LE SYSTÈME D'INFORMATION SCHENGEN

MÉMENTO SUR L'EXERCICE DU DROIT D'ACCÈS

Ce mémento a été rédigé par

l'Autorité de contrôle commune de

Schengen

Adresse: Secrétariat chargé de la protection des données
Conseil de l'Union européenne
Rue de la Loi 175 (OOFL59)
B-1048 BRUXELLES
Tél: +32(0)22818996

TABLE DES MATIÈRES

I. RAPPEL DES PRINCIPES GÉNÉRAUX 4
II. DESCRIPTION DE LA PROCÉDURE DE DROIT D'ACCÈS DANS CHACUN DES PAYS DE L'ESPACE SCHENGEN 7
III. SITUATIONS PARTICULIÈRES NÉCÉSSITANT UNE PROCÉDURE SPÉCIFIQUE: 7
IV. AUTRICHE 13
V. BELGIQUE 18
VI. RÉPUBLIQUE TCHÈQUE 20
VII. DANEMARK 22
VIII. FINLANDE 25
IX. FRANCE 26
X. ALLEMAGNE 28
XI. GRÈCE 30
XII. HONGRIE 32
XIII. ISLANDE 34
XIV. ITALIE 36
XV. LETTONIE 38
XVI. LUXEMBOURG 41
XVII. LITUANIE 43
XVIII. MALTE 47
XIX. PAYS-BAS 49
XX. NORVÈGE 51
XXI. POLOGNE 53
XXII. PORTUGAL 57
XXIII. SLOVAQUIE 58
XXIV. SLOVÉNIE 61
XXV. ESPAGNE 64
XXVI. SUÈDE 67
XXVII. SUISSE 69
ANNEXES (MODELES DE LETTRES) 70
Annexe 1 70
Annexe 2 71
Annexe 3 72

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

Destiné initialement à aider les personnes concernées à exercer leur droit d'accès, ce document se veut un outil pratique pouvant également être consulté par toute personne intéressée à titre professionnel par l'exercice du droit d'accès (autorités de protection des données, services de police, services des étrangers, avocats etc.).

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, des certificats d'immatriculation de véhicules et des plaques d'immatriculation de véhicules.

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 une mesure ne peut pas être exécutée conformément à ce droit national, l'État Schengen requis doit en informer sans délai l'État Schengen signalant.

En application des principes de la protection des données, la convention Schengen reconnaît des droits particuliers à toutes les personnes.

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 fait ou d'effacement lorsque les données sont enregistrées sur la base d'une erreur de droit;
- du droit de demander aux autorités nationales de protection des données de vérifier les données les concernant intégrées dans le SIS ainsi que l'utilisation qui est faite de ces données;
- 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 doit être refusé s'il est susceptible de nuire à l'exécution de la tâche légale consignée dans le signalement, ou pour la protection des droits et libertés d'autrui. Il doit être refusé dans tous les cas durant la période de validité d'un 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 régissant le droit d'accès et de rectification 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.

[1] Belgique, République tchèque, Hongrie, Malte, Lituanie, Lettonie, Pays-Bas, Luxembourg, France, Allemagne, Italie, Portugal, Espagne, Autriche, Grèce, Danemark, Slovénie, slovaquie, Pologne, Suède, Suisse, Finlande, Norvège et Islande (situation en octobre 2009).

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.

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 étroite 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 PROCEDURE DE DROIT D'ACCES 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 XXVII.

III. SITUATIONS PARTICULIERES NECESSITANT UNE PROCEDURE SPECIFIQUE:

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.

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, 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, étant donné qu'il ne devrait pas être possible qu'une personne réside sur le territoire d'un État membre de l'espace Schengen tout en étant, dans le même temps, 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 qui a délivré le titre de séjour 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 (au moyen d'une copie d'un document d'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 (y compris lorsqu'aucune donnée n'a été 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 dans la mesure où les demandes qui lui sont faites sont raisonnables.
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 18,89 EUR peut être demandée, ce montant pouvant être majoré si des dépenses supplémentaires sont réellement effectuées. 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)

Hohenstaufengasse 3,
A -1010 Vienne,
Tél.: ++43 1 531 15/2525,
Fax:++43 1 531 15/2690,
E-mail: dsk@dsk.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),
BGBl.(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 d'un 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 18,89 EUR 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.

6. Régime linguistique

Conformément à la législation autrichienne, l'intéressé peut engager la procédure de demande d'accès en allemand.

V. BELGIQUE

1. Nature du droit d'accès

Toute personne bénéficie d'un droit d'accès indirect à toutes les 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
Rue Haute 139
1000 Bruxelles

Commissie voor de bescherming van de persoonlijke levensfeer
Hoogstraat 139
1000 Bruxelles
Tél: ++32 (0)2 213 85 40
Fax: ++32 (0)2 213 85 65
Site web: http://www.privacycommission.be http://www.privacycommission.be/
E-mail: commission@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 le 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. RÉPUBLIQUE TCHÈQUE

1. Nature du droit d'accès

La personne concernée a un droit d'accès direct. Elle devrait principalement exercer ses droits à l'égard du SIS auprès du responsable du traitement, à savoir la police de la République tchèque.

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

Direction de la police de la République tchèque
P.O. Box 62/K-SOU
Strojnická 27
170 89 Prague 7

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

Le site Internet de l'autorité de protection des données (http://www.uoou.cz) contient des informations relatives aux modalités de demande d'informations sur les données de rectification ou d'effacement de ces données, y compris des formulaires que la personne concernée peut utiliser. Des informations sont également disponibles sur le site Internet de la police (http://www.policie.cz) et sur celui du ministère de l'intérieur (http://www.mvcr.cz/eu-schengen.aspx), ainsi que sur le site Internet généraliste tchèque consacré à l'Europe (http://www.euroskop.cz).

Toute personne concernée est habilitée à envoyer une demande écrite à la police de la République tchèque (cf. adresse ci-dessus), pour exercer son droit d'information sur les données la concernant intégrées dans le SIS ou son droit d'effacer ou de rectifier ces donnés. Les informations relatives au traitement de données à caractère personnel dans le SIS ne sont communiquées qu'à la personne concernée (ou à son avocat). La demande doit contenir des renseignements identifiant le demandeur (nom et prénoms complets, date et lieu de naissance et adresse). La police est tenue de fournir une réponse dans un délai de 60 jours. L'exercice du droit d'accès est gratuit.

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

Bureau de la protection des données à caractère personnel
Pplk. Sochora 27
170 00 Prague 7
République tchèque

Le Bureau de la protection des données à caractère personnel est compétent pour contrôler le traitement des données à caractère personnel dans la partie nationale du SIS, à la demande des personnes concernées, en cas de suspicion d'une procédure entachée d'erreur de droit ou lorsque le responsable du traitement (la police de la République tchèque) n'a pas apporté de réponse satisfaisante à la demande.

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

Dans sa réponse, la police doit indiquer si des données à caractère personnel relatives à la personne concernée ont été intégrées dans le SIS et préciser la nature de ces données, la raison de leur intégration (la finalité) et l'autorité ayant procédé à cette intégration.
Conformément aux articles 83 et 84 de la loi sur la police de la République tchèque, la police rejette la demande si la communication des informations concernées est susceptible de compromettre l'accomplissement de tâches de police dans le cadre d'une procédure pénale, de nuire à la sécurité nationale ou de mettre en péril les intérêts légitimes d'un tiers.

6. Références des principaux textes nationaux applicables

Loi n° 101/2000 publiée au Journal officiel sur la protection des données à caractère personnel et portant modification de certaines lois (articles 12 et 21).
Loi n° 273/2008 publiée au Journal officiel sur la police de la République tchèque (articles 83 et 84).

7. Régime linguistique

Le tchèque est la seule langue officielle de communication avec les autorités de la République tchèque. Néanmoins, l'autorité tchèque de protection des données communique également en anglais. Les informations de base concernant les modalités de demande d'exercice du droit d'accès qui figurent sur le site Internet de l'autorité de protection des données sont également disponibles en anglais.

VII. 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 Copenhague 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 Copenhague K
Tél: +45 3319 3200
Fax: ++45 3319 3218
E-mail: dt@datatilsynet.dk
Internet: www.datatilsynet.dk

Les réclamations concernant la décision prise par la police nationale en matière d'accès peuvent être adressées à l'autorité de protection des données. 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, de la comparution des personnes citées, de 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 localisation 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 nº 429 du 31 mai 2000 sur le traitement des données à caractère personnel.

VIII. FINLANDE

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 doivent être introduites auprès du commissariat de police du district par les intéressés eux-mêmes.

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.

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.

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 (0) 10 36 66700
Fax: ++358 (0) 10 36 66735
E-mail: tietosuoja@om.fi
Internet: www.tietosuoja.fi

Si la police 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).

5. Références des principaux textes nationaux applicables

Loi relative aux données à caractère personnel (523/1999)
Loi relative au traitement des données à caractère personnel par la police (761/2003)

IX. 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 l'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
8, rue Vivienne - CS 30223
F-75083 Paris Cedex 02
Tél.: ++33 1 53 73 22 22
Fax: ++33 1 53 73 22 00
E-mail: bmonegier@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
8, rue Vivienne - CS 30223
F-75083 Paris Cedex 02
Tél.: ++33 1 53 73 22 22
Fax: ++33 1 53 73 22 00
E-mail: bmonegier@cnil.fr
Internet: www.cnil.fr

5. Régime linguistique

La personne concernée peut introduire sa demande en français.

X. 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: sirenedeutschland@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, il n'existe pas d'exigences particulières concernant le formalisme de la demande et la procédure est gratuite.

Il incombe à l'autorité compétente (le Bundeskriminalamt) de décider des détails de la suite de la procédure.

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 (par exemple le Bundeskriminalamt) 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 und die Informationsfreiheit
Husarenstraße 30
D-53117 Bonn
Tél.: ++49-228-997799-0
Fax: ++49-228-997799-550
E-mail: poststelle@bfdi.bund.de
Internet: www.bfdi.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 si au moins l'un des motifs généralement valables pour refuser la communication d'informations, visés à l'article 19, paragraphe 4, de la loi fédérale sur la protection des données, s'applique à la demande, à savoir 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, ou si 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 généralement 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.

6. Régime linguistique

Conformément à la législation nationale (article 23 de la loi fédérale sur la procédure administrative non contentieuse - Verwaltungsverfahrensgesetz), la langue officielle est l'allemand mais, au regard de la citoyenneté de l'Union visée aux articles 17 et suivants du traité CE, les demandes ou requêtes présentées dans d'autres langues de l'UE que l'allemand sont également acceptées.

XI. 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). Si l'intéressé soumet sa demande à l'autorité de protection des données à caractère personnel, il lui est conseillé de l'adresser directement 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 la protection du citoyen
Police grecque
Direction "Coopération policière internationale"
3ème section SIRENE
Kanellopoulou 4
GR – 101 77 Athènes
Tél.: ++301 69.81.957
Fax: ++301 69 98 264/5
E-mail: info@sirene-gr.com
Internet: ---

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 5 euros 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 60 euros pour pouvoir exercer son droit d'opposition, conformément à l'article 13 de la loi 2472/1997 et à la décision 122 adoptée le 9 octobre 2001 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 5 euros 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 grecque de protection des données
Kifisias 1-3, 1er étage
GR – 115 23 Athènes
Tél.: ++30 210 6475600
Fax: ++301 210 6475628
E-mail: contact@dpa.gr
Internet: www.dpa.gr

L'autorité nationale de protection des données à caractère personnel contrôle 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.

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.

En ce qui concerne le régime linguistique, la langue officielle est le grec, mais les demandes en anglais sont également examinées.

XII. HONGRIE

1. Nature du droit d'accès

Le droit d'accès peut être exercé directement et indirectement.

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

État-major de la police nationale - Bureau SIRENE
H-1139 Budapest, Teve utca 4-6.
Tél.: +36 1 443 5861
E-mail: sirene@nebek.police.hu

Bureau du Commissaire parlementaire pour la protection des données
H-1051 Budapest, Nádor u. 22.
Tél: +36 1 475 7100
E-mail: privacy@obh.hu

Les demandes d'accès peuvent être introduites par l'intéressé lui-même auprès de tout poste de police sur le territoire de la Hongrie et de toute mission diplomatique de la République de Hongrie. Les demandes seront transmises au bureau SIRENE.

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

L'intéressé doit fournir une preuve crédible de son identité. Les demandes peuvent être introduites en hongrois, en anglais, en allemand ou en français. Les informations doivent être communiquées par écrit dans les délais les plus brefs, mais au plus tard dans les trente jours suivant l'introduction de la demande. Les demandes d'accès sont gratuites; si l'intéressé introduit une nouvelle demande au cours de la même année civile, les coûts relatifs à la communication des informations lui seront facturés.

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

Le commissaire pour la protection des données est compétent pour répondre aux demandes qui lui sont envoyées, après vérification dans les fichiers correspondants du Système d'information Schengen. Par ailleurs, si la personne concernée a des doutes concernant la réponse reçue du bureau SIRENE ou si ce dernier ne lui pas fourni de réponse, la personne concernée peut s'adresser au commissaire pour la protection des données.

5. Références des principaux textes nationaux applicables

Loi LXIII de 1992 sur la protection des données à caractère personnel et l'accès du public aux données d'intérêt public.

Loi CV de 2007 sur la coopération et l'échange d'informations dans le cadre de la convention d'application de l'accord de Schengen.

XIII. 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:

Ríkislögreglustjóri
Skúlagata 21
IS-150 Reykjavik
Tél: ++354 444 2500
Fax: ++354 444 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 et des droits de l'homme. Celui-ci peut demander à l'autorité de protection des données son avis sur la décision du bureau SIRENE.

Ministère de la justice et des droits de l'homme:
Dómsmála- og mannréttindaráduneytid
Skuggasund
IS -150 Reykjavík
Tél: ++354 545 9000
Fax: ++354 552 7340
E-mail: postur@dmr.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 nº 16/2000 relative au Système d'information Schengen en Islande et le règlement nº 112/2001 concernant le Système d'information Schengen en Islande.

7. Régime linguistique

Bien qu'aucune disposition légale ne le prévoie expressément, l'islandais est la langue de procédure en Islande. Toutefois, si une autorité islandaise reçoit une demande rédigée dans une autre langue que l'islandais, il sera répondu à cette demande. Si la demande émane d'une personne qui n'est pas en mesure de comprendre une réponse rédigée en islandais (par exemple un ressortissant étranger dont les intérêts ne sont pas représentés par une partie islandaise, par exemple un avocat), elle fera l'objet d'une réponse dans une langue comprise par cette personne.

XIV. ITALIE

1. Nature du droit d'accès

Le droit d'accès ne peut être exercé que de manière directe, en adressant une demande au responsable du traitement 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

Conformément aux directives fournies par le département de la sécurité publique susmentionné, toutes les demandes d'accès et de vérification sont à envoyer à l'adresse suivante:

Ministero dell'interno (Ministère de l'intérieur)
Dipartimento della pubblica sicurezza (Département de la sécurité publique)
Ufficio coordinamento e pianificazione delle forze di polizia
Divisione N.SIS
Via di Torre di Mezza Via 9/121 - 00173 Roma

S'ils jugent insatisfaisante la réponse apportée à leur demande, les personnes concernées peuvent adresser une réclamation au Garante per la protezione dei dati personali (Commissaire à la protection des données), à l'adresse suivante:

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma

Il est préférable d'envoyer les réclamations par courrier plutôt que par fax, afin de s'assurer que tous les documents seront intégralement lisibles. Les personnes introduisant une réclamation doivent y faire figurer des coordonnées suffisantes, y compris si possible leur adresse postale, afin de faciliter la correspondance.

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. Bien qu'il n'existe pas dans la législation applicable, pour l'accès à la partie nationale du SIS, de dispositions expresses exigeant de vérifier l'identité du demandeur, afin d'accélérer le traitement des demandes, celles-ci devraient être rédigées, si possible, en italien, en anglais, en français ou en allemand et **signées par la personne concernée**, contenir une brève description des motifs invoqués et être accompagnées de la **photocopie d'une pièce d'identité appropriée et en cours de validité de la personne concernée**.

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

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) le décret législatif n° 196 de 2003.

XV. LETTONIE

1. Nature du droit d'accès

Chacun (qu'il s'agisse de personnes ressortissantes d'un État membre de l'espace Schengen ou non) dispose d'un droit d'accès direct aux données à caractère personnel le concernant qui sont intégrées dans le SIS, et ce, en vertu des règlements ministériels n° 622 sur les modalités de demande d'informations par les personnes concernées et de communication auxdites personnes des informations les concernant intégrées dans le Système d'information Schengen et le système d'information SIRENE. La personne concernée devrait recevoir une réponse à sa demande dans un délai d'un mois.

L'organisme compétent pour statuer sur une réclamation introduite par une personne dont la demande de consultation des données à caractère personnel la concernant a été rejetée ou est restée sans réponse est l'Inspection publique des données, qui est également compétente pour contrôler la mise en œuvre du droit à rectifier des données incorrectes ou à effacer des données à caractère personnel entachées d'erreur de droit.

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

Les demandes d'accès direct sont à adresser (par écrit) à la police nationale ou aux représentations diplomatiques et consulaires de la République de Lettonie.

Police nationale
Čiekurkalna 1.linija 1, k-4
Riga, LV-1026
Tél: +371 67075212; fax +371 67371227
E-mail: kanc@vp.gov.lv

Les coordonnées des représentations diplomatiques et consulaires de la République de Lettonie sont disponibles sur le site Internet du ministre des affaires étrangères (lien direct: http://www.mfa.gov.lv/lv/Ministrija/mission).

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

Les demandes sont à présenter à la police nationale ou aux représentations diplomatiques et consulaires de la Lettonie, en personne ou par voie électronique, au moyen d'une lettre datée et signée. Lorsqu'elle présente sa demande en personne, la personne concernée doit prouver son identité en produisant une pièce d'identité. Si la demande est présentée par voie électronique, elle doit comporter une signature électronique sécurisée.

Les demandes doivent indiquer le nom et le prénom de la personne concernée, sa date de naissance, son code personnel (si elle en a un), son lieu de naissance, son État d'origine, le type (le cas échéant) et le numéro de sa pièce d'identité, le nom de l'autorité qui a délivré sa pièce d'identité, la date de délivrance et la date d'expiration de sa pièce d'identité, la quantité d'informations requises (informations relatives à la personne concernée, informations sur les destinataires des informations relatives à la personne concernée), la manière dont la personne souhaite recevoir la réponse à sa demande (en personne dans les locaux de la police nationale ou des représentations diplomatiques et consulaires de la Lettonie ou par courrier - dans ce cas, elle est invitée à indiquer l'adresse à laquelle la réponse doit être envoyée).

Cette procédure est gratuite.

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

Les agents de la police nationale ou des représentations diplomatiques et consulaires de la Lettonie qui reçoivent une demande d'informations provenant d'une personne concernée vérifient l'identité du demandeur et transmettent la demande au département de la police nationale exerçant les fonctions de bureau SIRENE letton.

Le bureau SIRENE effectue les vérifications nécessaires concernant la demande présentée et, dans un délai d'un moins, fournit une réponse à la personne concernée ou rejette sa demande d'informations, en envoyant une réponse à l'adresse ou à l'autorité indiquée par la personne concernée ou à la police nationale ou aux représentations diplomatiques et consulaires de la Lettonie.

5. Références des principaux textes nationaux applicables

- Loi sur la protection des données à caractère personnel;
- Loi sur le fonctionnement du Système d'information Schengen;
- Règlements ministériels n° 622 (du 11.9.2007) sur les modalités de demande d'informations par les personnes concernées et de communication auxdites personnes des informations les concernant intégrées dans le Système d'information Schengen et le système d'information SIRENE.

6. Régime linguistique

En ce qui concerne le régime linguistique, conformément à la loi sur la langue officielle de la République de Lettonie, qui régit également les droits d'accès au SIS, toutes les procédures engagées auprès d'autorités lettones devraient être menées en letton. Néanmoins, la loi sur les pétitions (article 7, section 1, point 4) dispose qu'une pétition ou une réclamation peut rester sans réponse si son texte ne peut être objectivement lu ou compris. Le bureau SIRENE letton a indiqué qu'il examinait également les demandes rédigées en anglais ou en russe.

XVI. 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'autorité à laquelle il convient d'adresser les demandes d'accès

Autorité de contrôle instituée par l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006 et la loi du 27 juillet 2007.

Parquet Général du Grand-Duché de Luxembourg
BP 15
L-2010 Luxembourg
Tél.: ++352 47 59 81–331
Fax: ++352 47 05 50
Adresse électronique: parquet.general@mj.etat.lu

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

La loi de 2002 ne prévoit pas de prescriptions particulière pour l'introduction des demandes.
Cette procédure est gratuite.
En vertu de l'article 17 de la loi de 2002, l'autorité de contrôle "procède aux vérifications et investigations utiles et fait opérer les rectifications nécessaires".

4. Résultats escomptés des demandes d'accès et contenu des informations communiquées

L'autorité de contrôle "informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution".

Aucune information n'est communiquée sur le contenu des données relatives à la personne concernée.

5. Références des principaux textes nationaux applicables

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, dans sa version 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 (NSIS) (ce règlement ne régit pas le droit d'accès).

6. Régime linguistique

La personne concernée peut engager la procédure à suivre pour l'exercice du droit d'accès dans l'une des langues suivantes:

- luxembourgeois;
- français;
- allemand;
- anglais.

XVII. LITUANIE

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

La personne concernée a un droit d'accès direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès, de rectification ou d'effacement sont à adresser au ministère de l'intérieur de la République de Lituanie, qui est le responsable du traitement des données:

Ministry of the Interior of the Republic of Lithuania
Šventaragio str. 2, LT-01510 Vilnius
Lituanie
Tél. +370 5 271 7130, fax +370 5 271 8551
Adresse électronique: korespondencija@vrm.lt

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Les demandes doivent être présentées par écrit et signées. Elle doivent mentionner l'identité de la personne qui souhaite avoir accès aux données la concernant, ou obtenir la rectification/l'effacement des données la concernant (nom(s) et prénom(s), numéro d'identification personnel (en l'absence de celui-ci, la date de naissance), le lieu de résidence, les coordonnées (numéro de téléphone ou adresse électronique)). Le demandeur doit remettre au responsable du traitement des données un document attestant de son identité. L'exercice de ces droits est gratuit.

4. Résultats escomptés des demandes d'accès et contenu des informations communiquées

La personne concernée a le droit d'obtenir des informations sur les sources et le type de données à caractère personnel qui ont été collectées à son sujet, la finalité de leur traitement et les destinataires auxquels les données sont ou ont été transmises.

Lorsqu'une personne concernée lui adresse une demande relative au traitement de ses données à caractère personnel, le responsable du traitement doit lui faire savoir si les données à caractère personnel la concernant font l'objet d'un traitement et lui transmettre les informations demandées au plus tard 30 jours civils à compter de la date de la demande.

Lorsque la personne concernée, après avoir pris connaissance de ses données à caractère personnel, estime que celles-ci sont erronées, incomplètes ou inexactes, ou que le traitement dont elle font l'objet est illicite et déloyal et qu'elle en informe par écrit le responsable du traitement, celui-ci doit vérifier les données à caractère personnel concernées sans délai et rectifier les données erronées, incomplètes ou inexactes et/ou suspendre le traitement de ces données, exception faite de leur conservation. S'il constate que les données à caractère personnel font l'objet d'un traitement illicite et déloyal, le responsable du traitement doit détruire les données à caractère personnel collectées de manière illicite et déloyale ou suspendre le traitement de ces données sans délai, exception faite de leur conservation.
Il doit informer sans délai la personne concernée et les destinataires des données que les données à caractère personnel ont été rectifiées ou détruites ou que leur traitement a été suspendu à la demande de la personne concernée.

Conformément à l'article 17, paragraphe 2, de la loi sur la protection juridique des données à caractère personnel, le responsable du traitement doit veiller à ce que la personne concernée puisse exercer ses droits, sauf dans les cas prévus par la loi lorsqu'il est nécessaire d'assurer:

1) la sûreté ou la défense de l'État;
2) l'ordre public, la prévention, la recherche, la détection et la poursuite d'infractions pénales;
3) des intérêts économiques ou financiers important de l'État;
4) la prévention, la recherche et la détection de manquements à la déontologie officielle ou professionnelle;
5) la protection des droits et libertés de la personne concernée ou de toute autre personne.

La communication à la personne concernée d'informations sur ses données à caractère personnel est refusée lorsqu'il est nécessaire de prendre des mesures relatives au signalement ou pour défendre les droits et libertés de tiers. Les informations sur les données à caractère personnel de la personne concernée ne lui sont pas communiquées avant l'expiration du délai applicable en cas de signalement donnant lieu à une surveillance secrète.
Le refus du responsable du traitement de donner suite à la demande de la personne concernée doit être justifié par un motif raisonnable. Le responsable du traitement est tenu d'informer la personne concernée du rejet de sa demande au plus tard 30 jours civils à compter de la date de réception de la demande.

Aux termes de l'article 109, paragraphe 1, de la convention de Schengen, le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le Système d'Information Schengen s'exerce dans le respect du droit de la partie contractante auprès de laquelle elle le fait valoir. Si le droit national le prévoit, l'autorité nationale de contrôle prévue à l'article 114, paragraphe 1, décide si des informations sont communiquées et selon quelles modalités. Une partie contractante qui n'a pas effectué le signalement ne peut communiquer des informations concernant ces données que si elle a donné préalablement à la partie contractante signalante l'occasion de prendre position.

Selon les dispositions relatives à la partie nationale lituanienne du Système d'information Schengen approuvées par l'arrêté n° 1V-324 du 17 septembre 2007 du ministre de l'intérieur de la République de Lituanie, lorsque le signalement relatif à la personne concernée a été émis par une autre partie contractante, le responsable du traitement des données ne peut communiquer à la personne concernée des informations sur ses données à caractère personnel traitées dans la partie nationale du SIS qu'après avoir reçu l'autorisation de la partie contractante signalante.

Lorsqu'il reçoit une demande écrite de la personne concernée visant à obtenir la rectification de ses données à caractère personnel erronées, incomplètes ou inexactes, l'effacement de ses données à caractère personnel ayant fait l'objet d'un traitement illicite ou la suspension du traitement de ses données, le responsable du traitement des données dans la partie nationale du SIS doit transférer immédiatement cette demande à l'institution compétente de la partie contractante et en informer la personne concernée. Après la rectification des données erronées ou inexactes et la mise à jour des données incomplètes par l'institution compétente de la partie contractante, ainsi qu'après leur effacement ou la suspension de leur traitement, le responsable du traitement des données dans la partie nationale du SIS doit en informer immédiatement la personne concernée et les destinataires des données de la partie nationale du SIS auxquels les données erronées, inexactes ou incomplètes ont été transmises.

5. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

State Data Protection Inspectorate
A.Juozapavičiaus str. 6 / Slucko str. 2, LT-09310 Vilnius
Lituanie
Tél. +370 5 279 1445, fax +370 5 261 9494
Adresse électronique: ada@ada.lt
Site web: www.ada.lt

Si la personne concernée n'est pas satisfaite de la réponse qu'elle a reçue du responsable du traitement, c'est-à-dire si celui-ci rejette la demande de la personne concernée de pouvoir exercer son droit d'accès à ses données à caractère personnel, d'obtenir la rectification ou l'effacement de ses données ou la suspension de leur traitement ultérieur, ou si le responsable du traitement n'envoie pas de réponse à la personne concernée dans les 30 jours civils suivant la date de la demande adressée par la personne concernée, celle-ci peut former un recours contre les actes (omissions) du responsable du traitement auprès de l'Inspection nationale de la protection des données dans les trois mois suivant la réception de la réponse du responsable du traitement ou dans les trois mois suivant la date à laquelle expire le délai de réponse. La personne concernée peut joindre des documents (réponse du responsable du traitement à sa demande, etc.) s'ils attestent des faits mentionnés dans son recours, afin de garantir l'efficacité de l'enquête sur ce dernier.

Après avoir reçu le recours de la personne concernée, l'Inspection nationale de la protection des données, conformément à ses compétences, vérifie la licéité du traitement des données à caractère personnel et statue sur les faits exposés dans le recours.

6. Références des principaux textes nationaux applicables

Loi sur la protection juridique des données à caractère personnel
Dispositions relatives à la partie nationale lituanienne du Système d'information Schengen approuvées par l'arrêté n° 1V-324 du 17 septembre 2007 du ministre de l'intérieur de la République de Lituanie.

7. Régime linguistique

Les demandes d'accès, de rectification ou d'effacement doivent être présentées dans la langue nationale (lituanien). Les demandes adressées dans toute autre langue seront examinées conformément à une procédure générale. Elles seront traduites dans la langue nationale (lituanien). La réponse sera rédigée dans la langue nationale (lituanien).

La langue de la procédure d'enquête sur un recours est la langue nationale (lituanien). Tout recours formé par une personne concernée auprès de l'Inspection nationale de la protection des données dans une langue autre que la langue nationale sera traduit dans la langue nationale (lituanien). La décision sur le recours et la réponse donnée au plaignant seront rédigées dans la langue nationale (lituanien).

XVIII. MALTE

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

La personne concernée a un droit d'accès direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès, de rectification ou d'effacement sont à adresser à l'autorité nationale compétente à l'adresse suivante:

Data Protection Officer Insp. Sandro Camilleri
Legal Unit
Police Headquarters
Floriana
Tél: 21224001
Adresse électronique: sandro.camilleri@gov.mt

3. Formalités d'introduction des demandes

Conformément à la législation maltaise, la demande doit être introduite par écrit et signée par la personne concernée. Elle doit être adressée en maltais ou en anglais, les deux langues officielles reconnues par la Constitution maltaise. La réponse doit être adressée dans la langue utilisée par l'auteur de la demande. Les informations doivent être communiquées sans frais et sans délai excessif.

4. Procédure

La convention de Schengen prévoit que le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le Système d'Information Schengen s'exerce dans le respect du droit de l'autorité compétente nationale auprès de laquelle elle le fait valoir.

Après avoir présenté une demande, une personne a le droit de recevoir par écrit des informations conformément aux dispositions générales relatives à la protection des données figurant dans la loi maltaise sur la protection des données (Cap 440). Des informations sous une forme intelligible doivent être communiquées sur les données à caractère personnel effectivement traitées, la source auprès de laquelle les données ont été collectées, la finalité du traitement et les éventuels destinataires des données. Le refus ou la limitation du droit d'accès ne sont autorisés que lorsque cela est justifié pour la répression d'infractions pénales, ou nécessaire pour la protection des personnes concernées ou des libertés d'autres personnes.

En cas de limitation ou de refus, la personne concernée est informée par écrit de cette décision, y compris des motifs de celle-ci, à moins qu'une telle communication ne risque de porter préjudice à une tâche légale de la police ou aux droits et libertés d'autres personnes.

5. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Office of the Data Protection Commissioner
2, Airways House,
High Street
Sliema.
Malte
Tél: +35623287100, fax: +35623287198
Adresse électronique: commissioner.dataprotection@gov.mt
Site web: www.dataprotection.gov.mt

En cas de limitation ou de refus, la personne concernée a le droit de former un recours auprès du commissaire à la protection des données dans un délai de 30 jours à compter de la date à laquelle la décision lui est communiquée ou de la date à laquelle elle peut raisonnablement être réputée connaître la décision.

Lors de l'examen du recours, le commissaire à la protection des données vérifie la décision et s'assure que le refus ou la limitation est raisonnable et fondé(e).

6. Référence du cadre juridique national applicable

Les instruments juridiques applicables sont la loi sur la protection des données (Cap 440) et l'avis juridique 142 de 2004 régissant le traitement des données à caractère personnel dans le secteur de la police.

XIX. PAYS-BAS

1. Nature du droit d'accès

Le droit d'accès aux Pays-Bas est direct. La loi sur les données policières (Wet politiegegevens) est applicable à la partie nationale du Système d'Information Schengen (NSIS). Un droit d'accès est garanti en vertu de l'article 25 de cette loi. Toute personne peut présenter par écrit au délégué à la protection des données de la police nationale (Korps Landelijke Politiediensten) une demande d'accès à ses données à caractère personnel figurant dans le SIS. Le demandeur devrait recevoir une réponse dans un délai de six semaines. Celle-ci contiendra une communication sur le contenu des données, à moins que des motifs de refus de communication ne conduisent à l'application de l'article 27 de la loi sur les données policières. La communication peut être refusée si cela est nécessaire:

a. à la bonne exécution d'une tâche policière;
b. à la protection d'intérêts importants de tiers;
c. dans l'intérêt de la sûreté de l'État.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès aux informations sont à adresser à l'instance suivante:

Korps Landelijke Politiediensten
Attention of the data protection officer
Postbus 3016
NL – 2700 KX Zoetermeer
Tél.: ++31-79-345 90 62
Fax: ++31-79-345 90 10

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Lorsqu'une personne introduit une demande d'information, le délégué à la protection des données prend contact avec elle au sujet des modalités de traitement de sa demande. Une copie de la carte d'identité doit être fournie. Un montant de 4,50 euros peut être exigé pour ce traitement.
Le délégué à la protection des données examine s'il peut accéder à la demande ou s'il existe des motifs juridiques qui justifient son rejet.

Les demandes concernant les signalements effectués en vertu de l'article 96 seront transmises à l'autorité responsable de cette catégorie de signalements: le service d'immigration et de naturalisation du ministère de la justice.
Les demandes concernant tous les autres signalements seront traitées par les autorités (policières) compétentes.

Après avoir pris connaissance des informations qui lui ont été transmises, la personne concernée peut introduire une demande visant à ce que ses données soient complétées, rectifiées ou effacées.

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Si le traitement de la demande donne lieu à un litige, une demande de médiation peut être adressée à l'instance suivante:

College Bescherming Persoonsgegevens
Postbus 93374
NL – 2509 AJ Den Haag
T2l.: ++31(0)708888500
Fax: ++31(0)708888501
Adresse électronique: info@cbpweb.nl
Site web: www.cbpweb.nl

Cette demande doit être présentée dans un délai de six semaines à compter de la réception des informations.
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 de Schengen et à la loi.
Comme solution de remplacement, ou si la médiation du CBP a échoué, une requête peut être adressée au tribunal d'arrondissement (section administrative) afin qu'il examine l'affaire et rende un jugement.

XX. NORVÈGE

1. Nature du droit d'accès

Le droit d'accès est direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Kriminalpolitisentralen
(Service national d'enquête en matière criminelle - NCIS)
PO Box 8163 Dep.
NO-0034 OSLO
Tél.: ++47 23 20 80 00
Adresse électronique:
Fax: + +47 23 20 88 80
Site web: www.kripos.no

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

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

4. Coordonnées et rôle éventuel de l'autorité chargée de la protection des données

Datatilsynet
PO Box 8177 Dep.
NO-0034 OSLO
Tél.: +47 22 39 69 00
Fax: + 47 22 42 23 50
Adresse électronique: postkasse@datatilsynet.no
Site web: www.datatilsynet.no

5. Résultats escomptés des demandes d'accès et contenu des informations communiquées

C'est l'autorité gestionnaire des fichiers (SNRC) 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 l'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 la loi relative au SIS (section 15) s’applique, d'autres raisons doivent toujours être 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 (LOV 1999-07-16-66)

Dispositions de la loi n° 66 du 16 juillet 1999 concernant le Système d'Information Schengen (dispositions relatives au SIS).

XXI. POLOGNE

1. Nature du droit d'accès

Le droit d'accès aux informations est direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Conformément à la loi du 24 août 2007 relative à la participation de la République de Pologne au Système d'information Schengen et au Système d'information sur les visas, le responsable du traitement des données en Pologne dans le cadre du Système d'information Schengen est le chef des services de police. C'est à lui qu'il convient d'adresser les demandes d'accès ou de rectification.

Adresse pour la correspondance:
General Headquarters of the Polish Police (KGP)
Central Technical Authority KSI
02-514 Warsaw
148/150 Puławska Street
Pologne

Pour la consultation du contenu d'une demande d'accès à des données à caractère personnel, il est possible de nous contacter par téléphone ou par voie électronique:

tél.: +48 (22) 601-53-29
tél.: +48 (22) 601-53-15
adresse électronique: cot.admin.ksi@policja.gov.pl

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Toute personne a le droit d'obtenir des informations complètes sur les données à caractère personnel la concernant qui sont traitées dans des fichiers de données.

En vertu de l'article 32, paragraphe 5, de la loi du 29 août 1997 relative à la protection des données à caractère personnel (Journal officiel de 2002, n° 101, point 926 avec les modifications ultérieures), la personne concernée peut exercer son droit d'obtenir des informations *tous les six mois*.

La demande d'accès est gratuite.

Selon l'article 32 (1-5a) de la loi relative à la protection des données à caractère personnel, la personne concernée peut demander les informations ci-après concernant le traitement de ses données à caractère personnel:

- des données la concernant figurent-elles dans le système?
- depuis combien de temps les données sont-elles traitées?
- quelle est la source des données?
- comment les données sont-elles diffusées?
- quelle est la finalité et le champ du traitement des données?
- dans quelle mesure et à qui les données ont-elles été communiquées?

Le responsable du traitement répondra à la demande d'informations dans un délai de 30 jours. Pour obtenir les informations, une demande doit être présentée par écrit en polonais.

La demande d'informations devrait mentionner:

1. le nom et le prénom du demandeur,
2. le numéro d'identification national polonais (le cas échéant),
3. la nationalité,
4. la date et le lieu de naissance,
5. la photocopie d'un document d'identification comportant une photographie reconnaissable,
6. le lieu de résidence (pays, ville, rue et numéro de l'habitation),
7. l'objet de la demande,
8. la signature de la personne introduisant la demande.

Conformément à l'article 32 de la loi du 14 juin 1960 établissant le Code de procédure administrative (Journal officiel de 2000, n° 98, point 1071 avec les modifications ultérieures), une partie peut être représentée dans une procédure administrative par un plénipotentiaire, à moins que la nature des activités ne requiert d'intenter une action en personne. L'article 33 du Code fixe les règles procédurales concernant la procuration, c'est-à-dire:

- le plénipotentiaire peut être une personne physique dotée de la capacité juridique;
- la procuration doit être notifiée par écrit;
- le plénipotentiaire dépose la procuration originale ou une copie certifiée conforme.

Un avocat, un conseil juridique ou un conseil en brevets peuvent authentifier eux-mêmes la copie d'une procuration qui leur est donnée.

Refus de communiquer des informations sur les données à caractère personnel faisant l'objet d'un traitement

En vertu de l'article 30 de la loi relative à la protection des données à caractère personnel, le responsable du traitement peut refuser d'autoriser l'accès lorsque cela:

1. résulterait en la diffusion d'informations relevant du secret d'État;
2. constituerait une menace pour la sûreté ou la défense de l'État, la vie ou la santé humaine ou la sécurité et l'ordre public;
3. constituerait une menace pour des intérêts économiques ou financiers fondamentaux de l'État;
4. résulterait en une atteinte majeure aux intérêts personnels des personnes concernées ou de tiers.

Le droit d'obtenir la rectification des données et de demander la suspension de leur traitement ou leur effacement

La personne concernée peut demander au responsable du traitement de compléter, mettre à jour, rectifier ou effacer ses données ou de suspendre leur traitement de façon temporaire ou permanente. Cependant, elle doit prouver que les données sont incomplètes, obsolètes ou inexactes, qu'elles ont été collectées en violation de la loi ou que leur traitement n'est plus nécessaire aux fins pour lesquelles elles ont été collectées.

La procédure de demande est menée conformément aux dispositions du Code de procédure administrative.

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Pour garantir un niveau adéquat de protection juridique aux personnes dont les données sont conservées dans le Système d'information Schengen, l'inspecteur général pour la protection des données à caractère personnel vérifie que l'utilisation des données ne viole pas les droits des personnes concernées. Ce contrôle est exercé conformément aux lois relatives à la protection des données à caractère personnel.

Adresse pour la correspondance:
Bureau of the Inspector General for Personal Data Protection (GIODO)
2 Stawki Street
00-193 Warsaw
Pologne
tél. +48 (22) 860-73-93
fax +48 (22) 860-70-86
http://www.giodo.gov.pl
kancelaria@giodo.gov.pl

Toute personne dont les données sont traitées dans le Système d'information Schengen a le droit de former un recours auprès de l'inspecteur général pour la protection des données à caractère personnel en ce qui concerne la mise en œuvre des dispositions relatives à la protection des données à caractère personnel.

5. Références des principaux textes nationaux applicables

- Loi du 24 août 2007 relative à la participation de la République de Pologne au Système d'information Schengen et au Système d'information sur les visas
- Loi du 29 août 1997 relative à la protection des données à caractère personnel
- Loi du 14 juin 1960 établissant le Code de procédure administrative
- Loi du 7 octobre 1999 relative à la langue polonaise.

XXII. PORTUGAL

1. Nature du droit d'accès

Les citoyens ont un droit d'accès indirect aux données figurant dans le SIS. Ce droit est garanti par l'autorité nationale de protection des données (APD).

2. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Les demandes doivent être faites par écrit, au moyen de l'un des deux formulaires prévus à cet effet, l'un pour le droit d'accès et l'autre pour le droit de rectification ou d'effacement. Ces formulaires sont disponibles en portugais, en anglais et en français sur le site Internet de l'APD. Les demandes doivent être déposées en personne au guichet de l'APD ou par courrier. Le demandeur doit présenter un document prouvant son identité (passeport) ou envoyer en annexe à sa demande une copie certifiée conforme de son passeport afin d'avoir accès aux données le concernant. L'exercice du droit d'accès est gratuit.

3. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Comissão Nacional de Protecção de Dados
Rua de S. Bento, 148, 3º
1200-821 Lisboa
PORTUGAL
Tél.: (+351) 213 928 400
Fax: (+351) 213 976 832
Site Internet: http://www.cnpd.pt

En ce qui concerne la communication d'informations, il est tenu compte de l'existence éventuelle d'informations susceptibles de nuire à la prévention de la criminalité et aux enquêtes judiciaires ou de constituer une menace pour la sûreté de l'État.
La communication des informations est effectuée par l'autorité nationale de protection des données.

4. Références des principaux textes nationaux applicables

Les actes législatifs applicables sont la loi n° 67/98 du 26 octobre 1998 (article 11, paragraphe 2) et la loi n° 2/94 du 19 février 1994.

XXIII. SLOVAQUIE

1. Nature du droit d'accès

L'article 109 de la Convention prévoit que toute personne a le droit d'accéder aux données la concernant qui sont intégrées dans le Système d'information Schengen (SIS). Ce droit est exercé conformément au droit national de la partie contractante. Dans le cas de la République slovaque, l'intéressé a un droit d'accès direct aux données le concernant.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès sont à adresser au ministère de l'Intérieur, qui est le responsable du traitement des données:

MINISTERSTVO VNÚTRA SLOVENSKEJ REPUBLIKY

Pribinova 2, 812 72 Bratislava
Slovenská republika
Tél.: 02/5094 1111
Fax: 02/5094 4397
envoyer un courriel
Site Internet: http://www.minv.sk

3. Formalités d'introduction des demandes: Informations et documents à fournir

En vertu de l'article 69 quater de la loi n° 171/1993 Coll. relative aux forces de police, chacun peut s'adresser par écrit au ministère de l'Intérieur afin de connaître les données à caractère personnel traitées le concernant. Parallèlement, le responsable du Système d'information Schengen est tenu de fournir gratuitement ces informations dans les trente jours suivant la réception de la **demande écrite.**

Le formulaire standard de demande est disponible sur le site Internet du ministère de l'Intérieur. La personne concernée est tenue de fournir certains renseignements personnels (nom, prénom, adresse permanente, lieu et date de naissance, nationalité) ainsi qu'une copie de sa carte d'identité ou de son passeport afin de prouver son identité.

4. Résultats escomptés des demandes d'accès et contenu des informations communiquées

La communication au demandeur des données à caractère personnel figurant dans les systèmes de la police s'effectue en application l'article 69 quater de la loi n° 171/1993 Coll. relative aux forces de police.
Dans le cas du Système d'information Schengen, si un signalement a été effectué au titre des articles 95 à 98 et de l'article 100 de la Convention de Schengen, le demandeur est informé des données le concernant (au minimum, les données suivantes: nom, prénom, date et lieu de naissance, sexe, nationalité et motif du signalement, c'est-à-dire la finalité du traitement de ses données à caractère personnel).

Si le droit d'accès à des informations concerne un signalement qui n'a pas été effectué par la République slovaque, le pays à l'origine de ce signalement doit pouvoir faire part de sa position concernant la possibilité de communiquer ces données au demandeur.
Si le signalement a été effectué en application de l'article 99 de la Convention de Schengen, le demandeur se verra probablement refuser la communication de ces données (le traitement a été effectué pour des raisons de sécurité nationale ou dans le cadre d'une enquête concernant des infractions particulièrement graves).

En d'autres termes, la communication des informations à la personne concernée est refusée si elle peut nuire à l'exécution de la tâche légale consignée dans le signalement ou pour la protection des droits et libertés d'autrui. Elle est refusée dans tous les cas durant la période de signalement aux fins de surveillance discrète.

En vertu de l'article 69 quater de la loi n° 171/1993 Coll. relative aux forces de police, la personne concernée a également le droit de **demander par écrit** au ministère de l'Intérieur la correction ou l'effacement des données à caractère personnel la concernant qui sont traitées dans le Système d'information Schengen (le formulaire standard de demande d'effacement/de correction des données est disponible sur le site Internet du ministère de l'Intérieur).

Si une personne soupçonne que des données à caractère personnel la concernant sont traitées sans autorisation, elle peut, en vertu de l'article 20, paragraphe 6, de la loi sur la protection des données, déposer **un recours** directement auprès de l'Office de la protection des données à caractère personnel de la République slovaque, qui vérifiera s'il y a violation des droits de la personne concernée dans le traitement et l'utilisation des données à caractère personnel figurant dans le Système d'information Schengen.

Le dépôt des recours est régi par l'article 45 de la loi n° 428/2002 Coll. relative à la protection des données à caractère personnel (le formulaire standard à utiliser pour déposer un recours est également disponible sur le site Internet du ministère de l'Intérieur).

5. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Úrad na ochranu osobných údajov Slovenskej republiky
Odborárske nám. 3
817 60 Bratislava 15
Slovenská republika
Tél.: +421 2 502 39 418
Fax: +421 2 502 39 441
Courriel: mstatny.dozor@pdp.gov.sk
Site Internet: http://www.dataprotection.gov.sk

6. Références des principaux textes nationaux applicables

Loi n° 428/2002 Coll. relative à la protection des données à caractère personnel (modifiée).

XXIV. SLOVÉNIE

1. Nature du droit d'accès

Il existe un droit d'accès direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes peuvent être présentées par écrit ou formulées oralement pour enregistrement auprès de la police (ministère de l'Intérieur), à l'adresse suivante:

Policija, Ministrstvo za notranje zadeve
Štefanova 2
1501 Ljubljana
Slovénie
Fax: + 386 1 428 47 33
Courriel: mgp.mnz@gov.si

Les demandes peuvent également être déposées aux points de passage frontaliers, auprès des administrations ainsi que des services diplomatiques et consulaires slovènes à l'étranger. Elles sont immédiatement transmises à la police.

Le formulaire de demande d'information sur les données figurant dans la partie nationale slovène du Système d'information Schengen (N.SIS) est disponible en anglais à l'adresse suivante: http://www.ip-rs.si/index.php?id=346

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

En Slovénie, l'exercice du droit par une personne à consulter ses propres données à caractère personnel est régi par la loi relative à la protection des données à caractère personnel (articles 30 et 31) et par la loi relative au commissaire à l'information.

En vertu de l'article 30 de la loi relative à la protection des données à caractère personnel, la police, qui est un organe subordonné au ministère de l'Intérieur et le responsable du traitement, est tenue

1. de permettre la consultation du fichier du SIS;
2. de certifier au demandeur si des données le concernant font l'objet d'un traitement et lui permettre de consulter les données à caractères personnel le concernant qui figurent dans la partie nationale du SIS, et de fournir une transcription ou une copie de ces données;

3. de fournir au demandeur un extrait des données à caractère personnel le concernant qui figurent dans la partie nationale du SIS;
4. de fournir une liste des destinataires auxquels les données à caractère personnel ont été transmises, en indiquant la date à laquelle ces données ont été communiquées, ainsi que les critères ayant motivé cette communication et sa finalité;
5. de fournir des informations relatives aux sources sur lesquelles se fondent les données qui figurent dans le SIS concernant la personne en question, ainsi que la méthode de traitement;
6. de fournir des informations sur la finalité du traitement et sur le type de données à caractère personnel traitées dans le SIS, ainsi que toutes les explications nécessaires à cet égard;
7. d'expliquer les procédures techniques et logiques de prise de décision.

Le traitement de cette demande est actuellement gratuit. Le demandeur peut se voir imputer uniquement les frais de photocopie, comme prévu dans les règles relatives à l'imputation des coûts liés à l'exercice du droit d'accès des personnes aux données à caractère personnel les concernant.

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Informacijski pooblaščenec
(Commissaire à l'information)
Vošnjakova 1
p.p. 78
1001 Ljubljana
Slovénie
Tél.: ++ 386 1 230 97 30
Fax: ++ 386 1 230 97 78
Courriel: mgp.ip@ip-rs.si
Site Internet: http://www.ip-rs.si

En cas de recours formé par un demandeur à la suite du rejet d'une demande de consultation des données à caractère personnel le concernant ou en cas de refus de réponse par l'autorité compétente, la décision est de la compétence du commissaire à l'information.

Les demandeurs qui considèrent que l'un de leurs droits a été violé en ce qui concerne une demande d'accès peuvent introduire un recours auprès du commissaire à l'information. Lorsque ce dernier reçoit le recours, il le transmet au responsable du fichier afin que celui-ci puisse émettre toute déclaration qu'il estime utile. Le commissaire à l'information rend ensuite une décision concernant le recours et la transmet aux intéressés, après avoir pris connaissance des déclarations, des rapports, des preuves et des autres pièces du dossier, y compris, si nécessaire, l'inspection des fichiers et des entretiens avec la personne concernée et le responsable du fichier.

Le traitement de ce recours est actuellement gratuit.

5. Résultats escomptés des demandes d'accès et contenu des informations communiquées

Si les données relatives à la personne concernée figurent dans le fichier du SIS et si la demande est approuvée, le responsable du fichier fournit sous la forme demandée à l'intéressé les données le concernant. La police doit permettre à l'intéressé de consulter les données le concernant, d'en obtenir une transcription ou une copie ou d'obtenir un certificat dans un délai maximum de quinze jours à compter de la date de réception de la demande ou, dans les mêmes délais, informer par écrit l'intéressé du motif du rejet de sa demande. La police est tenue de fournir à l'intéressé l'extrait mentionné au point 3 ci-dessus, la liste visée au point 4, les informations indiquées aux points 5 et 6 ainsi que les explications visées au point 7 dans les 30 jours suivant la réception de la demande ou, dans les mêmes délais, de l'informer par écrit du motif du rejet de sa demande.

De même, le droit des personnes à consulter les données à caractère personnel les concernant peut être limité à titre exceptionnel, conformément à l'article 36 de la loi relative à la protection des données à caractère personnel, afin de protéger la souveraineté nationale et la défense nationale, la sûreté nationale et l'ordre constitutionnel de l'État, la sécurité, les intérêts politiques et économiques du pays ou d'assurer l'exercice des compétences de police, la prévention, la recherche, la détection et la poursuite d'infractions pénales et d'infractions légères, la découverte et la répression de violations des normes éthiques pour certaines professions, pour des raisons monétaires, budgétaires ou fiscales, aux fins du contrôle de la police et de la protection des personnes auxquelles ces données à caractère personnel se rapportent ou des droits et libertés d'autres personnes. Ces limitations ne peuvent être appliquées que dans la mesure nécessaire et aux fins pour lesquelles elles ont été prévues.

6. Références des principaux textes nationaux applicables

- Loi relative à la protection des données à caractère personnel (Journal officiel de la République de Slovénie n° 94/2007, texte officiel consolidé). Une traduction non officielle en anglais de cette loi est disponible à l'adresse Internet suivante: http://www.ip-rs.si/index.php?id=339;
- Loi relative au commissaire à l'information (Journal officiel de la République de Slovénie n° 113/2005). Une traduction non officielle en anglais de cette loi est disponible à l'adresse Internet suivante: http://www.ip-rs.si/index.php?id=325;
- Règles relatives à l'imputation des coûts liés à l'exercice du droit d'accès des personnes aux données à caractère personnel les concernant (Journal officiel de la République de Slovénie n° 85/2007). Seule la version en langue slovène est disponible à l'adresse Internet suivante: http://www.ip-rs.si/zakonodaja/zakon-o-varstvu-osebnih-podatkov/pravilnik-o-zaracunavanju-stroskov-pri-izvrsevanju-pravice-posameznika-do-seznanitve-z-lastnimi-osebnimi-podatki/.

XXV. ESPAGNE

1. Nature du droit d'accès

La personne concernée a un droit d'accès direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès aux informations sont à adresser à l'instance suivante:

Secretaría de Estado de Seguridad
Ministerio del Interior
Amador de los Ríos, 2
E – 28010 Madrid
Tél.: 060
Fax: ---
Courriel: estafeta@mir.es
Site Internet: http://www.mir.es

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Toutes les demandes d'accès doivent être adressées par écrit au responsable du traitement (Secretaria de Estado de Seguridad del Ministerio del Interior) par tout moyen permettant de prouver l'envoi et la réception de la demande.

Il n'existe pas de formulaire standard de demande ni de prescriptions formelles. Néanmoins, conformément aux procédures administratives générales, la demande devrait comporter une description complète de la requête et être accompagnée d'une photocopie d'un document prouvant l'identité de la personne concernée, à savoir la carte nationale d'identité ou le passeport. En outre, la personne concernée peut joindre une copie de tout document qu'elle estime pertinent pour justifier sa requête.

Cette procédure est gratuite.

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Agencia Española de Protección de Datos (Autorité chargée de la protection des données)
C/ Jorge Juan, 6
E - 28001 – Madrid
Tél.: + 34 901 100 099
Fax: + 34 91 445 56 99
Courriel: ciudadano@agpd.es
Site Internet: http://www.agpd.es

Comme indiqué précédemment, la personne concernée a un droit d'accès direct. Toutefois, elle dispose également d'un droit d'accès indirect par l'intermédiaire de l'autorité espagnole de protection des données (appelée ci-après "APD espagnole") lorsqu'un responsable du traitement ne répond pas à une demande d'accès formulée par une personne concernée ou lorsque la réponse fournie n'est pas satisfaisante. Dans les deux cas, la personne concernée peut introduire un recours auprès de l'APD espagnole. En vertu de la section 117 du décret royal 1720/2007 approuvant le règlement d'application de la loi organique n° 15/1999 relative à la protection des données à caractère personnel, la procédure est engagée à la demande de la personne concernée, qui expose clairement les éléments motivant son recours et précise les dispositions de la loi relative à la protection des données à caractère personnel qui, selon elle, ont été violées.

Dès réception du recours par l'APD espagnole, une procédure de protection des droits des personnes est engagée. En application de cette procédure, l'APD espagnole transmet le recours au responsable du traitement afin que ce dernier puisse faire valoir tous les arguments qu'il juge utiles pour justifier le rejet de la demande d'accès ou la réponse adressée au demandeur.

Ces observations éventuelles sont transmises au demandeur qui peut formuler des déclarations ou observations complémentaires. Celles-ci sont à leur tour transmises au responsable du traitement, qui a la possibilité de fournir des explications sur sa décision ainsi que sur les observations et déclarations formulées par le demandeur.

Une fois en possession des arguments, déclarations et documents, le directeur de l'APD espagnole rend une décision sur le recours introduit.

Il est important de souligner que la décision doit être rendue et notifiée dans les six mois suivant la date de réception du recours par l'APD espagnole.

Si la décision est rendue en faveur du demandeur, l'APD espagnole en informe le responsable du traitement, qui doit permettre à la personne concernée d'exercer son droit d'accès dans les dix jours suivant la notification. En outre, le responsable du traitement est tenu de prouver par écrit à l'APD espagnole, dans les mêmes délais, qu'il s'est conformé à sa décision.

5. Résultats escomptés des demandes d'accès et contenu des informations communiquées

Si le signalement a été effectué par les autorités espagnoles, il appartient au responsable du traitement de décider du contenu des informations communiquées aux demandeurs. En général, la personne concernée reçoit une copie des documents administratifs comportant les données à caractère personnel figurant dans le fichier.

Toutefois, si le signalement a été effectué par les autorités d'un autre État Schengen, le responsable du traitement est tenu d'informer son homologue dans le pays concerné du recours introduit, conformément au principe de coopération entre les autorités nationales en matière de protection des données à caractère personnel. Il appartient alors aux autorités de l'autre État Schengen de décider quelles informations peuvent être communiquées à la personne concernée.

6. Régime linguistique

Toute personne concernée qui souhaite engager une procédure visant à exercer son droit d'accès en Espagne devrait s'adresser aux autorités en Espagnol.

XXVI. SUÈDE

1. Nature du droit d'accès

Il existe un droit d'accès direct.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Les demandes d'accès doivent être adressées à la Direction de la police nationale (Rikspolisstyrelsen), qui est l'autorité responsable de la partie suédoise du Système d'information Schengen.

Rikspolisstyrelsen
Box 12256
Polhemsgatan 30
S - 102 26 Stockholm
Tél.: ++46 (0)8-401 90 00
Fax: ++46 (0)8-401 99 90
Courriel: mrikspolisstyrelsen@polisen.se
Site Internet: http://www.polisen.se

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Les demandes doivent être adressées par écrit à la Direction de la police nationale et signée personnellement par le demandeur. En général, il doit être répondu aux demandes d'accès dans un délai d'un mois. Les demandeurs peuvent accéder gratuitement aux informations une fois par année civile.

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Datainspektionen
Box 8114
Fleminggatan 14, 9th floor
S-104 20 Stockholm
Tél.: ++46 (0)8-657 61 00
Fax: ++46 (0)8-652 86 52
Courriel: mdatainspektionen@datainspektionen.se
Site Internet: http://www.datainspektionen.se/

Le Bureau d'inspection des données contrôle que le traitement des données à caractère personnel est conforme aux règles fixées par la loi relative aux données à caractère personnel ainsi que par les autres textes législatifs pertinents en matière de protection des données. Ce bureau peut effectuer un contrôle sur la base d'une réclamation ou de sa propre initiative. Les personnes qui contestent la manière dont leur demande d'accès aux informations figurant dans le SIS a été traitée peuvent introduire un recours auprès du Bureau d'inspection des données. Ce recours pourra donner lieu à une enquête visant à vérifier si les règles relatives au droit d'accès ont bien été respectées. Les décisions de la Direction de la police nationale concernant le droit d'accès sont également susceptibles de recours devant le tribunal administratif.

5. Résultats escomptés des demandes d'accès et contenu des informations communiquées

La décision de communiquer les informations est fondée sur les dispositions de la loi sur la confidentialité (1980:100), qui peut interdire la communication de certaines données. Si la communication des données est autorisée, c'est la Direction de la police nationale qui est compétente pour le faire.

6. Références des principaux textes nationaux applicables

Législation applicable: sections 26 et 27 de la loi relative aux données à caractère personnel (1998:204) et section 8 de la loi relative au Système d'information Schengen (2000:344).

7. Régime linguistique

Il n'existe pas de règles particulières concernant cette question en Suède. Une demande formulée en anglais serait acceptée.

XXVII. SUISSE

1. Nature du droit d'accès

Il existe un droit d'accès direct. L'autorité compétente pour le traitement des demandes concernant l'accès aux données à caractère personnel figurant dans le SIS est le conseiller à la protection des données de l'Office fédéral de la police suisse.

2. Coordonnées de l'autorité à laquelle il convient d'adresser les demandes d'accès

Office fédéral de la police
Conseiller à la protection des données ou Bureau SIRENE
Nussbaumstrasse 29
CH-3003 Berne
Site Internet: http://www.fedpol.ch/

3. Formalités d'introduction des demandes: informations et documents à fournir et frais éventuels

Les demandes concernant les données à caractère personnel traitées dans le SIS doivent être adressées directement au Conseiller à la protection des données de l'Office fédéral de la police (les demandes se font uniquement par écrit et doivent être accompagnées d'une copie de la carte d'identité ou du passeport en cours de validité).

4. Coordonnées et rôle éventuel de l'autorité nationale chargée de la protection des données

Préposé fédéral à la protection des données et à la transparence (PFPDT)
Feldeggweg 1,
CH-3003 Berne
Tél.: +41(0)31 322 43 95,
Fax: +41-(0)31 325 99 96
Site Internet: http://www.edoeb.admin.ch

Seules les demandes de vérification sont à adresser au Préposé fédéral à la protection des données et à la transparence (PFPDT), qui est le niveau fédéral de l'autorité suisse de protection des données.

ANNEXES (MODELES DE LETTRES)

Annexe 1

Modèle de lettre de demande d'accès

Dénomination et adresse de l'autorité compétente

JJ MM XXXX,

Lieu

Madame, Monsieur,

conformément à l'article 109 de la Convention de Schengen,
Je, soussigné(e) _____ (prénom, nom de famille), de nationalité _____, né(e) à _____ le _____, domicilié(e) à _____ (adresse), demande à avoir accès aux données à caractère personnel me concernant qui sont intégrées dans le Système d'information Schengen.

Veuillez trouver ci-joint les documents suivants:
1. copie d'un document d'identité en cours de validité au sens de la législation nationale de l'État Schengen (passeport/carte d'identité/permis de conduire/(autre document d'identité en cours de validité);
2. copie de l'autorisation légale de représenter le demandeur;
3. autre.

Le demandeur / Le représentant légal

(Signature)

Annexe 2

Modèle de lettre de demande de vérification

Dénomination et adresse de l'autorité compétente.

JJ MM XXXX,

Lieu

Madame, Monsieur,

conformément à l'article 114, paragraphe 2, de la Convention de Schengen,
Je, soussigné(e) _____(prénom, nom de famille), de nationalité _____, né(e) à _____ le _____, domicilié(e) à _____ (adresse), demande la vérification des données à caractère personnel me concernant qui sont intégrées dans le Système d'information Schengen ainsi que de l'utilisation qui en est faite.

Veuillez trouver ci-joint les documents suivants:
1. copie d'un document d'identité en cours de validité au sens de la législation nationale de l'État Schengen (passeport/carte d'identité/permis de conduire/(autre document d'identité en cours de validité);
2. copie de l'autorisation légale de représenter le demandeur;
3. autre.

Le demandeur / Le représentant légal

(Signature)

Annexe 3

Modèle de lettre de demande de correction

Dénomination et adresse de l'autorité compétente.

JJ MM XXXX,

Lieu

Madame, Monsieur,

conformément à l'article 110 de la Convention de Schengen,
Je, soussigné(e) _____(prénom, nom de famille), de nationalité _____, né(e) à _____ le _____, domicilié(e) à _____ (adresse), demande la correction de données à caractère personnel erronées me concernant qui sont intégrées dans le Système d'information Schengen / la suppression des données à caractère personnel me concernant qui figurent de manière illégale dans le Système d'information Schengen. Les données à caractère personnel me concernant doivent être corrigées/supprimées pour la raison suivante:

_____

_____

_____

_____

Veuillez trouver ci-joint les documents suivants:

1. copie d'un document d'identité en cours de validité au sens de la législation nationale de l'État Schengen (passeport/carte d'identité/permis de conduire/(autre document d'identité en cours de validité);
2. copie de l'autorisation légale de représenter le demandeur;
3. autre.

Le demandeur / Le représentant légal

(Signature)