




Informations de base	
2005/0232(CNS) CNS - Procédure de consultation Décision	Procédure terminée
Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) Abrogation 2018/0152A(COD) Modification 2017/0351(COD) Subject 7.10.04 Franchissement et contrôles aux frontières extérieures, visas 7.30.05.01 Europol, CEPOL 7.30.20 Lutte contre le terrorisme	

Acteurs principaux			
Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	<div>LIBE</div> Libertés civiles, justice et affaires intérieures	LUDFORD Baroness Sarah (ALDE)	23/01/2006
Conseil de l'Union européenne	Formation du Conseil	Réunions	Date
	Justice et affaires intérieures(JAI)	2696	2005-12-01
	Justice et affaires intérieures(JAI)	2794	2007-04-19
	Justice et affaires intérieures(JAI)	2807	2007-06-12
Commission européenne	DG de la Commission	Commissaire	
	Justice et consommateurs	BARROT Jacques	

Evénements clés			
Date	Evénement	Référence	Résumé
24/11/2005	Publication de la proposition législative	COM(2005)0600 	Résumé
01/12/2005	Débat au Conseil		
16/02/2006	Annonce en plénière de la saisine de la commission		
19/04/2007	Débat au Conseil		Résumé
14/05/2007	Vote en commission		Résumé
21/05/2007	Dépôt du rapport de la commission, 1ère lecture/lecture unique	A6-0195/2007	

06/06/2007	Débat en plénière		
07/06/2007	Décision du Parlement	T6-0229/2007	Résumé
07/06/2007	Résultat du vote au parlement		
12/06/2007	Adoption de l'acte par le Conseil suite à la consultation du Parlement		Résumé
12/06/2007	Fin de la procédure au Parlement		
13/08/2008	Publication de l'acte final au Journal officiel		


Informations techniques	
Référence de la procédure	2005/0232(CNS)
Type de procédure	CNS - Procédure de consultation
Sous-type de procédure	Note thématique
Instrument législatif	Décision
Modifications et abrogations	Abrogation 2018/0152A(COD) Modification 2017/0351(COD)
Base juridique	Traité sur l'Union européenne (après Amsterdam) M 034-p2c Traité sur l'Union européenne (après Amsterdam) M 030-p1
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/6/32176

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE370.254	10/03/2006	
Amendements déposés en commission		PE372.109	10/05/2007	
Rapport déposé de la commission, 1ère lecture/lecture unique		A6-0195/2007	21/05/2007	
Texte adopté du Parlement, 1ère lecture/lecture unique		T6-0229/2007	07/06/2007	Résumé

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2005)0600 	24/11/2005	Résumé

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
		N6-0058/2006		

EDPS	Document annexé à la procédure	JO C 097 25.04.2006, p. 0006-0010	20/01/2006	Résumé
------	--------------------------------	-----------------------------------	------------	--------

Informations complémentaires		
Source	Document	Date
Commission européenne	EUR-Lex	

Acte final	
Décision 2008/0633 JO L 218 13.08.2008, p. 0129	Résumé

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 24/11/2005 - Document de base législatif

OBJECTIF : permettre aux autorités compétentes des États membres en matière de sécurité intérieure et à EUROPOL de consulter le VIS en vue de prévenir et de lutter contre le terrorisme et les formes graves de criminalité.

ACTE PROPOSÉ : Décision du Conseil.

CONTEXTE : Dans le cadre de la mise en place progressive d'un Espace de liberté, de sécurité et de justice (ELSJ), l'Union européenne garantit la libre circulation des personnes mais aussi un niveau élevé de sécurité. Dans ce contexte, une priorité absolue a été accordée au développement et à l'établissement d'un système d'information sur les visas (VIS) en tant que système d'échange de données sur les visas entre les États membres, système qui a été créé le 8 juin 2004, avec l'adoption par le Conseil de la décision 2004/512/CE portant création du VIS (voir fiche de procédure CNS /2004/0029). Toutefois, la poursuite du développement et de l'établissement du VIS, notamment dans le domaine de la sécurité intérieure, y compris la lutte contre le terrorisme, requiert la mise en place d'un cadre juridique global complétant le règlement en vigueur, et ce, dans le strict respect des règles relatives à la protection des données à caractère personnel. C'est précisément l'objet de la présente proposition de décision.

CONTENU : La proposition vise à créer la base juridique nécessaire, dans le cadre du titre VI du traité sur l'Union européenne, pour **permettre aux autorités des États membres compétentes en matière de sécurité intérieure et à EUROPOL d'accéder au système d'information sur les visas (VIS)** et pour fixer les conditions de cet accès. Cela leur permettra de consulter le VIS aux fins de la prévention et de la détection des infractions terroristes et des formes de criminalité et infractions relevant de la compétence d'EUROPOL conformément à l'article 2 de la convention EUROPOL (« infractions pénales graves »), ainsi qu'aux fins des enquêtes en la matière.

Techniquement, seules les autorités définies à l'annexe I de la proposition seraient autorisées à consulter les informations requises et selon des modalités clairement définies à la proposition (en particulier, dans le respect le plus strict de la protection des données à caractère personnel). Pour ce faire, chaque État membre auquel le règlement VIS est déjà applicable devra désigner une autorité nationale unique qui deviendra son point d'accès national et central au VIS (chaque point d'accès central sera ainsi chargé de consulter le VIS pour le compte des autorités compétentes de la sécurité intérieure de l'État dont il dépend). L'annexe II détermine, quant à elle, toutes les unités centrales des États membres qui peuvent consulter les données du VIS.

La proposition fixe en outre toutes les conditions techniques de l'accès aux données du VIS :

- conditions d'accès spécifiques pour les États membres auxquels le règlement VIS est applicable : dans les limites de leurs pouvoirs respectifs, ces autorités devront se conformer à une série de règles et conditions pour pouvoir accéder aux données du VIS (en particulier, passage par un point d'accès central et consultation au cas par cas après réception d'une demande de consultation dûment motivée pour des raisons de prévention de terrorisme, d'enquêtes....);
- conditions d'accès spécifiques pour les États membres auxquels le règlement VIS n'est pas applicable : dans les mêmes conditions que celles prévues ci-avant, les autorités des États membres qui n'ont pas accès au VIS devront demander aux autorités compétentes d'un État membre qui a accès au VIS et à son point d'accès national, la possibilité d'accéder aux données du VIS qui l'intéressent, après demande dûment motivée;

- conditions d'accès spécifiques pour EUROPOL : dans les conditions déjà prévues par la proposition *mutatis mutandis* et à condition que cet accès soit justifié dans le cadre des compétences d'EUROPOL.

La proposition énumère les règles de **protection des données à caractère personnel** auxquelles la présente proposition devra obéir (en particulier, interdiction de transmettre des informations recueillies dans la cadre de la mise en œuvre de la présente proposition à des autorités autres que celles désignées par la proposition et dans le cadre strict imposé par la décision). À noter que des dispositions sont prévues en vue de créer un système de relevé des opérations de traitement des données résultant de la consultation du VIS, en vue de contrôler la légalité de la transmission des données.

La proposition fixe également les modalités de suivi et d'évaluation du fonctionnement de la présente proposition.

Elle fixe enfin les modalités de participation au VIS pour certains États membres ne participant pas normalement à la politique commune en matière de visas (Royaume-Uni et Irlande, qui seraient associés à la mise en œuvre de la proposition) ou pour les pays associés à la mise en œuvre de l'acquis Schengen (Islande, Norvège et Suisse).

IMPLICATIONS FINANCIÈRES :

- domaine politique concerné et activité associée : Rubrique 3 des perspectives financières – justice et affaires intérieures : 1806 – Mise en place d'un ELSJ en matière civile et criminelle ;

- commentaire budgétaire inhérent à la proposition: la proposition a une incidence sur le budget de la Communauté dans la mesure où le nombre supplémentaire d'accès au VIS généré par les autorités compétentes en matière de sécurité intérieure par l'intermédiaire des points d'accès centraux doit être pris en compte lors de la mise en place et de la maintenance du système. L'application de la présente décision n'impliquerait qu'une légère augmentation des dépenses administratives à la charge du budget des Communautés européennes pour les réunions et les services de secrétariat du nouveau comité établi conformément à l'article 10 de la proposition ;

- période d'application de la mesure : à partir de 2006 (et à titre indicatif, jusqu'en 2011) ;

- ressources financières prévues (en engagements et en paiements) : **néant** en dépenses opérationnelles.

- incidence globale sur les ressources humaines non inclus dans le montant de référence financière (ressources humaines et dépenses connexes + frais administratifs divers) : **1.382.640 EUR** de 2006 à 2011 dont :

- dépenses ressources humaines : 1,134 mios EUR couvrant l'équivalent de 1,75 personnes/an (un quart/temps de fonctionnaire A + 1,5 temps pleins de fonctionnaires B et/ou C, soit 189.000 EUR/an);
- autres dépenses administratives : 246.000 EUR (41.000 EUR/an de frais de réunions).

Total indicatif du coût de l'action : (engagements/paiements, uniquement frais de ressources humaines) : **1.382.640 EUR**.

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 12/06/2007

Le Conseil approuvé la décision concernant l'accès en consultation au VIS par les autorités désignées des États membres et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. Il s'est également félicité de l'accord intervenu avec le Parlement européen en première lecture sur le règlement concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (voir [COD/2004/0287](#)).

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 23/06/2008 - Acte final

OBJECTIF : permettre aux autorités compétentes des États membres en matière de sécurité intérieure et à EUROPOL de consulter le VIS en vue de prévenir et lutter contre le terrorisme et les formes graves de criminalité.

ACTE LÉGISLATIF : Décision 2008/633/JAI du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière

CONTEXTE : Dans le cadre de la mise en place progressive d'un Espace de liberté, de sécurité et de justice (ELSJ), l'Union européenne garantit la libre circulation des personnes mais aussi un niveau élevé de sécurité. Dans ce contexte, une priorité absolue a été accordée au développement et à l'établissement d'un système d'information sur les visas (VIS) en tant que système d'échange de données sur les visas entre les États membres (voir

[CNS/2004/0029](#)). Toutefois, la poursuite du développement et de l'établissement du VIS, notamment dans le domaine de la sécurité intérieure, y compris la lutte contre le terrorisme, requiert la mise en place d'un cadre juridique global complétant le règlement en vigueur, et ce, dans le strict respect des règles relatives à la protection des données à caractère personnel. C'est pourquoi, le Conseil a adopté la présente décision destinée à permettre aux autorités des États membres compétentes en matière de sécurité intérieure d'accéder au VIS, dans des cas dûment spécifiés à la décision, en vue, notamment, de leur permettre de consulter des informations précieuses pouvant les aider à prévenir le terrorisme et les formes graves de criminalité.

À noter que la présente décision complète le règlement (CE) n° 767/2008 du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), dans la mesure où elle fournit une base juridique dans le cadre du titre VI du traité sur l'UE, autorisant les autorités désignées et EUROPOL à avoir accès au VIS (voir [COD/2004/0287](#)).

CONTENU : La décision fixe les conditions dans lesquelles **les autorités des États membres compétentes en matière de sécurité intérieure et EUROPOL peuvent accéder au système d'information sur les visas (VIS)**, aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière.

Autorités et points d'accès centraux désignés : les États membres devront désigner les autorités qui seront autorisées à consulter les données du VIS. À cet effet, ils devront définir une liste d'« **autorités désignées** » qui pourra être modifiée. Les États membres devront également désigner le ou **les points d'accès centraux** par lesquels l'accès au VIS s'effectuera. La liste des autorités désignées et des points d'accès devra être transmise à la Commission et au Secrétariat général du Conseil pour le 2 décembre 2008 et devra être publiée au Journal officiel de l'Union européenne.

Au niveau national, chaque État membre devra également tenir une liste des unités opérationnelles qui, au sein des autorités désignées, seront autorisées à avoir accès au VIS par l'intermédiaire du ou des points d'accès centraux. **Seul le personnel dûment habilité** des unités opérationnelles, ainsi que du ou des points d'accès seront **autorisés à avoir accès au VIS**.

Accès au VIS : la décision fixe toutes les conditions techniques de l'accès aux données du VIS :

- **Procédure d'accès** : pour accéder au VIS, les unités opérationnelles autorisées devront présenter aux points d'accès centraux une demande écrite ou électronique d'accès au VIS, dûment motivée. Les points d'accès devront alors vérifier que toutes les conditions pour l'accès aux informations sont remplies et autoriser l'accès. Les informations du VIS sont communiquées de telle sorte que la sécurité des données n'est pas compromise. En cas d'urgence exceptionnelle, les points d'accès pourront également recevoir des demandes orales et les traiter immédiatement (en vérifiant *a posteriori* que les conditions nécessaires étaient remplies) ;
- **Conditions d'accès aux données du VIS par les autorités désignées**: l'accès au VIS ne sera accordé aux autorités requises que si un certain nombre de conditions sont réunies dont notamment le fait qu'il existe des motifs de penser que la consultation des données du VIS contribuera de manière significative à la prévention ou à la détection des infractions en question, ou aux enquêtes en la matière. En tout état de cause, la consultation du VIS sera limitée aux informations suivantes: nom, prénom, sexe; date, lieu et pays de naissance du titulaire ; nationalité ; type et numéro du document de voyage et dates de délivrance et d'expiration ; destination principale et durée du séjour prévu ; but du voyage ; empreintes digitales ; photographies... etc. ainsi que données relatives au refus, à l'annulation, au retrait ou à la prorogation du visa ;
- **Conditions d'accès spécifiques pour les États membres auxquels le règlement VIS n'est pas applicable** : dans les mêmes conditions que celles prévues ci-avant, les autorités des États membres qui n'ont pas normalement accès au VIS devront demander aux autorités désignées et aux points d'accès nationaux la possibilité d'accéder à certaines données du VIS dans des conditions précises et moyennant demande motivée ;
- **Conditions d'accès spécifiques pour EUROPOL** : dans les conditions déjà prévues par la décision *mutatis mutandis* et à condition que cet accès soit justifié dans le cadre des compétences d'EUROPOL, cet organe communautaire pourra accéder aux données du VIS, dans les limites de ses missions. Le traitement des informations obtenues par EUROPOL sera soumis à l'accord de l'État membre qui a introduit les données dans le VIS.

En tout état de cause, toute personne accédant aux données du VIS devra recevoir une **formation appropriée** sur les règles en matière de sécurité et de protection des données avant d'être autorisé à traiter des données stockées dans le VIS.

Protection des données : dans le souci d'assurer une juste protection des données à caractère personnel et, en particulier, d'**exclure un accès systématique**, le traitement de données du VIS ne devrait avoir lieu qu'au **cas par cas**, notamment lorsque l'accès en consultation est lié à :

- un événement particulier,
- un péril associé à une infraction grave,
- une ou à plusieurs personnes déterminées à l'égard desquelles il existe des raisons sérieuses de croire qu'elles commettront ou qu'elles ont commis une infraction terroriste ou une autre infraction pénale grave, ou qu'elles sont en relation avec une ou de telles personnes.

Pour s'assurer qu'un traitement adéquat des données est effectué, la décision prévoit que chaque État membre institue, conformément à son droit national, un **organe compétent chargé de contrôler le traitement des données** par les autorités désignées. Ces organes devront disposer de ressources suffisantes pour s'acquitter de leurs tâches et devront effectuer un audit sur le traitement des données tous les 4 ans.

Lien avec la décision-cadre sur la protection des données dans le cadre de la coopération policière : une fois qu'elle sera entrée en vigueur, la proposition de [décision-cadre](#) du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale devrait être applicable aux traitements de données à caractère personnel réalisés en vertu de la présente décision. Toutefois, dans l'attente et afin de compléter ces règles, la décision prévoit une série de dispositions destinées à assurer la protection des données. Il est ainsi prévu que chaque État membre garantisse dans son **droit national** un niveau de protection approprié des données correspondant au moins à celui résultant de la convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de la jurisprudence correspondante ainsi que d'autres textes juridiques liés.

Transfert des données à des tiers : la décision précise que les données du VIS ne doivent en aucune manière être transférées à des pays tiers ou des organisations internationales. Toutefois, en cas d'urgence exceptionnelle, ces données pourront être transférées exclusivement aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, et dans des conditions strictes prévues à la décision, sous réserve de l'accord de l'État membre qui a introduit les données dans le VIS. Des relevés de ces transferts seront dûment établis et mis à la disposition des autorités nationales chargées de la protection des données.

Sécurité des données : les États membres restent entièrement responsables de la sécurité des données pendant leur transmission aux autorités désignées. Ils devront prévoir des mesures de sécurité *ad hoc* pour sécuriser au maximum le stockage et le transfert des données (notamment, pour éviter toute copie ou modification des données ou tout traitement non autorisé). Des mesures très strictes de contrôle et d'autocontrôle par les autorités désignées sont notamment prévues.

Autres mesures techniques destinées à sécuriser et protéger les données : la décision prévoit également une série de mesures liées :

- à la **conservation des données** : les données extraites du VIS ne pourront être conservées que si cela est clairement nécessaire et dans des cas dûment prévus à la décision,
- au **droit de rectification et d'effacement des données** : une personne aura le droit de faire rectifier des données la concernant si elles sont inexactes, ou de les faire effacer si elles ont été stockées illégalement,
- aux **relevés** des informations transmises : toutes les opérations de traitement des données résultant de la consultation du VIS devront être enregistrées afin de pouvoir contrôler l'admissibilité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du système, ainsi que l'intégrité et la sécurité des données.

Responsabilité et sanctions : des dispositions sont prévues pour garantir que de toute personne ou que tout État membre ayant subi un dommage du fait d'un traitement illicite des données ou des dispositions de la décision, puisse obtenir réparation. Des mesures sont également prévues pour que toute utilisation non conforme aux dispositions de la décision soit passible de sanctions, y compris administratives et/ou pénales, effectives, proportionnées et dissuasives.

Coûts : les États membres et EUROPOL devront mettre en place et gérer leurs propres frais, l'infrastructure technique et les coûts liés à l'accès au VIS.

Suivi et évaluation : la décision fixe les modalités de suivi et d'évaluation du fonctionnement de la décision. Conformément au règlement 767/2008/CE, une instance gestionnaire devra être instituée en vue de contrôler le fonctionnement global du VIS. Il incombera à cette instance d'évaluer également les systèmes prévus en application de la présente décision en termes de résultats, de coût-efficacité, de sécurité et de qualité du service. Il est également prévu qu'après 2 ans d'activité du VIS (puis tous les 2 ans), l'instance gestionnaire soumette au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique du VIS en application de la présente décision. Parallèlement, 3 ans après le début de l'activité du VIS et ensuite tous les 4 ans, la Commission soumettra un rapport d'évaluation global du VIS en application de la présente décision incluant des réflexions sur le fonctionnement futur du système.

Dispositions territoriales : la décision fixe les modalités de participation à la présente décision, de certains États membres ne participant normalement pas à la politique commune en matière de visas (Royaume-Uni et Irlande, qui seront associés à la mise en œuvre de la décision dans des conditions spécifiques) ou pour les pays associés à la mise en œuvre de l'acquis Schengen (Islande, Norvège et Suisse).

ENTRÉE EN VIGUEUR : la décision entre en vigueur le 02/09/2008. Elle prend effet à compter de la pleine entrée en vigueur du [règlement \(CE\) n° 767/2008](#) sur le VIS.

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 19/04/2007

Le Comité mixte a pris acte des principaux résultats du trilogue mené le 28 mars 2007 entre le Conseil, le Parlement européen et la Commission au sujet d'un projet de règlement concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour.

Le résultat du trilogue a été encourageant et la présidence du Conseil a indiqué qu'il était réaliste d'envisager un accord sur le règlement VIS avec le Parlement européen en première lecture.

La présidence a également informé le Conseil de l'état d'avancement des travaux sur un projet de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière.

Le Comité mixte a approuvé un compromis global pour la poursuite des négociations avec le Parlement européen en vue de parvenir dans les meilleurs délais à un accord avec cette institution sur les deux instruments.

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 07/06/2007 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté le rapport de la Baronne Sarah LUDFORD (ALDE, UK) modifiant, dans la cadre de la procédure de consultation, la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins d'enquête en la matière.

Le texte adopté convient que la possibilité donnée à Europol et aux autorités nationales d'avoir accès au VIS ne peut que contribuer de manière positive à la sécurité intérieure et à la lutte contre le terrorisme. L'exigence d'un strict respect des règles relatives à la protection des données à caractère personnel et de conditions d'accès définies est toutefois soulignée.

Les principaux amendements proposés par Parlement sont les suivants :

- chaque État membre devra garantir dans son droit national un niveau de protection des données correspondant au moins à celui résultant de la convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ainsi que, pour les États membres qui l'ont ratifié, du protocole additionnel du 8 novembre 2001 ; il sera également tenu compte de la recommandation n° R (87) 15 du Comité des ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police du 17 septembre 1987 ;

- les députés proposent que chaque État membre désigne précisément les autorités ainsi que les points d'accès centraux par lesquels l'accès au VIS s'effectue. Chaque État membre tiendra une liste des autorités désignées ainsi que des points d'accès centraux et en informera la Commission. Les demandes d'accès au VIS devront être adressées aux points d'accès centraux par les unités opérationnelles des autorités désignées. Seul le personnel dûment habilité des unités opérationnelles, ainsi que du ou des points d'accès centraux, seront autorisés à avoir accès au VIS ;

- les données à caractère personnel obtenues du VIS doivent être traitées uniquement aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. Ainsi, le traitement des données VIS ne devrait avoir lieu qu'au cas par cas, toute consultation devant être justifiée par une réelle plus-value dans les enquêtes. La décision définit une série de conditions à réunir afin d'avoir accès aux données, soumises à un contrôle préalable de l'autorité nationale réceptrice de la demande (sauf en cas d'urgence, où le contrôle s'effectue a posteriori) ;

- sauf en cas d'urgence exceptionnelle et sous certaines conditions, les données à caractère personnel obtenues du VIS ne doivent pas être transférées à des pays tiers ou à des organisations internationales ou mises à leur disposition ;

- avant d'être autorisé à traiter des données stockées dans le VIS, le personnel des autorités ayant un droit d'accès doit recevoir une formation appropriée sur les règles en matière de sécurité et de protection des données et être informé des infractions et des sanctions pénales éventuelles en la matière ;

- chaque État membre doit adopter les mesures de sécurité nécessaires en ce qui concerne les données devant être extraites du VIS puis stockées, notamment pour: i) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques; ii) refuser l'accès des personnes non autorisées aux installations nationales dans lesquelles l'État membre stocke des données ; iii) empêcher toute lecture, copie, modification ou tout effacement non autorisés de supports de données ; iv) empêcher l'inspection, la modification ou l'effacement non autorisés de données à caractère personnel stockées ; v) empêcher le traitement non autorisé de données du VIS ; vi) garantir que les personnes autorisées à accéder au VIS n'aient accès qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des identités d'utilisateur individuelles et uniques ainsi qu'à des modes d'accès confidentiels; vii) garantir que toutes les autorités ayant un droit d'accès au VIS créent des profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées à accéder aux données ; viii) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données ; ix) garantir qu'il puisse être vérifié et constaté quelles données ont été extraites du VIS, à quel moment, par qui et à quelle fin; x) empêcher que des données à caractère personnel puissent être lues et copiées de façon non autorisée lors de leur transmission à partir du VIS ; xi) contrôler l'efficacité des mesures de sécurité et prendre les mesures d'organisation en matière de contrôle interne ;

- toute personne ou tout État membre ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions de la décision a le droit d'obtenir réparation de l'État membre responsable du dommage subi. Cet État est exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait dommageable ne lui est pas imputable;

- les données extraites du VIS peuvent être conservées dans les fichiers nationaux uniquement lorsque cela est nécessaire dans un cas particulier, et pendant une durée n'excédant pas celle nécessaire dans le cas concerné;

- toute personne a le droit de faire rectifier des données la concernant qui sont inexacts dans les faits ou de faire effacer des données la concernant qui sont stockées illégalement. La personne concernée est informée du suivi donné à l'exercice de son droit de rectification et d'effacement dans les meilleurs délais, et en tout cas au plus tard trois mois après la date à laquelle elle a demandé la rectification ou l'effacement, ou plus tôt si la législation nationale prévoit un délai plus court. Dans chaque État membre, toute personne a le droit de former un recours ou de déposer une plainte devant les autorités ou les juridictions compétentes de l'État membre qui lui a refusé le droit d'accès ou le droit de rectification ou d'effacement des données ;

- chaque État membre et Europol doit veiller à ce que toutes les opérations de traitement des données résultant de la consultation du VIS en vertu de la décision soient enregistrées afin de pouvoir contrôler l'admissibilité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du système, ainsi que l'intégrité et la sécurité des données.

Il est enfin rappelé que la présente décision constitue un développement des dispositions de l'acquis de Schengen auxquelles l'Irlande et le Royaume-Uni ne participe pas. Toutefois, conformément à la décision-cadre 2006/960/JAI, les informations contenues dans le VIS peuvent être communiquées au Royaume-Uni et à l'Irlande par les autorités compétentes des États membres dont les autorités désignées ont accès au VIS en vertu de la présente décision et les informations tenues dans les registres nationaux relatifs aux visas du Royaume-Uni et de l'Irlande peuvent être transmises aux services répressifs compétents des autres États membres.

Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 20/01/2006 - Document annexé à la procédure

AVIS DU CONTRÔLEUR EUROPÉEN DES DONNÉES

Le Contrôleur européen de la protection des données (CEPD) a été appelé à se prononcer sur le projet de décision en objet.

Globalement, sa position sur la proposition peut se résumer comme suit : il est crucial de ne permettre l'accès au dispositif prévu aux autorités compétentes chargées de la sécurité intérieure et à EUROPOL, **qu'au cas par cas** et **selon des mesures de précaution très strictes**. La proposition atteint ce but d'une manière globalement satisfaisante, en dépit des quelques améliorations dont elle pourrait faire l'objet, en particulier :

- l'une des conditions d'accès au VIS -conformément à l'article 5 de la proposition- devrait être que la consultation contribuera de «**manière substantielle**» à la prévention et à la détection d'une infraction grave;
- les relevés de toutes les opérations de traitement des données résultant de la consultation du VIS, exigés par l'article 10 de la proposition devraient permettre une évaluation de cette condition dans chaque cas individuel ;
- les deux **clés de recherche** pour l'accès au VIS, mentionnées à l'article 5, paragraphe 2, à savoir «le but du voyage» et les «photographies» devraient être réexaminées et devraient être mises à disposition, en tant qu'information supplémentaire en cas de réponse positive ;
- le niveau de protection des données appliqué à la consultation devrait être équivalent, quelle que soit l'autorité consultant les données VIS ;
- l'article 8 (protection des données à caractère personnel) et l'article 10 (établissement de relevés) devraient également s'appliquer aux États membres auxquels le règlement VIS n'est pas applicable ;
- une approche coordonnée en matière de contrôle devrait être assurée également en ce qui concerne l'accès au VIS tel qu'il est prévu dans la proposition ;
- les dispositions relatives aux systèmes de suivi devraient également permettre des vérifications internes de conformité avec les exigences de protection des données.