

**Avis sur la notification d'un contrôle préalable reçue du Délégué à la protection des données du Secrétariat général du Conseil de l'Union européenne concernant la "*Gestion des permis de port d'arme pour les agents désignés du Bureau de Sécurité*".**

Bruxelles, le 16 décembre 2014 (Dossier 2012-0923)

## **1. Procédure**

Le 29 octobre 2012, le Délégué à la protection des données (ci-après "le DPD") du Secrétariat Général du Conseil de l'Union européenne (ci-après "le Conseil") a envoyé au Contrôleur européen de la protection des données (CEPD) une notification au sens de l'article 27 du règlement 45/2001 (ci-après "le règlement") concernant la "*Gestion des permis de port d'arme pour les agents désignés du Bureau de Sécurité*".

À la demande du CEPD, le DPD du Conseil a fourni subséquemment des informations supplémentaires.

Le projet d'avis a été envoyé au DPD du Conseil le 2 décembre 2014 pour commentaires. Des commentaires ont été fournis le 8 décembre 2014.

## **2. Faits**

### **Finalité**

Le traitement en question concerne l'organisation des demandes d'un permis de port d'arme et la gestion de ces permis. Il est effectué par le Bureau de Sécurité du Conseil (ci-après "le Bureau de Sécurité").

### **Personnes concernées**

Les personnes concernées sont les fonctionnaires désignés du Bureau de Sécurité.

### **Base légale**

La notification fait référence aux normes suivantes:

- le règlement de sécurité (Décision 2011/292/UE du 31/03/2011);
- l'article 19 de la Décision 181/10 du Conseil concernant les tâches du Bureau de Sécurité qui prévoit l'autorisation de porter une arme de service: "*Pendant leur service, les agents du Bureau de sécurité sont autorisés à porter une arme de service et à en faire usage conformément à la législation de l'État d'accueil et dans le respect de toutes les instructions spécifiques qui leur sont adressées par le Secrétaire général*" et
- l'article 23 du Statut des fonctionnaires de l'Union européenne qui prévoit: "*Sous réserve des dispositions du protocole sur les privilèges et immunités, les intéressés ne sont pas dispensés de s'acquitter de leurs obligations privées, ni d'observer les lois et les règlements de police en vigueur*".

## Procédure

Afin de pouvoir exercer la fonction d'agent en service armé, les fonctionnaires du Bureau de Sécurité doivent recevoir une autorisation de port d'arme délivrée par les autorités des pays où ces activités sont exercées. En l'espèce, il s'agit donc des autorités belges et luxembourgeoises, lieux où le Conseil a son siège.

L'arme de service est portée pendant les heures de service du fonctionnaire concerné.

Le fonctionnaire qui souhaite obtenir un permis doit remplir un formulaire de demande et fournir au Bureau de Sécurité les données suivantes:

- données d'identification (copie de carte d'identité);
- motif de la demande et circonstances dans lesquelles l'arme sera portée;
- la lettre de demande émanant du Bureau de Sécurité qui certifie que l'agent travaille dans le service de sécurité; (seulement pour la Belgique) extrait du casier judiciaire;
- (seulement pour la Belgique) attestation délivrée par un médecin attestant que la personne est apte à porter/manipuler une arme;
- (seulement pour la Belgique) une attestation des formations théoriques et pratiques relative au maniement des armes et de l'entraînement régulier;
- (seulement pour la Belgique) une attestation de formation relative aux droits et aux devoirs du personnel et aux principes fondamentaux du droit belge;
- (seulement pour la Belgique) une copie de l'autorisation de détention de l'arme à feu de défense pour laquelle le permis de port est sollicitée.

Selon la procédure belge, pour chaque nouvelle demande et/ou chaque renouvellement (tous les trois ans), la personne concernée doit présenter à nouveau un extrait de son casier judiciaire et une attestation médicale.

Selon la procédure luxembourgeoise, le renouvellement a lieu tous les cinq ans.

Le Bureau de Sécurité transfère toutes ces données aux autorités belges/luxembourgeoises en vue de la délivrance de l'autorisation.

En Belgique : selon la procédure prévue par la Loi sur les armes, la lettre de demande émanant du Bureau de Sécurité avec le formulaire de demande est transmis au Gouverneur de la province de domiciliation du fonctionnaire (pour Bruxelles : au Gouverneur de l'Arrondissement administratif de Bruxelles-Capitale). Avant de délivrer l'autorisation, le gouverneur demande des avis et procède à des vérifications auprès du Parquet du Procureur du Roi de l'arrondissement judiciaire du lieu de domicile du fonctionnaire, auprès du Parquet du Procureur du Roi du lieu de travail du fonctionnaire (Bruxelles) et au Service Public Fédéral Intérieur (Cellule de Crise). Le Service Public Fédéral Intérieur a établi une Circulaire Ministérielle OOP 21, avec des directives aux Gouverneurs de Province pour situer le cadre de travail du Bureau de Sécurité et les missions de protection et de service "armé" de ses fonctionnaires.

Au Luxembourg : la lettre de demande émanant du Bureau de Sécurité est transmise au Ministère de la Justice (Service des armes prohibées) qui délivre l'autorisation.

Le Bureau de Sécurité garde une copie des données ainsi transmises.

Les documents d'autorisation belge ("Permis de port d'arme à feu") et luxembourgeois ("Autorisation de port d'arme") contiennent les informations suivantes : identité du titulaire (nom et prénom, lieu et date de naissance, nationalité et adresse privée, photo), spécifications

de l'arme de service, dates de validité de l'autorisation, identification de l'autorité ayant émis le document, stipulations en matière de législation.

Le traitement est en partie automatisé. Les copies des correspondances (entre le Bureau de Sécurité, le fonctionnaire et les autorités), les formulaires et attestations fournis par le fonctionnaire sont collectées de manière manuelle.

Les données qui sont encodées dans une base de données sur le serveur du Conseil sont les suivantes : nom et prénom de la personne concernée, lieu et date de naissance, nationalité et adresse privée, spécifications de l'arme de service attribuée et spécification de l'autorité, émetteur des autorisations et dates de validité des autorisations. À l'aide de cette base de données, ces données sont tenues à jour. La base de données sert également d'instrument de rappel au gestionnaire pour les renouvellements périodiques des permis et des autorisations.

### **Destinataires externes**

Les autorités belges et luxembourgeoises comme indiqué ci-dessus.

### **Droits d'accès, de rectification, de verrouillage, d'effacement**

La notification fait référence à la Section 5 de la Décision du Conseil du 13 septembre 2004 relative aux procédures établies par le Conseil garantissant les droits des personnes concernées.

### **Conservation des données**

D'après la notification et la note d'information, les données (administratives, formulaires, attestations, autorisations, permis, justificatifs de renouvellement) sont conservées pendant toute la carrière du fonctionnaire au sein du service et elles sont détruites deux ans après le départ du fonctionnaire.

Étant donné qu'il s'agit de procédures officielles établies sur la base d'une législation nationale spécifique, le Conseil a indiqué que la période de deux ans après le départ du fonctionnaire semble raisonnable, et permet de garder une documentation exacte pour pouvoir répondre à une éventuelle requête des autorités nationales intéressées.

### **Droit à l'information**

La note d'information est communiquée aux personnes concernées au moment de la collecte des données.

### **Sécurité et stockage**

Les personnes du Bureau de Sécurité qui ont accès aux données relatives au traitement doivent signer une clause de confidentialité qui fait référence à l'article 10 du règlement et qui précise en particulier qu'en ce qui concerne les données relatives à la santé, elles ont une obligation de secret professionnel similaire à celle à laquelle est soumis un praticien de la santé.

Les documents papiers (copies de correspondances et documentation remise par les fonctionnaires) sont stockés dans des classeurs dans une armoire fermée à clef dans un bureau qui est fermé par une serrure électronique.

Actuellement, l'accès à la base de données est limité à un gestionnaire.

### 3. Aspects légaux

#### 3.1 Contrôle préalable

**L'applicabilité du règlement** : Le traitement des données concerné constitue un traitement de données à caractère personnel ("*toute information concernant une personne physique identifiée ou identifiable*", selon l'article 2.a du règlement). Le traitement des données est effectué par une institution de l'Union européenne (ci-après "l'UE"), le Conseil, dans l'exercice d'activités qui relèvent du champ d'application du droit de l'UE<sup>1</sup>. Les formulaires de demande et les attestations sont collectés sous format papier et des données sont encodées dans une base de données sur le serveur du Conseil, comme il est expliqué dans les faits. Le traitement est donc partiellement automatisé et lorsqu'il est manuel, appelé à figurer dans un fichier ; par conséquent le règlement est applicable.

**Motifs de contrôle préalable** : L'article 27.1 du règlement soumet au contrôle préalable du CEPD tout "*traitement susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités*". A l'article 27.2, figure une liste des traitements susceptibles de présenter de tels risques, comme "*les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté ...*" (article 27.2.a).

Afin de pouvoir exercer la fonction d'agent en service armé, les fonctionnaires doivent fournir un extrait de casier judiciaire et une attestation médicale en vertu des procédures nationales belges et luxembourgeoises respectivement où les activités du Conseil sont exercées. Des données relatives à des infractions et à la santé sont donc traitées de manière structurelle dans le cadre du traitement. C'est pourquoi, ce traitement doit faire l'objet d'un contrôle préalable sur la base de l'article 27.2.a. du règlement.

La notification officielle a été reçue en date du 29 octobre 2012. Depuis lors, le CEPD a eu un échange d'informations supplémentaire avec le DPD du Conseil. Étant donné que ce dossier est un contrôle préalable ex post, le délai de deux mois endéans lequel le CEPD doit rendre son avis ne s'applique pas. Le CEPD a cependant mis tout en œuvre pour le traiter dans un délai raisonnable.

#### 3.2 Licéité du traitement

D'après l'article 5 du règlement, le traitement de données ne peut être effectué que sur une des bases y stipulées.

Parmi les cinq bases énoncées dans l'article 5, le traitement remplit les conditions prévues par l'article 5.a du règlement, selon laquelle le traitement des données peut être effectué si "*le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes...ou relevant de l'exercice légitime de l'autorité publique dont est investie l'institution*".

---

<sup>1</sup> Les concepts "*institutions et organes communautaires*" et "*droit communautaire*" ne peuvent plus être utilisés après l'entrée en vigueur du Traité de Lisbonne le 1er décembre 2009. L'article 3 du règlement doit donc être lu à la lumière du Traité de Lisbonne.

Le traitement en l'espèce est basé sur l'article 19 de la Décision 181/10 du Conseil et l'article 23 du Statut des fonctionnaires. Ces dispositions mentionnent l'exercice légitime de l'autorité publique dont est investie l'institution, notamment le Conseil dans le cadre de sa collaboration et l'échange des données avec les autorités nationales belges et luxembourgeoises en conformité avec les lois et les règlements nationaux en vigueur relatifs à l'autorisation de port d'arme de service.

En outre, sur la base de l'article 5.b du règlement, le traitement est nécessaire au respect d'une obligation légale à laquelle le Conseil est soumis, à savoir les lois et les règlements de la police belge et luxembourgeoise respectivement.

En l'espèce, le traitement des extraits de casiers judiciaires et des attestations médicales est nécessaire afin que le Conseil puisse assurer que seuls les agents habilités à porter une arme deviennent titulaires de permis de port d'arme. Ce traitement est donc nécessaire à la gestion des permis de port d'arme et à l'autorisation de ces permis par les autorités nationales. Ce traitement s'inscrit dans le cadre général de la gestion de la sécurité du Conseil.

La licéité du traitement proposé est donc respectée.

### **3.3 Traitement portant sur des catégories particulières de données**

L'article 10.1 du règlement prévoit que le traitement de données à caractère personnel relatives à la santé est interdit sous réserve des dérogations prévues notamment à l'article 10.2 et 10.5 du règlement.

En l'espèce, si les personnes concernées souhaitent être autorisées à exercer la fonction d'agent faisant un service armé, elles doivent fournir une attestation médicale qui déclare qu'elles sont aptes à porter et à manipuler une arme selon la législation nationale belge ou luxembourgeoise, selon le cas. Ce traitement est prévu par l'article 19 de la Décision 181/10 du Secrétaire Général du Conseil qui indique explicitement qu'afin que les agents du Bureau de Sécurité soient autorisés à porter une arme de service et en faire usage, ils doivent se conformer à la législation de l'État d'accueil, notamment la législation belge et luxembourgeoise respectivement. De même l'article 23 du Statut des fonctionnaires oblige le Conseil à observer les lois et les règlements de police en vigueur. Ce traitement peut donc être considéré comme nécessaire afin de respecter les obligations du Conseil en matière de droit du travail au sens de l'article 10.2.b du règlement.

Quant au traitement des extraits judiciaires, l'article 10.5 du règlement prévoit que "*le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que s'il est autorisé par les traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités...*". Le CEPD note que le traitement en question est autorisé par l'article 19 de la Décision 181/10 du Secrétaire Général du Conseil qui implique le respect de la législation nationale en vigueur qui, en l'espèce, prévoit le traitement en question. De même, l'article 23 du Statut des fonctionnaires et le Protocole sur les privilèges et immunités oblige le Conseil à observer les lois et les règlements de police en vigueur. Le traitement est donc en conformité avec l'article 10.5 du règlement.

### **3.4 Qualité des données**

Conformément à l'article 4.1.c du règlement, les données à caractère personnel doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont*

*collectées et pour lesquelles elles sont traitées ultérieurement*". Il convient donc de vérifier que les données sont en relation avec la finalité du traitement pour lequel elles sont traitées.

Le CEPD considère que la collecte des données, comme elle est exposée dans les faits, satisfait les conditions au regard des finalités du traitement, notamment l'organisation et la gestion des demandes de permis de port d'arme et l'autorisation de ces permis par les autorités nationales.

Par ailleurs, l'article 4.1.d du règlement dispose que les données doivent être *"exactes et, si nécessaire, mises à jour"*. Selon cet article, *"toutes les mesures raisonnables sont prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées"*.

Dans le cas présent, la procédure mise en place, en particulier la nécessité de produire un nouveau casier judiciaire et une nouvelle attestation médicale à chaque renouvellement de l'autorisation (tous les trois ans pour la Belgique permet raisonnablement de penser qu'une partie du système en lui-même garantit la qualité des données. En revanche, les autres documents fournis lors de la demande initiale ne doivent pas être actualisés. Il est cependant possible que la personne concernée fasse de nouvelles formations relatives au maniement des armes au cours de sa carrière et que les attestations de formation remises dans le cadre de la délivrance de l'autorisation initiale ne soient plus d'actualité. Les droits d'accès et de rectification doivent donc être garantis à la personne concernée, afin de permettre à ces dernières de rendre leur dossier le plus complet/à jour possible. Ces droits constituent le second moyen d'assurer l'exactitude et la mise à jour des données concernant les personnes concernées (voir point 3.7 sur le droit d'accès).

De plus, les données doivent être *"traitées loyalement et licitement"* (article 4.1.a). La licéité du traitement a déjà fait l'objet d'une analyse dans le point 3.2 de cet avis. Quant à la loyauté, elle est liée aux informations qui doivent être transmises à la personne concernée (voir point 3.8 sur le droit à l'information).

### **3.5 Conservation des données**

Le principe général énoncé dans le règlement prévoit que les données doivent être *"conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement"* (article 4.1.e du règlement).

En l'espèce, les données sont conservées pendant toute la carrière du fonctionnaire au sein du service et elles sont détruites deux ans après le départ du fonctionnaire. Le CEPD note que le Conseil estime nécessaire de garder une documentation exacte pour pouvoir répondre à une éventuelle requête des autorités nationales intéressées. Cependant, selon la description des faits, les autorités nationales possèdent déjà l'ensemble des documents et attestations dont le Conseil ne garde que des copies.

Le CEPD considère donc que cette durée de conservation n'est pas justifiée. Le CEPD recommande que le Conseil fournisse des justifications au regard de ladite durée de rétention ou établisse une durée proportionnelle à la finalité pour laquelle la documentation est collectée.

### **3.6 Transfert de données**

Les articles 7, 8 et 9 du règlement prévoient certaines obligations qui s'appliquent lorsque des données personnelles sont transférées à des tiers. Les règles diffèrent selon que le transfert est effectué entre ou au sein des institutions ou organes de l'UE (article 7), à des destinataires relevant de la directive 95/46 (article 8), ou à d'autres types de destinataires (article 9).

En l'espèce, étant donné que le Conseil transmet des données aux autorités nationales belges et luxembourgeoises respectivement, l'article 8.a du règlement est applicable. Le transfert est prévu dans les législations nationales afin que les autorités nationales puissent accorder aux fonctionnaires du Conseil l'autorisation ou pas d'un permis de port d'arme. Dès lors, le CEPD considère que la condition de nécessité est établie ; les données transférées aux autorités nationales sont nécessaires dans le cadre de l'exécution de leur mission effectuée dans l'intérêt public, au sens de l'article 8.a du règlement.

### **3.7 Droits d'accès et de rectification**

L'article 13 du règlement pose le principe du droit d'accès aux données -et ses modalités- à la demande de la personne concernée par le traitement. L'article 14 du règlement dispose du droit de rectification pour la personne concernée.

Le CEPD note que les droits d'accès et de rectification sont prévus dans la Décision du Conseil 2004/644/CE et que le Conseil peut garantir ces droits aux personnes concernées conformément aux articles 13 et 14 du règlement.

### **3.8 Information de la personne concernée**

Les articles 11 et 12 du règlement portent sur les informations à fournir à la personne concernée afin de garantir un traitement transparent de ses données à caractère personnel. Ces articles énumèrent une série de mentions obligatoires et certaines autres facultatives. Ces dernières sont applicables dans la mesure où, compte tenu des circonstances particulières du traitement en l'espèce, elles sont nécessaires afin d'assurer un traitement loyal des données à l'égard de la personne concernée.

Dans le cas présent, une partie des données requises est fournie directement par la personne concernée aux gestionnaires du Bureau de Sécurité. D'autres données sont fournies par les autorités nationales belges et luxembourgeoises. Par conséquent, tant l'article 11 que l'article 12 du règlement sont applicables.

Le CEPD note qu'une note d'information est communiquée aux personnes concernées au moment de la collecte des données et qu'elle contient les informations nécessaires, en conformité avec les articles 11 et 12 du règlement.

### **3.9 Mesures de sécurité**

Conformément à l'article 22 du règlement relatif à la sécurité des traitements, *"le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à caractère personnel à protéger"*.

Le CEPD note que les gestionnaires du Centre qui traitent les attestations médicales doivent signer une Clause de confidentialité les soumettant à une obligation de secret professionnel

équivalente à celle d'un praticien de la santé. Vu la nature sensible des données traitées, le CEPD est satisfait de cette mesure organisationnelle adoptée par le Conseil qui vise à préserver la confidentialité des données et à empêcher un accès non autorisé des données dans le sens de l'article 22 du règlement.

Quant au reste des mesures de sécurité prises afin d'assurer un niveau de sécurité adéquat au traitement en l'espèce, le CEPD n'a pas de raison de croire que le Conseil n'a pas respecté les mesures de sécurité requises à l'article 22 du règlement.

**Conclusion:**

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement pour autant qu'il soit tenu compte des observations faites ci-dessus. Cela implique, en particulier, que le Conseil :

fournisse des justifications au regard de la durée de rétention des données en question ou établisse une durée proportionnelle à la finalité pour laquelle cette documentation est collectée.

Fait à Bruxelles, le 16 décembre 2014

**(signé)**

Giovanni BUTTARELLI  
Le Contrôleur européen de la protection des données