 de la convention Schengen, alors qu'il réside régulièrement dans un autre État membre.

Cette situation paraît illogique, une personne résidant sur le territoire d'un État membre de l'espace Schengen ne pouvant être, au même moment, enregistrée dans le SIS en tant que personne "indésirable" dans l'espace Schengen.

Dans ces circonstances, il est important que toute autorité de protection des données vérifie, lorsqu'elle découvre que la personne qui exerce son droit d'accès au SIS se trouve dans la situation décrite ci-dessus, le respect de la procédure prévue à l'article 25, paragraphe 2, de la convention Schengen, qui conduit dans la plupart des cas au "désignalement" de la personne concernée. En effet, si le pays signalant estime qu'il n'y a pas lieu de retirer le titre de séjour régulièrement délivré, le "désignalement" du SIS doit être automatique. La convention ne laisse aucune appréciation sur ce point à l'État signalant.

L'étude effectuée sur cette question par l'ACC a révélé que cette procédure n'est pas systématiquement mise en œuvre et qu'elle peut s'avérer très longue pour la personne concernée. Il semble en outre que les États membres pensent disposer de la faculté d'apprécier la nécessité d'effacer un signalement sur la base de l'article 25, paragraphe 2, de la convention Schengen.

Au vu de ces constats, les autorités de protection des données devraient appliquer les principes suivants:

- vérifier si la personne signalée dans le SIS se trouve en possession d'un titre de séjour en cours de validité délivré par un des États membres de l'espace Schengen,
- dans cette hypothèse, rappeler aux autorités concernées le caractère automatique du "désignalement" (sauf exception) et insister pour que l'effacement des données dans le SIS intervienne rapidement.

IV. AUTRICHE

1. Nature du droit d'accès (direct, indirect ou mixte)

En Autriche, le droit d'accès aux données à caractère personnel est en principe un droit de contrôle direct; en d'autres termes, les demandes d'information doivent être adressées au responsable du traitement des données (« Auftraggeber » dans la terminologie autrichienne), qui y répond personnellement. Cette règle s'applique de manière générale en vertu de la loi autrichienne en matière de protection des données, et s'appliquerait également plus spécialement aux informations relatives aux signalements des articles 95 à 100 de la convention conservés dans le SIS.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Une demande d'information doit être adressée à l'autorité policière (en tant que responsable du traitement des données) dont l'intéressé veut savoir si elle traite des données le concernant.

3. Formalisme de la demande: informations et documents à fournir – coût éventuel

Conformément à l'article 26 de la loi en matière de protection des données (Datenschutzgesetz ou DSG) de 2000, le responsable du traitement des données doit informer l'intéressé lorsque:

- celui-ci forme une demande écrite (la demande peut également être faite oralement avec l'accord du responsable);
- il apporte de manière appropriée la preuve de son identité.

L'information doit comprendre:

- les données traitées,
- les informations disponibles sur leur origine,
- les destinataires ou groupes de destinataires éventuels des données transmises,
- la finalité de l'utilisation des données,
- la base juridique sous une forme généralement compréhensible,
- de plus, sur demande de l'intéressé, le nom et l'adresse des prestataires chargés de traiter les données le concernant.

L'information n'a pas à être communiquée lorsque:

- la protection de l'intéressé l'exige pour des raisons particulières,
- l'intérêt légitime prédominant du responsable du traitement des données ou d'un tiers s'y oppose,
- l'intérêt public prédominant s'y oppose parce qu'il est, par exemple, nécessaire:
 - de protéger les institutions constitutionnelles de la République d'Autriche, ou
 - de garantir la disponibilité opérationnelle de l'armée fédérale, ou
 - de protéger les intérêts de la défense globale du pays, ou
 - de protéger des intérêts importants de la République d'Autriche ou de l'Union européenne dans les domaines de la politique étrangère, de l'économie ou des finances, ou
 - de prévenir, empêcher ou poursuivre des infractions.

Si la protection de l'intérêt public impose un refus de communiquer les informations lors de l'exécution, il convient d'indiquer dans tous les cas où aucune information n'est fournie (même si aucune donnée n'est effectivement utilisée) que "aucune donnée concernant l'intéressé dont la communication est obligatoire n'est utilisée" (paragraphe 5).

Ce refus est soumis au contrôle de la Commission pour la protection des données (*Datenschutzkommission*) et peut faire l'objet d'une procédure de recours spécifique.

Il peut être renoncé à communiquer l'information si l'intéressé ne participe pas à la procédure ou s'il ne verse pas l'indemnisation fixée.

L'intéressé doit participer à la procédure sur demande.

Le responsable du traitement des données doit communiquer les informations dans un délai de huit semaines ou justifier par écrit un refus total ou partiel de les communiquer.

L'information est gratuite si elle concerne un fichier actuel et si l'intéressé n'a pas encore formé la même demande pendant l'année en cours.

Dans tous les autres cas, une indemnisation forfaitaire de 260 ATS peut être demandée. Si l'information a donné lieu à une rectification, l'indemnisation doit être remboursée.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Datenschutzkommission (Commission pour la protection des données)

Ballhausplatz 1,

A -1014 Vienne,

Tél.: ++43 1 531 15/2525,

Fax:++43 1 531 15/2690,

E-mail: v3post@bka.gv.at

Si, à l'expiration du délai de huit semaines, l'autorité policière n'a pas fourni de réponse, ou si l'intéressé est informé qu'aucune donnée dont la communication est obligatoire n'a été traitée, il peut faire appel à la Commission pour la protection des données conformément à l'article 31, paragraphes 1 et/ou 4, de la DSG de 2000.

Si, dans le cadre d'une procédure de recours en vertu de l'article 31, paragraphe 4, de la DSG de 2000, le responsable du traitement des données invoque la confidentialité pour des raisons d'intérêt public prédominant, la Commission pour la protection des données doit vérifier que la confidentialité est nécessaire et notifier la divulgation des données lorsqu'elle n'est pas justifiée par rapport à l'intéressé.

L'autorité peut contester cette notification devant le tribunal administratif. En l'absence de recours, elle doit donner suite à la notification de la Commission pour la protection des données dans un délai de huit semaines; dans le cas contraire, la Commission peut divulguer elle-même les données à l'intéressé.

5. Références des principaux textes nationaux applicables

Article 26 de la loi en matière de protection des données de 2000 (DSG 2000),

BGBI.(Journal Officiel) I, n° 165/1999.

Art. 26 (1) Le responsable du traitement des données doit informer l'intéressé des données traitées le concernant lorsque ce dernier forme une demande écrite et apporte de manière appropriée la preuve de son identité. La demande peut également être faite oralement avec l'accord du responsable. L'information doit comprendre sous une forme généralement compréhensible les données traitées, les informations disponibles sur leur origine, les destinataires ou groupes de destinataires éventuels des données transmises, la finalité de l'utilisation des données et les bases juridiques correspondantes. Sur demande de l'intéressé, elle doit également comprendre le nom et l'adresse des prestataires chargés de traiter les données le concernant. Si l'intéressé ne s'y oppose pas, l'information écrite peut être remplacée par une information orale avec possibilité de prendre connaissance des données et d'en faire une copie ou une photocopie.

(2) L'information ne doit pas être communiquée lorsque la protection de l'intéressé l'exige pour des raisons particulières ou lorsque l'intérêt légitime prédominant du responsable du traitement des données ou d'un tiers, et notamment l'intérêt public prédominant, s'y oppose. L'intérêt public prédominant peut résulter de la nécessité:

1. de protéger les institutions constitutionnelles de la République d'Autriche, ou
2. de garantir la disponibilité opérationnelle de l'armée fédérale, ou
3. de protéger les intérêts de la défense globale du pays, ou
4. de protéger des intérêts importants de la République d'Autriche ou de l'Union européenne dans les domaines de la politique étrangère, de l'économie ou des finances, ou
5. de prévenir, empêcher ou poursuivre des infractions.

La recevabilité du refus de communiquer les informations pour les motifs indiqués aux points 1 à 5 est soumise au contrôle de la Commission pour la protection des données conformément à l'article 30, paragraphe 3, et peut faire l'objet d'une procédure de recours spécifique devant cette Commission conformément à l'article 31, paragraphe 4.

(3) L'intéressé doit participer à la procédure sur demande dans des limites raisonnables afin d'éviter au responsable du traitement des données tout travail injustifié et disproportionné.

(4) La demande doit être satisfaite dans un délai de huit semaines à compter de sa réception; si elle a été rejetée totalement ou partiellement, l'intéressé doit être informé par écrit du motif du rejet. Il peut aussi être renoncé à communiquer l'information si l'intéressé n'a pas participé à la procédure conformément au paragraphe 3 ou s'il n'a pas versé l'indemnisation fixée.

(5) Lors de la phase d'exécution, pour ce qui est des tâches visées au paragraphe 2, points 1 à 5, il convient de procéder comme suit lorsque la protection de l'intérêt public motive un refus de communiquer l'information. Dans tous les cas où aucune information n'est fournie, et donc également parce qu'aucune donnée n'est effectivement utilisée, la justification quant au fond sera remplacée par une indication selon laquelle aucune donnée concernant l'intéressé dont la communication est obligatoire n'est utilisée. La recevabilité de cette procédure est soumise au contrôle de la Commission pour la protection des données conformément à l'article 30, paragraphe 3, et peut faire l'objet d'une procédure de recours spécifique devant cette Commission conformément à l'article 31, paragraphe 4.

(6) L'information doit être communiquée gratuitement si elle concerne le contenu actuel d'un fichier et si l'intéressé n'a pas encore fait de demande d'information au cours de l'année dans le même domaine d'activités. Dans tous les autres cas, une indemnisation forfaitaire de 260 ATS peut

être demandée et ce montant peut être augmenté si les frais réels sont plus élevés. L'indemnisation versée doit être remboursée sans préjudice de demandes de dédommagement éventuelles si des données ont été manipulées illégalement ou si l'information a donné lieu à une rectification.

(7) Dès qu'il a connaissance d'une demande d'information, le responsable du traitement des données n'est pas autorisé à détruire les données concernant l'intéressé pendant une période de quatre mois et, en cas de recours devant la Commission pour la protection des données conformément à l'article 31, avant la conclusion définitive de la procédure.

(8) Lorsque la loi autorise le public à prendre connaissance de fichiers de données, l'intéressé peut demander à être informé de l'étendue du droit de consultation. La procédure de consultation est régie par les dispositions spécifiques des lois instituant le livre ou le registre public.

(9) Les informations provenant du casier judiciaire sont régies par les dispositions particulières de la loi sur le casier judiciaire de 1968 relatives aux extraits de casier judiciaire.

(10) Lorsqu'un contractant décide de son propre chef, en vertu des dispositions législatives, des règles déontologiques ou des règles de conduite visées à l'article 6, paragraphe 4, d'utiliser une demande de données conformément à l'article 4, point 4, troisième phrase, l'intéressé peut également adresser d'abord sa demande d'information à la personne qui a fait élaborer la demande. Cette dernière doit lui communiquer gratuitement, s'ils ne sont pas encore connus, le nom et l'adresse du contractant dans un délai de deux semaines, afin que l'intéressé puisse exercer son droit d'accès conformément au paragraphe 1.

V. BELGIQUE

1. Nature du droit d'accès

Toute personne bénéficie d'un droit d'accès indirect aux données à caractère personnel la concernant traitées par les services de police. Pour exercer ce droit, elle adresse une demande à la Commission de la protection de la vie privée.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Commission de la protection de la vie privée

Boulevard de Waterloo, 115,

B-1000 Bruxelles

Tél: ++32-(0)2 542 72 00

Fax: ++32 (0)2 542 72 01

E-mail: commission@privacy.fgov.be

Internet: www.privacy.fgov.be

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

La demande est introduite auprès de la Commission par courrier daté et signé. Elle contient les nom et prénom, la date de naissance et la nationalité de la personne concernée ainsi qu'une photocopie de son document d'identité.

La demande contient également, *dans la mesure où le demandeur dispose de ces informations*, la désignation de l'autorité ou du service concerné de même que tous les éléments pertinents relatifs aux données contestées - nature, circonstances, origine de la prise de connaissance des données contestées et rectifications éventuellement souhaitées.

La procédure est gratuite.

4. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

Lorsqu'elle reçoit une demande d'accès indirect aux données à caractère personnel traitées par un service de police, la Commission procède aux vérifications nécessaires auprès du service concerné. À l'issue du contrôle, elle informe la personne concernée que ces vérifications ont été effectuées. Le cas échéant, en cas de traitements de données gérés par un service de police en vue de contrôles d'identité et après avis du service concerné, la Commission fournit à la personne toute autre information qu'elle estime appropriée.

5. Références des principaux textes nationaux applicables

- La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel, modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995, en particulier son article 13;
- L'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier ses articles 36 à 46.

VI. DANEMARK

1. Nature du droit d'accès

La personne concernée a un droit d'accès direct.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Les demandes de droit d'accès sont à adresser à la police nationale qui est le responsable du traitement:

Rigspolitiet
Polititorvet 14
DK-1488 Copenhagen V
Tél.: ++45 3314 8888

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

Il n'existe pas d'exigences particulières concernant le formalisme de la demande.

Il importe de répondre dans les meilleurs délais à une demande de droit d'accès; si le délai excède exceptionnellement une période de 4 semaines, le responsable du traitement doit en informer la personne concernée. Cette notification indique le motif pour lequel il ne peut pas être pris de décision avant l'écoulement du délai de 4 semaines ainsi que la date à laquelle la décision est susceptible d'être prise.

D'une manière générale, le droit d'accès est accordé par écrit si la personne concernée le demande. Dans les cas où la personne concernée se présente en personne auprès du responsable du traitement, il convient de déterminer si la personne concernée souhaite une réponse écrite ou une communication verbale des données.

Les demandes de droit d'accès sont gratuites.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Datatilsynet (Inspection des données)

Borgergade 28, 5. sal

DK - 1300 Copenhagen K

Tél: +45 3319 3200

Fax: ++45 3319 3218

E-mail: dt@datatilsynet.dk

Internet: www.datatilsynet.dk

Les réclamations peuvent être adressées à l'autorité de protection des données concernant la décision prise par la police nationale en matière d'accès. En traitant les réclamations, l'autorité de protection des données examine les éléments du dossier en vue de s'assurer qu'aucune donnée n'a été introduite d'une manière qui est incompatible avec les règles de la convention de Schengen.

5. Résultats à attendre de la demande d'accès. Contenu de la communication

Conformément à l'article 31, paragraphe 1 de la loi sur la protection des données à caractère personnel, le responsable du traitement (dans le cas présent la police nationale) doit informer toute personne qui lui a adressé une demande si des données la concernant ont été traitées. Lorsque des données de ce type sont traitées, la communication qui est adressée à l'intéressé doit faire apparaître clairement de quelles données il s'agit, l'objet du traitement, les catégories de destinataires des données et toute information disponible sur la provenance des données.

Conformément à l'article 31, paragraphe 1 en association avec l'article 30, paragraphe 2 de la loi, ces dispositions ne sont pas d'application si des motifs d'intérêt public impérieux priment par rapport à l'intérêt manifesté par la personne concernée à obtenir cette information, notamment:

- (1) la sécurité nationale
- (2)
- (3) la sécurité publique
- (4) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements au code de déontologie de professions libérales réglementées.
- (5)
- (6)

Conformément à l'article 95 et aux articles 98 à 100 de la convention de Schengen, l'introduction d'informations dans le Système d'information Schengen est réalisée aux fins de l'arrestation des personnes recherchées, la présentation des personnes citées à comparaître, la notification d'un jugement répressif ou d'une citation à comparaître, d'une surveillance discrète ou d'un contrôle spécifique de personnes et de véhicules ainsi que de la découverte d'objets aux fins de saisie ou de preuves dans une procédure pénale.

Eu égard à ces objectifs, dans certains cas la personne concernée ne devra pas être mise au courant que des informations ont été introduites à son sujet au titre de l'article 95 et des articles 98 à 100 de la convention, faute de quoi cette personne aurait la possibilité de prendre des dispositions susceptibles de porter gravement atteinte aux mesures à mettre en œuvre dans le cadre du signalement (cf. à cet égard l'article 109, paragraphe 2, de la convention de Schengen).

6. Références des principaux textes nationaux applicables

Loi n° 429 du 31 mai 2000 sur le traitement des données à caractère personnel.

VII. FINLANDE

1. Nature du droit d'accès

Le fichier de données Schengen est la partie nationale visée à l'article 92, paragraphe 2, de la convention d'application de l'accord de Schengen (article 3, point b) 1), de la loi relative aux registres policiers des personnes). La Direction générale de la police est propriétaire du fichier et le service central de la police judiciaire en est le gestionnaire, sous la supervision de la Direction générale de la police (article 5 de la loi précitée).

Les demandes de vérification de données sont adressées directement à l'autorité qui gère ces données, à savoir la police.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Les demandes relatives au droit de vérification peuvent être adressées à la Direction générale de la police, au service central de la police judiciaire ou au commissariat de police du district.

Coordonnées du service central de la police judiciaire:

Jokiniemenkuja 4

PL 285

FIN -01301 Vantaa

Tél.: ++358 (09) 8388 661

Fax:

E-mail:

Internet:

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

Les demandes doivent être introduites auprès de la police par les intéressés eux-mêmes, qui doivent apporter la preuve de leur identité.

L'exercice du droit de vérification n'est soumis au paiement d'un droit que s'il ne s'est pas encore écoulé un an depuis la dernière fois que l'intéressé a exercé ce droit (article 16 de la loi sur les registres policiers).

Le gestionnaire du fichier doit, dans un délai raisonnable, donner aux personnes y figurant la possibilité de consulter les informations qui y sont contenues et fournir ces informations lorsqu'une demande par écrit lui a été adressée à cet effet (article 28 de la loi relative aux données à caractère personnel).

Les décisions relatives à la divulgation d'informations sont prises par le service central de la police judiciaire.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Albertinkatu 25 A
PL 315,
FIN - 00181 Helsinki
Tél.: ++358 (9) 18 251
Fax: ++358 (9) 1825 7835
E-mail: tietosuoja@om.fi
Internet: www.tietosuoja.fi

Si le service central de la police judiciaire, gestionnaire du fichier, refuse d'accorder un droit d'accès aux données du SIS en se fondant sur l'article 27 de la loi relative aux données à caractère personnel, un certificat attestant cette décision doit être délivré et il doit être suggéré à la personne figurant dans le fichier de s'adresser à l'autorité compétente en matière de protection des données. Cette personne peut ensuite saisir cette autorité.

L'autorité compétente en matière de protection des données prend des décisions contraignantes en matière de droit de vérification des données. Il est possible d'introduire des recours contre les décisions de l'autorité auprès du tribunal administratif compétent et, ultérieurement, auprès de la Cour administrative suprême (articles 28 et 29 de la loi relative aux données à caractère personnel).

VIII. FRANCE

1. Nature du droit d'accès

Le droit d'accès est mixte.

Il est direct lorsque les personnes enregistrées dans le SIS sont:

- des personnes recherchées dans l'intérêt des familles (article 97 de la convention),
- des mineurs faisant l'objet d'une opposition à sortie du territoire (article 97),
- des mineurs fugueurs (article 97),
- des personnes mentionnées ou identifiables à l'occasion du signalement d'un véhicule volé (article 100).

Dans tous les autres cas, le droit d'accès au SIS est indirect. Conformément à l'article 39 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés désignera l'un de ses membres, magistrat ou ancien magistrat, appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Si la demande concerne un des quatre cas de figure pour lesquels le droit d'accès est direct, elle doit être adressée directement à la

Direction générale de la police nationale

Ministère de l'intérieur

11, rue des Saussaies

F-75008 Paris

Tél.: +33(0)1.49.27.49.27

Fax: ---

E-mail: ---

Internet: www.interieur.gouv.fr

Dans les autres cas, la demande d'accès doit être adressée à la

Commission nationale de l'informatique et des libertés

21, rue Saint-Guillaume

F-75340 Paris Cedex 07

Tél.: ++33 1 53 73 22 22

Fax: ++33 1 53 73 22 00

E-mail: ffourets@cnil.fr

Internet: www.cnil.fr

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

L'exercice du droit d'accès est strictement personnel. La demande doit être présentée par l'intéressé lui-même (en aucun cas par un membre de sa famille), ou par l'avocat qu'il aura mandaté.

Aucun formalisme particulier n'est exigé. Toutefois, le demandeur doit indiquer ses nom, prénom, date et lieu de naissance, et joindre à son courrier la photocopie lisible d'un document attestant son identité. En outre, une copie de tout document utile (notification d'un refus de visa fondé sur un signalement dans le SIS, décision de justice favorable au demandeur telle que l'abrogation d'un arrêté d'expulsion) doit être annexée à la demande.

La procédure de droit d'accès est gratuite.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Commission nationale de l'informatique et des libertés

21, rue Saint-Guillaume

F-75340 Paris Cedex 07

Tél.: ++33 1 53 73 22 22

Fax: ++33 1 53 73 22 00

E-mail: ffourets@cnil.fr

Internet: www.cnil.fr

Dans l'hypothèse où il s'agit d'un droit d'accès indirect (par exemple, la personne est fichée sur la base de l'article 96 de la convention: non-admission), la Commission nationale de l'informatique et des libertés effectue les vérifications (vérification de l'existence du signalement, du pays à l'origine du signalement).

Si le signalement a été effectué par les autorités françaises, le membre de la CNIL vérifie le bien-fondé du signalement (validité de la mesure d'éloignement du territoire, etc.) et demande éventuellement l'effacement des informations enregistrées.

Si le signalement a été effectué par les autorités d'un autre pays Schengen, la CNIL saisit son homologue étranger conformément au principe de coopération entre autorités nationales de protection des données. Dans cette hypothèse, les vérifications sont faites par l'homologue de la CNIL, qui l'informe de ses recherches et investigations. La CNIL est alors en mesure de répondre au demandeur.

Dans l'hypothèse où une personne rencontre des difficultés à exercer son droit d'accès direct aux informations enregistrées dans le SIS, la CNIL peut intervenir auprès du ministère français de l'intérieur.

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

Si la personne est fichée, elle est informée du pays à l'origine de son signalement dans le SIS.

S'il s'agit d'un pays où le droit d'accès aux informations est direct, elle est informée, après accord de l'autorité de contrôle nationale du pays signalant, des motifs de son fichage et, le cas échéant, des démarches qui peuvent être engagées pour obtenir la modification, voire la suppression des informations. Si, à l'issue des vérifications, la personne a été supprimée du SIS, elle en est également informée, dès lors que le pays à l'origine du signalement en est d'accord.

Si la personne est fichée par un pays où le droit d'accès aux informations est indirect, elle est informée, conformément à l'article 39 de la loi du 6 janvier 1978, de ce "qu'il a été procédé aux vérifications".

Ce principe est à nuancer pour les personnes signalées par la France.

Dans les cas où la demande de droit d'accès indirect fait suite à un refus de visa, la CNIL vérifie si le demandeur est signalé dans le SIS sur la base de l'article 96 de la convention.

Si la personne n'est pas fichée dans le SIS, la CNIL saisit le ministère des affaires étrangères pour obtenir des précisions complémentaires, afin de savoir si le refus résulte de l'inscription de la personne dans un fichier créé exclusivement à l'intention du ministère. Dans ce cas, les vérifications utiles sont opérées.

Si la personne est signalée dans le SIS par la France, en raison d'un arrêté d'expulsion ou d'une peine d'interdiction du territoire, la CNIL en informe le demandeur et lui indique les voies de recours (demande d'abrogation de l'arrêté ou demande de relèvement de l'interdiction du territoire auprès de la juridiction qui a prononcé la peine).

Dans les autres cas, le demandeur est informé de ce que les vérifications ont été faites et, le cas échéant, des démarches qu'il peut entreprendre auprès du consulat compte tenu de sa situation.

6. Références des principaux textes nationaux applicables

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (article 39).

IX. ALLEMAGNE

1. Nature du droit d'accès

Le droit d'accès en Allemagne est de nature directe. Il est exercé directement auprès du service responsable de la saisie. S'il le souhaite, l'intéressé peut aussi exercer son droit d'accès en passant par l'autorité de protection des données.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Bundeskriminalamt (Office fédéral de la police criminelle)

- SIRENE-Büro -

D - 65173 Wiesbaden

Tél: ++611 551 65 11

Fax: ++611 551 65 31

E-mail: sirenedeu@bka.bund.de

3. Formalisme de la demande: informations et documents à fournir – coût éventuel

Il convient, pour éviter toute confusion, de donner son nom (le cas échéant son nom de jeune fille), son prénom et sa date de naissance. Pour le reste, aucune forme particulière n'est requise pour la présentation de la demande. Quant à la procédure, elle est gratuite.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

L'autorité nationale de protection des données peut venir en aide à l'intéressé dans l'exercice de ses droits en transmettant la demande d'accès à l'organisme responsable de la saisie des données (p. ex. le Bundeskriminalamt) (ou Office fédéral de la police criminelle) ou encore en contrôlant, sur demande de l'intéressé, le respect de la législation en matière de protection des données par le responsable du traitement des données. Ses coordonnées sont les suivantes:

Der Bundesbeauftragte für den Datenschutz

Friedrich-Ebert-Str. 1

D -53173 Bonn

Tél: ++49-228-81995-0

Fax: ++49-228-81995-550

E-mail: poststelle@bfd.bund.de

Internet: www.bfd.bund.de

Si la demande concerne un signalement au sens de l'article 96 de la convention d'application de l'accord de Schengen, les informations sont habituellement communiquées.

Si la demande concerne un signalement au sens de l'article 95 ou de l'article 99 de la CAAS, la transmission des informations peut être refusée sur la base de l'article 19, paragraphe 4, de la loi fédérale sur la protection des données si cette transmission est de nature soit à compromettre la bonne exécution des tâches relevant de la compétence de l'organisme chargé de la saisie, soit à mettre en péril la sécurité ou l'ordre public; il en va de même lorsque les données ou leur saisie doivent être tenues secrètes en vertu d'une règle de droit ou en raison de leur nature même, notamment en raison de l'intérêt supérieur justifié d'un tiers, l'intérêt que représente pour l'intéressé la transmission des informations passant de ce fait au second plan.

Si le signalement au sens de l'article 95 de la CAAS a été effectué à l'initiative d'un organisme étranger, il y a lieu, le cas échéant, de tenir compte de la position prise par l'instance dont émane le signalement, conformément à l'article 109, paragraphe 1, troisième phrase, de la CAAS. En général, les informations sont transmises par le Bundeskriminalamt - SIRENE-Büro. Si l'intéressé s'est adressé à l'autorité nationale de protection des données, les informations sont transmises par le responsable fédéral de la protection des données. Les informations transmises comportent la base juridique du signalement, sa date, l'instance qui l'a effectué, ainsi que la durée prévisible de conservation des données.

5. Références des principaux textes nationaux applicables

Les principaux textes nationaux applicables sont l'article 109 de la convention d'application de l'accord de Schengen, en liaison avec l'article 19 de la loi fédérale sur la protection des données ou les réglementations correspondantes sur le droit d'accès figurant dans les lois des Länder sur la protection des données.

X. GRÈCE

1. Nature du droit d'accès

L'article 12 de la loi 2472/1997 prévoit que le droit d'accès s'exerce directement (l'intéressé adresse directement sa demande au bureau SIRENE).

La pratique a toutefois montré que la procédure de demande directe a pour seul effet d'entraîner une perte de temps, étant donné qu'elle n'aboutit pas. Les autorités ont par conséquent estimé que la procédure de demande indirecte permet de donner immédiatement satisfaction au citoyen; c'est donc la procédure de demande indirecte qui est appliquée sans, bien sûr, que la procédure directe ne soit exclue.

L'intéressé soumet donc, en règle générale, sa demande à l'autorité de protection des données à caractère personnel, qui la transmet ensuite au bureau SIRENE.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

La loi prévoit que l'intéressé adresse sa demande au bureau SIRENE, dont l'adresse complète est la suivante:

Ministère de l'ordre public
Police grecque
Secteur "sûreté et maintien de l'ordre"
Direction "Coopération policière internationale"
T.E.E./SCHENGEN-Bureau SIRENE
Kanellopoulou 4
GR – 101 77 Athènes
Tél.: ++301 69.81.957
Fax: ++301 69 98 264/5
E-mail: ---
Internet: ---

Toutefois, dans la pratique, l'intéressé adresse sa demande à l'autorité suivante:

Autorité de protection des données à caractère personnel

Omirou 8, 6ème étage

GR – 105 64 Athènes

Tél.: ++301 33.52.633

Fax: ++301 33.52.617

E-mail: contact@dpa.gr

Internet: www.dpa.gr

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

L'intéressé doit obligatoirement mentionner dans sa demande ses nom et prénom, le prénom de son père, sa date de naissance complète et sa nationalité. Les autres données telles que le numéro d'identité ou le numéro du passeport, le prénom de la mère, l'adresse et le numéro de téléphone sont facultatives. L'intéressé fournit une photocopie de son passeport.

L'intéressé doit payer 1 000 drachmes au responsable du traitement (le bureau SIRENE) pour pouvoir exercer son droit d'accès, conformément à l'article 12 de la loi 2472/1997, et 20 000 drachmes pour pouvoir exercer son droit d'opposition, conformément à l'article 13 de la loi 2472/1997 et à la décision 436 adoptée le 7 décembre 1998 par l'autorité de protection des données à caractère personnel. Il conviendrait d'ajouter que, en vue d'exercer le droit d'accès au SIS, la somme symbolique de 1000 GRD n'est jamais perçue et que l'Autorité grecque de protection des données à caractère personnel envisage même d'abolir officiellement cette redevance.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Les coordonnées de l'autorité nationale de protection des données à caractère personnel sont les suivantes:

Autorité de protection des données à caractère personnel

Omirou 8, 6ème étage

GR – 105 64 Athènes

Tél.: ++301 33.52.633

Fax: ++301 33.52.617

E-mail: contact@dpa.gr

Internet: www.dpa.gr

L'autorité nationale de protection des données à caractère personnel transmet la demande de l'intéressé au bureau SIRENE, et lui communique les informations qui le concernent dans la mesure où les conditions requises à cet effet sont réunies. L'autorité contrôle en outre la légitimité et le bien-fondé du signalement du demandeur dans le SIS.

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

S'il s'agit d'un signalement au titre de l'article 96 de la convention de Schengen, les informations concernant le demandeur lui sont communiquées.

Si le signalement a été effectué au titre de l'article 95 ou de l'article 99 de la convention de Schengen, il est probable que la communication de ces informations sera refusée. En outre, ces données ne sont pas communiquées si elles sont traitées pour des raisons de sécurité nationale ou dans le cadre d'une enquête sur des infractions particulièrement graves, conformément à l'article 12, paragraphe 5, de la loi 2472/1997. Dans le cas d'un signalement au titre de l'article 95 de la convention de Schengen introduit à l'initiative d'un organisme étranger, il est tenu compte de l'avis de celui-ci pour communiquer les données à l'intéressé.

Dans la pratique, les données sont communiquées à l'intéressé par l'autorité de protection des données à caractère personnel.

Les informations transmises à l'intéressé comportent la base juridique du signalement, la date de son enregistrement dans le SIS, le service qui l'a effectué et sa durée de conservation.

6. Références des principaux textes nationaux applicables

Les dispositions qui s'appliquent sont l'article 109 de la convention de Schengen, l'article 12 de la loi 2472/1997 relatif à l'exercice du droit d'accès et l'article 13 de cette même loi relatif à l'exercice du droit d'opposition.

Remarque:

Si l'intéressé a été enregistré dans le SIS par les autorités policières grecques, il adresse directement au responsable du traitement sa demande en vue de l'exercice de ses droits d'accès et d'opposition, prévus respectivement aux articles 12 et 13 de la loi 2472/1997.

XI. ISLANDE

1. Nature du droit d'accès

Le droit d'accès à l'information est direct.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

La demande est à adresser au Bureau SIRENE d'Islande, qui est dirigé par le Chef de la police nationale islandaise (CPNI).

L'adresse du CPNI est:

Ríkislogreglustjóri
Skulagata 21
IS-150 Reykjavík
Tél: ++354 570 2500
Fax: ++354 570 2501
E-mail: rls@rls.is
Internet: www.rls.is

Des formulaires de demande spéciaux peuvent être remplis dans les commissariats de police ou au siège de la Direction de la police nationale islandaise. C'est le Bureau SIRENE qui décide si les informations demandées peuvent être communiquées.

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

Le demandeur doit apporter la preuve de son identité et la demande doit être remplie en présence d'un fonctionnaire de police. Le demandeur ne peut demander l'accès qu'à des informations le concernant personnellement. Toutefois, un tuteur légal peut demander l'accès à des informations concernant son pupille. L'exercice du droit de regard est gratuit, mais une personne donnée ne peut consulter son dossier qu'une fois par an, sauf si des circonstances exceptionnelles justifient un accès plus fréquent. Dans ce cas, le Bureau SIRENE consulte l'autorité de protection des données.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Lorsqu'un demandeur a reçu la réponse-type: "Aucun renseignement vous concernant n'est enregistré/la communication des renseignements enregistrés est interdite" (cf. point 5), le Bureau SIRENE doit toutefois informer le demandeur qu'il lui est loisible de faire appel de la décision auprès du ministère de la justice. Celui-ci peut demander à l'autorité de protection des données son avis sur la décision du Bureau SIRENE.

Ministère de la justice:

Domsmalaraduneyti
Arnarhvoli
IS -150 Reykjavík
Tél: ++354 560 9010
Fax: ++354 552 7340
E-mail: postur@dkm.stjr.is
Internet: www.domsmalaraduneyti.is

Adresse de l'autorité de protection des données:

Persónuvernd
Rauðarárstígur 10
IS -105 Reykjavík
Tél: ++354 510 9600
Fax: ++354 510 9606
E-mail: postur@personuvernd.is
Internet: www.personuvernd.is

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

Le Bureau SIRENE répond sans tarder à toutes les demandes, et au plus tard dans un délai d'un mois à compter de la date de réception de la demande. Si un demandeur est fiché, il est informé de l'objet et des raisons du fichage. Lorsque l'objet du fichage rend nécessaire la préservation du secret, ou lorsque l'intérêt de tiers est en jeu, ou encore lorsqu'une opération de surveillance discrète est en cours, la personne fichée n'a pas le droit d'accéder aux données le concernant. Il lui est alors fait la même réponse qu'à un demandeur non fiché, à savoir: "Aucun renseignement vous concernant n'est enregistré/la communication des renseignements enregistrés est interdite."

6. Références des principaux textes nationaux applicables

Les principaux textes nationaux applicables sont la loi n° 16/2001 relative au système d'information Schengen en Islande et le règlement n° 112/2001 concernant le système d'information Schengen en Islande.

XII. ITALIE

1. Nature du droit d'accès

À cette date, la législation, qui pourrait bientôt faire l'objet d'une mise à jour, ne prévoit qu'un accès indirect, par le biais d'une demande adressée à l'Autorité nationale de contrôle, qui répond sur la base des vérifications effectuées directement ou par l'intermédiaire du département de la sécurité publique du ministère de l'intérieur.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Les demandes d'accès indirect doivent être adressées à:

Garante per la protezione dei dati personali
(autorité chargée de la protection des données à caractère personnel)

Piazza di Montecitorio, 121

I -00186 Rome

Tél.: ++39-06-69677713

Fax: ++39-06-69677785

E-mail: garante@garanteprivacy.it

Internet: www.garanteprivacy.it

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

Aucune formalité particulière n'est exigée pour la présentation de la demande (elle peut être envoyée par courrier ou par fax) et aucun coût ou droit de secrétariat n'a été prévu. À la différence de ce que prévoit la loi nationale sur le droit d'accès aux bases de données communes, il n'existe pas, pour la partie nationale du SIS, de disposition expresse exigeant de vérifier l'identité du demandeur. Toutefois, dans tous les cas, le "Garante" opère une vérification, même lorsque la demande émane d'un avocat ou d'un mandataire. Souvent, la copie d'une pièce d'identité est jointe.

4. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

Lorsqu'elle reçoit une demande d'accès, de vérification, de rectification ou d'effacement de données, l'Autorité nationale de contrôle procède aux contrôles et aux vérifications nécessaires par le biais de la structure nationale susmentionnée ou directement par une inspection ou un accès aux locaux et aux documents. Dans des cas plus simples, le demandeur reçoit une réponse fondée sur les vérifications effectuées par l'autorité nationale. Toutefois, si une enquête approfondie est nécessaire, celle-ci est menée selon une procédure discrète et confidentielle dont est chargé (conformément à la loi) un membre de l'Autorité de contrôle, désigné au cas par cas. En cas d'enquête approfondie, le membre de l'autorité chargé du dossier peut, si la spécificité de l'enquête l'exige, demander l'aide d'un personnel spécialisé de l'Autorité de contrôle ou d'autres autorités de l'État (appartenant aux forces de police) tenues au secret professionnel. À l'issue des vérifications, si le traitement des données à caractère personnel n'apparaît pas conforme aux dispositions législatives ou réglementaires, l'Autorité de contrôle informe l'autorité compétente des *modifications et ajouts nécessaires et en vérifie l'exécution*¹.

Une fois les vérifications terminées et conformément à la législation en vigueur, l'intéressé est informé, dans tous les cas, du résultat des recherches, y compris de l'État à l'origine du signalement, sauf dans les cas où cette indication n'est pas autorisée, à savoir lorsqu'elle pourrait *entraver la poursuite des objectifs* du signalement ou *compromettre les actions ou opérations visant à sauvegarder l'ordre et la sécurité publique, à assurer la prévention et la répression de la criminalité, ou tant qu'est maintenu le signalement aux fins de surveillance discrète* (prévue à l'article 99 de la convention d'application de l'accord de Schengen) ou encore *lorsqu'il s'avère nécessaire de protéger les droits d'autrui*. Cette communication comprend également les données relatives à l'intéressé.

5. Références des principaux textes nationaux applicables

Les principales dispositions législatives nationales applicables sont:

- a) la loi n° 388 du 30 septembre 1993 relative à la ratification et à la mise en œuvre de l'accord de Schengen et de sa convention d'application (en particulier les articles 9, 10, 11 et 12);
- b) la loi n° 675 du 31 décembre 1996 relative à la protection des données à caractère personnel (en particulier l'article 4, paragraphe 1, point a), et l'article 31, paragraphe 1, point p)).

¹ N.d.T. : Tous les passages en italique sont des traductions non officielles de la législation italienne.

XIII. LUXEMBOURG

1. Nature du droit d'accès

L'accès est indirect en ce sens que le droit d'accès ne peut être exercé que par l'intermédiaire de l'autorité de contrôle.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Autorité de contrôle instituée par l'article 12-1 (4) de la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques

Parquet Général du Grand-Duché de Luxembourg

BP 15

L-2010 Luxembourg

Tél.: ++352 47 59 81-331

Fax: ++352 47 05 50

E-mail: parquet.general@mj.etat.lu

Internet: ---

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

La loi de 1979 n'impose aucune condition de forme particulière pour les demandes.

La procédure est gratuite.

En vertu de l'article 12-1 (5) de la loi de 1979, l'autorité "procède aux vérifications et investigations utiles et fait opérer les rectifications nécessaires".

4. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

L'autorité "informe l'intéressé que la banque ne contient aucune donnée contraire à la convention, à la loi et à ses règlements d'exécution ou aux conditions imposées par le ministre".

L'intéressé n'obtient aucune information sur le contenu des données le concernant.

5. Références des principaux textes nationaux applicables

Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, telle que modifiée.

Règlement grand-ducal du 9 août 1993 autorisant la création et l'exploitation d'une banque de données nominatives constituant la partie nationale du système d'information Schengen (N.SIS) (le règlement ne régit pas le droit d'accès).

XIV. PAYS-BAS

1. Nature du droit d'accès

La partie nationale du système d'information Schengen relève, pour ce qui concerne les signalements basés sur l'article 96 de la convention d'application de Schengen, de la loi sur la protection des données à caractère personnel (wetbescherming persoonsgegevens). Les autres signalements relèvent de la loi sur les registres de police (Wetbescherming politieregisters).

Ces deux lois accordent aux personnes qui font l'objet d'un signalement le droit de prendre connaissance de celui-ci.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Les demandes d'accès doivent être adressées à l'instance suivante:

Korps Landelijke Politiediensten
Attention of the data protection officer
Postbus 3016
NL – 2700 KX Zoetermeer
Tél: ++79 345 90 62
Fax: ++79 345 90 10

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

Lorsqu'une personne introduit une demande d'accès, le Service central d'enquête et d'information (Divisie Centrale Recherche Informatie) prend contact avec elle au sujet des modalités de traitement de sa demande. Un montant de 10 NLG peut être exigé pour ce traitement.

Le service en question examine s'il peut accéder à la demande ou s'il existe des motifs juridiques qui justifient son rejet.

L'accès à un signalement effectué sur la base de l'article 96 peut se faire sous la forme d'une copie remise à l'intéressé.

Quant aux autres catégories de signalements, soit on en communique le contenu, soit l'intéressé en prend effectivement connaissance, mais il n'est pas possible d'en obtenir une copie.

Après avoir pris connaissance du signalement, la personne concernée peut introduire une demande visant à compléter, à rectifier ou à effacer les dossiers qu'il contient.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Si le traitement de la demande donne lieu à un litige, une demande de conciliation peut être adressée à l'organe suivant:

College Bescherming Persoonsgegevens

Postbus 93374

NL - 2509 AJ Den Haag

Tél: ++31(0)703811300

Fax: ++31(0)703811301

E-mail: mail@cbpweb.nl

Internet: www.cbpweb.nl

L'intervention du College Bescherming Persoonsgegevens (autorité néerlandaise de protection des données) est gratuite si la demande est rejetée. Le College Bescherming Persoonsgegevens peut également être invité à examiner si les données ont été enregistrées dans le système d'information Schengen conformément à la convention d'application de Schengen et à la loi. A titre de rechange, ou si la conciliation du CBP a échoué, une requête peut être adressée au tribunal d'arrondissement de La Haye afin qu'il examine l'affaire et rende un jugement.

XV. NORVÈGE

1. Nature du droit d'accès

Le droit d'accès est direct.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Kriminalpolitisenralen

(Service national d'enquête en matière criminelle - NCIS)

PO Box 8163 Dep.

NO-0034 OSLO

Tél: ++ 47 23 20 80 00

Fax: ++ 47 23 20 88 80

E-mail:

Internet: www.kripos.no

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

La demande de droit d'accès doit être faite par écrit et signée. Une réponse est adressée par écrit dans un délai raisonnable qui ne peut excéder 30 jours à compter de la réception de la demande.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Datatilsynet

PO Box 8177 Dep.

NO-0034 OSLO

Tél.: + 47 22 39 69 00

Fax: + 47 22 42 23 50

E-mail: postkasse@datatilsynet.no

Internet: www.datatilsynet.no

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

C'est l'autorité gestionnaire des fichiers (NCIS) qui se prononce en première instance sur les demandes. Si la demande a été présentée au gestionnaire des fichiers, elle est déférée à l'autorité qui a ordonné l'enregistrement, accompagnée d'une demande d'avis. Si la demande a été déposée auprès de l'autorité qui a ordonné l'enregistrement, celle-ci transmet la demande au gestionnaire des fichiers, accompagnée d'un avis.

Si le droit d'accès n'est pas accordé parce que le demandeur n'a pas fait l'objet d'un enregistrement ou parce que la clause d'exclusion de l'acte instituant le SIS (section 15) s'applique, d'autres raisons sont toujours invoquées afin qu'il ne ressorte pas des motifs exposés qu'il existe des enregistrements auxquels l'accès serait refusé.

6. Références des principaux textes nationaux applicables

Loi relative au système d'information Schengen (Loi 1999-07-16-66)

Règlements d'application de la loi n° 66 du 16 juillet 1999 relative au système d'information Schengen (règlements SIS).

XVI. PORTUGAL

1. Nature du droit d'accès

Les citoyens ont un droit d'accès indirect aux données du SIS. Ce droit est garanti par la commission nationale de protection des données.

2. Formalisme de la demande: informations et documents à fournir - coût éventuel

Les demandes doivent être présentées par écrit, et doivent contenir l'identité de la personne qui souhaite accéder aux données la concernant. Les demandeurs doivent joindre un document confirmant leur identité (carte d'identité ou passeport). L'exercice du droit d'accès est gratuit.

3. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Comissão Nacional de Protecção de Dados (Commission nationale de protection des données)

Rua de S. Bento, n° 148 – 3

P -1200-821 LISBONNE

Tél: ++351 21- 392 84 00

Fax: ++351 21- 397 68 32

E-mail: geral@cnpd.pt

Internet: www.cnpd.pt

Dans le cadre de la communication de l'information, on tient compte de l'éventuelle existence d'informations susceptibles de compromettre soit la prévention de la criminalité et le bon déroulement d'enquêtes judiciaires, soit la sécurité de l'État.

La communication est faite par la commission nationale de protection des données.

4. Références des principaux textes nationaux applicables

La législation applicable est la loi n° 67/98 du 26 octobre 1998 (article 11, paragraphe 2) et la loi n° 2/94 du 19 février 1994.

XVII. ESPAGNE

1. Nature du droit d'accès

Le droit d'accès aux données est direct.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Secretaría de Estado de Seguridad (Secrétariat d'État pour la sécurité)

Paseo de la Castellana, n° 64

E -28046 Madrid

Tél.: ++34 91 537 23 07

Fax: ++34 91 537 23 24/562 87 43

E-mail: ---

Internet: ---

3. Formalisme de la demande: informations et documents à fournir – coût éventuel

La demande doit être envoyée au responsable du fichier par tout moyen permettant d'établir qu'elle a été envoyée et reçue; elle doit contenir:

- les nom et prénom de l'intéressé et la photocopie du document établissant son identité, comme par exemple, la carte nationale d'identité ou le passeport;
- la demande proprement dite;
- l'adresse à laquelle le courrier doit être adressé, la date et la signature du demandeur;
- des documents à l'appui de la demande, le cas échéant.

À l'heure actuelle, cette procédure est gratuite.

4. Coordonnées de l'autorité nationale de protection des données, et rôle qu'elle peut jouer

Agencia de Protección de Datos (Agence pour la protection des données)

C/ Sagasta, n° 22

E -28004 Madrid

Tél: ++34 91 399 62 18/399 62 19

Fax: ++34 91 447 10 92

E-mail: inspeccion@agenciaprotecciondatos.org

Internet: www.agenciaprotecciondatos.org

Les intéressés qui estiment que certains de leurs droits ont été lésés à l'occasion d'une demande de droit d'accès peuvent déposer une réclamation auprès de l'Agence. Une fois la réclamation reçue, une copie de celle-ci est transmise au responsable du fichier afin qu'il formule les observations qu'il juge pertinentes. Enfin, après avoir reçu les observations et pris connaissance des rapports et des preuves et une fois que les autres mesures d'instruction sont prises, notamment, si nécessaire, l'examen des fichiers, ainsi que l'audition de l'intéressé et du responsable du fichier, le Directeur de l'Agence statue sur la réclamation déposée et notifie sa décision aux intéressés.

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication.

Au cas où les informations concernant l'intéressé figureraient dans le fichier SIS et y auraient été introduites par les autorités espagnoles et que la décision serait positive, le responsable du fichier remet à l'intéressé une copie imprimée des données le concernant qui figurent dans ce fichier.

6. Références des principaux textes nationaux applicables

- Loi organique 15/1999, du 13 décembre, relative à la protection des données à caractère personnel,
- Décret royal 428/1993, du 26 mars, portant adoption du statut de l'Agence de protection des données,
- Décret royal 1332/1994, du 20 juin, développant certains principes de la loi organique,
- Instruction 1/1998, du 19 janvier, de l'Agence pour la protection des données, relative à l'exercice des droits d'accès, de rectification et d'effacement.

XVIII. SUÈDE

1. Nature du droit d'accès

Le droit d'accès aux données est direct.

2. Coordonnées de l'organisme auquel la demande de droit d'accès doit être adressée

Toute demande d'accès aux données doit être adressée à la Direction nationale de la police (rikspolisstyrelsen), l'autorité responsable des données à caractère personnel.

Rikspolisstyrelsen

Box 12256

Polhemsgatan 30

S -102 26 Stockholm

Tél: ++46 (0)8-401 90 00

Fax: ++46 (0)8-401 99 90

E-mail: rikspolisstyrelsen@rps.police.se

Internet:

3. Formalisme de la demande: informations et documents à fournir - coût éventuel

La demande devra être adressée par écrit à la Direction nationale de la police et signée par le demandeur lui-même. L'information doit normalement lui être transmise dans le mois de la demande. Le demandeur peut obtenir gratuitement l'accès aux informations une fois par année civile.

4. Coordonnées de l'autorité nationale de protection des données et rôle qu'elle peut jouer

Datainspektionen

Box 8114

Fleminggatan 14, 9ème étage

S -104 20 Stockholm

Tél.: ++46 (0)8-657 61 00

Fax: ++46 (0)8-652 86 52

E-mail: datainspektionen@datainspektionen.se

Internet: www.datainspektionen.se

5. Résultats à attendre de la demande de droit d'accès. Contenu de la communication

La transmission ou non-transmission des données dépend des dispositions de la loi sur la confidentialité (1980:100), laquelle peut interdire la communication de certaines données. Lorsque les données peuvent être transmises, c'est la Direction nationale de la police qui s'en charge.

6. Références des principaux textes nationaux applicables

Législation applicable: les articles 26 et 27 de la loi sur les données à caractère personnel (1998:204), ainsi que l'article 8 de la loi relative au système d'information Schengen (2000:344).
