Avis sur une notification de contrôle préalable reçue du délégué à la protection des données du Parlement européen concernant le dossier «Dispositif de vérification biométrique»

1. Procédure

Le 9 octobre 2013, le Contrôleur européen de la protection des données (**CEPD**) a reçu du délégué à la protection des données (**DPD**) du Parlement européen (**Parlement**) une notification de contrôle préalable portant sur le traitement de données à caractère personnel dans le contexte du dispositif de vérification biométrique du Parlement.

Le CEPD a également reçu divers documents en rapport avec cette notification, à savoir :

1. Décision du Bureau du Parlement sur le concept global de sécurité ;
2. Décision du Bureau relative à l'internalisation de la sécurité du Parlement ;
3. Déclaration de confidentialité relative au dispositif de vérification biométrique.

Le CEPD a également reçu le 21 octobre 2013 de plus amples informations techniques relatives au système biométrique sélectionné par le Parlement ainsi que des réponses à une série de questions techniques qui avaient été posées. Le délai dans lequel le CEPD doit rendre son opinion a ensuite été prolongé de deux mois le 9 décembre 2013 en raison de la complexité des faits et ce en conformité avec l'article 27(4) du règlement. Le 10 janvier 2014 le délai a été suspendu en vue de la tenue d'une réunion avec le Parlement. La réunion s'est tenue le 30 janvier 2014. À la suite de cette réunion, une nouvelle série de questions a été envoyée au Parlement. Le Parlement a donné réponse à ces questions le 26 mars 2014.

La notification a été soumise pour contrôle préalable au titre de l'article 27, paragraphe 1 du règlement (CE) n° 45/2001 ("le règlement").

2. Les faits

À la suite de la décision visant à l'internalisation de ses activités de sécurité, le Parlement a décidé de réutiliser un dispositif existant de vérification biométrique dans le but d'assurer l'occupation des postes de sécurité par les seuls agents de prévention et de surveillance et par le personnel de sécurité habilités.

Ce système biométrique est actuellement utilisé par la société externe en charge de la sécurité du Parlement (Securitas). La décision d'internalisation aura comme conséquence que le Parlement emploiera à l'avenir des agents de prévention et de surveillance dépendant directement de son autorité ainsi que des gardes de sécurité dépendant d'un prestataire externe pour des besoins spécifiques […]. Selon la notification, le choix de la solution fait suite au projet de concept global de sécurité adopté par l'institution. La Direction des ressources et plus particulièrement les unités en charge du planning et du dispatching sont responsables, dans la pratique, de la mise en œuvre du traitement. L'enrôlement des agents dans le système se fait par le service Planning pour les agents du PE et par Securitas pour les agents de Securitas, […].

La mise en place d'un tel dispositif a été jugée indispensable par le Parlement pour répondre aux impératifs de sécurité auxquels il fait face. Ces impératifs de sécurité couvrent en particulier la gestion des agents de prévention et de surveillance responsables des nombreux accès physiques du Parlement. Le Parlement doit être en mesure de s'assurer de l'identité des agents en poste afin d'éviter les prises de postes frauduleuses. Il convient en effet :
- d'éviter que les agents de prévention et de surveillance internes au Parlement n'échangent leur poste avec les gardes dépendant du prestataire externe et inversement, et ce pour des raisons de sécurité et de responsabilité, notamment en cas d'accident ;
- d'éviter que certains agents, en accord avec d'autres (l'agent les précédant ou les suivant au même poste) ne respectent pas leurs horaires de travail, augmentant ainsi le niveau de risque pour la sécurité ;
- d'assurer que les agents occupent bien le poste qu'ils sont **habilités à occuper**. Sont mentionnés à titre d'exemples : (i) les agents placés en poste aux crèches gérées par le Parlement et qui doivent avoir suivi une formation spécifique et doivent fournir un extrait de casier judiciaire spécial; (ii) les postes liés au maniement des portiques et radioscopes (rayons-x) qui nécessitent également d'avoir suivi une formation spécifique; (iii) […] ; (iv) les postes aux entrées des parkings, qui requièrent du matériel spécifique et (v) la prise en compte des interdictions médicales individuelles, qui doivent être respectées.

Selon le Parlement, une telle nécessité implique donc que l'unité en charge du planning puisse à la fois être informée de, et maîtriser de manière efficace et fiable, les prises de poste pour pouvoir réagir en cas d'absence ou de prise de poste frauduleuse pouvant entraîner l'accès frauduleux aux instructions de sécurité de l'institution (par exemple […]).

En ce qui concerne le principe de fonctionnement du système, le lecteur biométrique capture une image tridimensionnelle de la main. Suite à cette capture, le lecteur convertit l'image en un modèle électronique. Ce modèle, ainsi que le numéro d'identification de l'utilisateur associé, sont stockés dans des bases de données qui, dans le cas […].

Dans la procédure prévue au niveau du Parlement, l'unité en charge du planning définit la répartition des agents. Au moment de la prise/départ de poste l'agent devra présenter son badge et sa main afin de s'identifier. L'utilisateur utilise un lecteur de badge intégré au lecteur biométrique pour saisir son numéro d'identification. Le lecteur biométrique invite ensuite l'utilisateur à placer sa main. Le lecteur compare alors la main posée au modèle unique stocké […].

Par conséquent, la concordance est faite entre les caractéristiques biométriques et l'identifiant (badge) ([…]) d'une part, et l'identifiant, le numéro de personnel et les nom et prénom de l'agent […] d'autre part.

Les **personnes concernées** sont les agents de sécurité du Parlement et de Securitas. En ce qui concerne la procédure d'enrôlement, celle-ci est confiée au personnel d'encadrement.

Les **données collectées** dans le cadre de ce traitement sont :
- nom et prénom ;
- modèle biométrique (correspondant à des caractéristiques biométriques traduites sous forme numérique selon une norme/codage déterminé) et non données biométriques brutes ;
- l'identifiant (badge) de l'agent ;
- le numéro de personnel ;
- données relatives à l'horaire de prise de poste et de départ.

En ce qui concerne **les destinataires des données** traitées, les données relatives aux prestations horaires seront transférées aux Unités compétentes de la DG PERS (transfert effectué de la base Planning à la base Streamline):

- droits individuels et rémunération ;
- gestion du personnel et des carrières (impact des congés longue durée pour la carrière).

Il est également indiqué que, lorsque cela est applicable, les données sont transférées à l'unité de gestion des absences médicales.

[…].

En ce qui concerne les données biométriques, […]. Ces données biométriques ne sont pas transférées à l'unité en charge du Planning, qui ne reçoit que les données relatives à l'identifiant de l'agent et aux horaires de prise de poste et de départ, qu'elle vérifie et valide.

En ce qui concerne les **droits des personnes concernées**, la notification prévoit que les personnes concernées peuvent à tout moment exercer leurs droits d'accès, de rectification, de verrouillage, d'effacement et d'opposition en adressant une demande au Planning. […].

De plus, au regard des droits des personnes concernées, le responsable du traitement doit se prononcer dans un délai de 15 jours ouvrables à partir de la réception de la demande de verrouillage. Si la demande est acceptée, elle doit être exécutée dans un délai de 30 jours ouvrables et la personne concernée en est informée. En cas de refus d'une demande de verrouillage, le responsable du traitement dispose d'un délai de 15 jours ouvrables pour en informer la personne concernée par lettre motivée.

De manière similaire, le responsable du traitement doit répondre dans un délai de 15 jours ouvrables à partir de la réception de la demande d'effacement. Si la demande est acceptée, celle-ci doit être exécutée sans délai. Si le responsable du traitement considère que la demande n'est pas justifiée, il dispose d'un délai de 15 jours ouvrables pour en informer, par lettre motivée, la personne concernée.

Selon la notification, **l'information** aux personnes concernées se fera via :
- une formation aux agents nouvellement recrutés, à laquelle le Délégué à la protection des données du Parlement participe ;
- une déclaration sur la protection des données reprenant toutes les caractéristiques du traitement en question tel que requis aux articles 11 et 12 du règlement. Un projet de déclaration de confidentialité a été fourni par le Parlement.

En ce qui concerne **la conservation des données**, la notification prévoit […]

Au niveau de la **durée de conservation**, selon la procédure actuellement prévue :
Les données relatives à l'identité des agents, l'identifiant (badge) ainsi que les caractéristiques biométriques seront conservés […] pendant la durée durant laquelle l'agent est appelé à exercer des fonctions d'agent de prévention et de surveillance – tâches et fonctions de sécurité.

En ce qui concerne les **caractéristiques techniques et de sécurité** du système biométrique, le responsable du traitement a fourni de l'information supplémentaire en ce qui concerne l'architecture et la description du système choisi :

celles-ci contiennent principalement : […]

3. Analyse légale

3.1. Contrôle préalable

Applicabilité du règlement : le présent avis relatif à un contrôle préalable porte sur le traitement de données à caractère personnel réalisé par le Parlement européen.

Le règlement s'applique au *«traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier»* et au traitement *«par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire»*. Pour les motifs décrits ci-après, tous les éléments qui donnent lieu à l'application du règlement sont présents.

Tout d'abord, des *données à caractère personnel* telles qu'elles sont définies à l'article 2, point a), du règlement sont collectées et traitées ultérieurement. Ensuite, les données à caractère personnel collectées sont soumises à un *«traitement automatisé»* au sens de l'article 2, point b), du règlement. En effet, les données à caractère personnel telles que les données d'identification personnelle, dont les empreintes de la main, sont collectées et soumises à un «traitement automatisé», par exemple lorsque le service prélève les empreintes. Enfin, le traitement est mis en œuvre par une institution, dans le cas présent le Parlement, pour l'exercice d'activités qui relèvent du champ d'application du droit de l'UE (article 3, paragraphe 1, du règlement).

Motif de contrôle préalable : l'article 27, paragraphe 1, du règlement soumet au contrôle préalable du CEPD les *«traitements susceptibles 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»*. Le CEPD estime[1] que la présence et le traitement de données biométriques autres que des photographies, comme c'est le cas dans la présente affaire étant donné que des empreintes biométriques de mains sont collectées, peut présenter des risques particuliers au regard des droits et libertés des personnes concernées. Il tire cette conclusion essentiellement de la nature des données biométriques, en raison de caractéristiques inhérentes à ce type de données. Par exemple, les données biométriques rendent les caractéristiques du corps humain «lisibles à la machine» et susceptibles de faire l'objet d'une utilisation ultérieure. Ces risques peuvent justifier la nécessité de soumettre le traitement de données au contrôle préalable du CEPD sur la base de l'article 27, paragraphe 1, du règlement afin de vérifier que des garanties strictes ont été mises en œuvre.

Par ailleurs, le CEPD estime que dans certains cas, l'intégration de la technologie RFID (carte à puce RFID intégrée dans le badge) peut engendrer des risques spécifiques. Dans le cas présent, l'utilisation de la technologie RFID n'est prévue que pour le badge qui, à l'heure actuelle, ne contient pas de biométrie. D'après les informations reçues, le Parlement envisage cependant […]. Dans ce cas, le CEPD tient à signaler que cela pourraient entrainer une modification des risques du traitement.

[1] Voir aussi les dossiers 2010-0427 du 8 septembre 2011, 2007-635 du 7 avril 2008 et 2008-223 du 30 juin 2008, disponibles sur le site du CEPD.

Délais : le contrôle préalable ayant pour objectif de répondre à des situations susceptibles de présenter des risques particuliers, l'avis du CEPD doit, selon l'article 27 du règlement, être rendu avant le début du traitement. Dès lors, le traitement ne devrait pas être mis en œuvre tant que le CEPD n'a pas donné son approbation formelle.

La notification a été reçue le 9 Octobre 2013. En vertu de l'article 27, paragraphe 4, du règlement, la période de deux mois au cours de laquelle le CEPD doit rendre son avis (en l'espèce la procédure a été suspendue pendant un total de 75 jours afin d'obtenir des informations supplémentaires, auxquels s'ajoutent 20 jours afin de permettre la formulation de commentaires sur le projet d'avis). Le présent avis doit donc être adopté au plus tard le 15 mai 2014.

3.2. Licéité du traitement

Le traitement de données à caractère personnel n'est autorisé que s'il est fondé sur l'article 5 du règlement. Parmi les divers motifs énoncés à l'article 5 du règlement, l'article 5, point a) semble s'appliquer au traitement notifié. En effet, au terme de celui-ci, le traitement de données à caractère personnel ne peut être effectué que s'il est *«nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités instituant les Communautés européennes ou d'autres actes législatifs adoptés sur la base de ces traités […]»*.

Afin de déterminer si le traitement est conforme à l'article 5, point a), du règlement, trois éléments doivent être pris en compte : premièrement, si les traités ou d'autres actes législatifs prévoient le traitement effectué, deuxièmement, si le traitement est effectué dans l'intérêt public, et troisièmement, si le traitement est effectivement nécessaire à l'exécution de cette mission (test de nécessité). Les trois exigences sont étroitement liées.

* La **base juridique** applicable pour le traitement en question est décrite dans les actes suivants :

- Décision du Bureau du 6 juillet 2011 relative au concept global de sécurité ;
- Décision du Bureau du 11 juin 2012 relative à l'internalisation de la sécurité du Parlement.

Ces décisions prévoient le développement, au sein du Parlement, d'un "concept global de sécurité" ainsi que l'internalisation progressive de la sécurité du Parlement.

Les décisions du bureau du Parlement sont prévues par les règles de procédure du Parlement, règles prises sur la base de l'article 232 du Traité sur le fonctionnement de l'Union Européenne.

Le traitement est réalisé dans le cadre de **l'exercice légitime de l'autorité publique**. Le CEPD constate que le Parlement réalise les activités de traitement dans le cadre d'une mission relevant de l'exercice légitime de son autorité publique sur la base des actes législatifs susmentionnés adoptés sur la base du statut des fonctionnaires. Le Parlement a adopté un concept global de sécurité dont le traitement notifié fait partie.

Concernant la nécessité du traitement **(test de nécessité)**, conformément à l'article 5, point a), du règlement, le traitement de données doit être *«nécessaire à l'exécution d'une mission»* tel que mentionné plus haut. À cet égard, le considérant 27 établit que *«(l)e traitement de données à caractère personnel effectué pour l'exécution de missions d'intérêt public par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes»*.

La nécessité de l'utilisation du système de vérification biométrique avancée par le Parlement est basée sur les besoins généraux de sécurité, qui comprennent la gestion spécifique de son personnel de sécurité (pallier les éventuels manquements de la part de son personnel telle que la prise de poste frauduleuse). Le CEPD ne peut cependant perdre de vue que le choix de la solution technique spécifique (en ce compris la reconnaissance biométrique de main) est aussi liée au fait que cette solution est actuellement utilisée par la société de gardiennage externe sous contrat avec le Parlement (Securitas). Cet élément, même s'il n'est pas l'élément principal ayant conduit à la décision finale de l'utilisation de cette solution, ne peut être écarté de l'actuelle analyse.

Il est donc difficile de démontrer la nécessité absolue de mettre en œuvre le système biométrique spécifique choisi par le Parlement plutôt qu'un autre. Il faut ainsi considérer que "nécessité" ne signifie pas que le procédé est inévitable, mais bien qu'il peut être considéré comme raisonnablement nécessaire dans le cadre spécifique de la réalisation de l'objectif visé. Il semble que dans le cadre circonscrit de la gestion du personnel de prévention et de surveillance - qui a un impact direct sur la sécurité du Parlement en général -, le traitement puisse être considéré comme raisonnablement nécessaire. Rappelons que le but ultime du traitement est la protection physique du personnel, des informations et des biens de l'institution.

En effet, au vu de l'importance de ces intérêts, le Parlement peut effectivement juger nécessaire d'adopter des mesures de sécurité spéciales, notamment la mise en place de systèmes de contrôle d'identité rigoureux des membres de la sécurité donnant lieu au traitement de données à caractère personnel en question.

La mise en œuvre de ce système biométrique spécifique ainsi que celui […] semblent être des mesures adéquates pour limiter la prise de poste frauduleuse.

Néanmoins, le CEPD remarque qu´à l'heure actuelle, la procédure de vérification consiste essentiellement en un processus de vérification […].

Le CEPD considère ce système moins respectueux de la vie privée qu'un système dans lequel la procédure de vérification consiste en un processus de vérification 1:1 dans le badge (un à un) – dans lequel les minuties seraient intégrées dans la carte du détenteur et comparées avec les minuties scannées (à des fins de vérification), sur place, à l'aide du lecteur/scanneur de données biométriques. La comparaison/vérification serait effectuée localement par le lecteur de données biométriques, […]. Le CEPD est favorable à ce système, qui empêche toute utilisation ultérieure illicite et attaque de hameçonnage, qui sont généralement le corollaire de l'utilisation de bases de données[2].

Sur la base de son approche constante relative à des traitements de données biométriques[3], le CEPD ne peut entièrement soutenir l'approche prise par le Parlement tant que le système actuellement utilisé demeure en l'état. Bien que le Parlement ait annoncé son intention de migrer le système actuel vers ce deuxième système de vérification 1 :1, il n'y a pas à l'heure actuelle d'échéancier précis pour une telle migration. Le CEPD demande donc au Parlement de mettre tout en œuvre afin d'effectuer cette migration selon un échéancier précis à fournir.

[2] Voir l'avis sur une notification de contrôle préalable reçue du délégué à la protection des données de la Banque centrale européenne concernant l'intégration dans un système de contrôle d'accès préexistant d'une technologie d'analyse de l'iris pour les zones hautement sécurisées de la BCE, 14 février 2008 (2007-501), disponible sur le site du CEPD.

[3] Voir note de bas de page 1.

3.3. Qualité des données

Adéquation, pertinence et proportionnalité : en vertu de l'article 4, paragraphe 1, point 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 s'agit du principe de qualité des données.

Concernant les données biométriques, le CEPD note que le système est basé sur un modèle biométrique de contour de main.

Le type de données collectées, les caractéristiques biométriques de la main et des informations d'identification connexes, correspond aux données requises pour l'exploitation du système sur la base de données biométriques. De ce point de vue, le CEPD souligne que les données collectées pourraient être jugées adéquates et pertinentes aux fins du traitement.

Loyauté et licéité : l'article 4, paragraphe 1, point a), du règlement requiert que les données soient traitées loyalement et licitement. La question de la licéité a été analysée plus haut (voir le point 3.2), tandis que celle de la loyauté est étroitement liée à la question de l'information des personnes concernées, traitée ci-après au point 3.9.

Exactitude : selon l'article 4, paragraphe 1, point d), du règlement, les données à caractère personnel doivent être *«exactes et, si nécessaire, mises à jour ; 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»*.

En l'espèce, les données à caractère personnel concernées par le traitement comprennent des données biométriques, utilisées à des fins de contrôle d'identité. Certaines caractéristiques clés des systèmes biométriques ont un impact direct sur le niveau d'exactitude des données générées aux cours des phases d'enrôlement ou d'identification inhérentes à ce type de système. Selon que le système biométrique est établi d'une manière qui intègre ces éléments clés ou non, l'exactitude des données constituera (ou non) un paramètre à prendre en compte.

Le CEPD a analysé, dans des avis précédents relatifs aux contrôles d'accès, les règles à suivre lors de la mise en œuvre de systèmes biométriques. L'analyse suivante décrit ces éléments clés et évalue dans quelle mesure ces éléments ont été pris en considération dans le dispositif de vérification biométrique du Parlement.

Premièrement, toute phase d'enrôlement doit prévoir des moyens d'identification alternatifs des personnes qui ne sont pas éligibles, même temporairement, à la procédure d'enrôlement, par exemple en raison d'empreintes de mains endommagées. Cette procédure est généralement qualifiée de ***«procédure de secours»***[4]. En ce qui concerne l'enrôlement, le terminal valide ou refuse l'enrôlement et ce refus a lieu en cas de mauvaise qualité de l'enrôlement, etc.

Ensuite, dans la phase d'utilisation de la technologie, il est également possible que la vérification biométrique ne soit pas possible. Le CEPD note qu'il est prévu la mise en place

[4] Pour une description des principes de protection des données applicables dans le cadre des procédures de secours, voir l'avis du Contrôleur européen de la protection des données sur le projet de règlement du Conseil (CE) portant fixation de la forme des laissez-passer délivrés aux membres et aux agents des institutions, JO C 313 du 20.12.2006, p. 36.

d'une telle solution de secours dans le cas d'une impossibilité de vérification biométrique (la notification utilise l'appellation d'erreur du système). En effet, dans un tel cas, […]

Le CEPD note également qu'une autre mesure, visant à assurer l'exactitude des données, est mise en œuvre par la technologie employée. Si une personne n'utilise pas les appareils régulièrement, les données recueillies au moment de la vérification ne correspondront plus aux données stockées. Ceci s'explique par le fait que les mains humaines changent naturellement (gain ou perte de poids, changement d'articulations avec l'âge, etc.). Pour éviter ce problème, chaque fois qu'une mesure/vérification est faite, une moyenne des mesures est réalisée automatiquement et stockée sur le dispositif en tant que données renouvelées ; les données précédentes sont remplacées par les nouvelles données renouvelées.

Le CEPD juge ces procédures de secours satisfaisantes à la lumière de l'article 4.1.a.

3.4. Conservation des données

En vertu de l'article 4, paragraphe 1, point e), du règlement, les données à caractère personnel 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.

En ce qui concerne la durée de la conservation actuellement prévue […], le CEPD note que la durée établie pour les différentes catégories de données liées à l'identification et aux caractéristiques biométriques, pourrait être jugée justifiée.

Cependant, au regard des commentaires déjà émis […], la durée de conservation […] devra être revue pour établir une durée de conservation appropriée, […].

3.5. Transfert des données

Des transferts au titre de l'Article 7 du règlement sont prévus. Le CEPD rappelle que l'article 7 du règlement autorise les transferts de données à caractère personnel s'ils sont *«nécessaires à l'exécution légitime de missions relevant de la compétence du destinataire»*. Aux fins du respect de cette disposition, lors du transfert de données à caractère personnel, le responsable du traitement doit s'assurer que i) le destinataire possède les compétences appropriées et que ii) le transfert est nécessaire. Le CEPD estime que ces conditions sont respectées dans le cas présent.

En effet, les données relatives aux prestations horaires seront transférées de l'unité planning aux autres unités compétentes de la DG PERS, à savoir l'unité "droits individuels et rémunération" et l'unité "gestion du personnel et des carrières". Ces transferts seront effectués de la base Planning à la base Streamline. Lorsqu'applicable, les données sont transférées vers l'unité en charge de la gestion des absences médicales. Ces destinataires devront traiter les données pour les finalités pour lesquelles celles-ci leurs ont été envoyées, dans le respect de l'article 7 du règlement.

3.6. Traitement du numéro personnel ou de l'identifiant unique

L'article 10, paragraphe 6, du règlement dispose que *"le contrôleur européen de la protection des données détermine les conditions dans lesquelles un numéro personnel ou tout autre identifiant utilisé de manière générale peut faire l'objet d'un traitement par une institution ou un organe communautaire"*. Le présent avis n'établira pas les conditions générales de

l'utilisation d'un numéro personnel, mais envisagera les mesures spécifiques nécessaires dans le contexte de la vérification biométrique au sein du Parlement.

Le CEPD a d'ores et déjà précisé, dans un précédent avis de contrôle préalable[5], le statut d'un numéro de carte à puce intégrée dans une carte. Le numéro d'identification associé à la carte à puce RFID fait partie des données à caractère personnel couvertes par le règlement n° 45/2001. En effet, ce numéro d'identification, lorsqu'il est utilisé pour évaluer le comportement d'un membre du personnel et qu'il est lié au numéro personnel (au nom d'une personne, comme c'est le cas dans le présent dossier), donne lieu à un traitement de données à caractère personnel, nécessitant dès lors le respect des principes de protection des données.

L'utilisation du numéro personnel est nécessaire parce que l'identifiant de la carte est communiqué au système de contrôle biométrique. Dans le cas présent, l'utilisation du numéro personnel des membres du personnel aux fins de la vérification des données relatives au droit d'accès dans le système est raisonnable si l'on considère que ce numéro est utilisé pour identifier la personne dans le système et permet ainsi de garantir l'exactitude des données. Il n'y a aucune raison de déterminer d'autres conditions en l'espèce.

3.7. Droits d'accès et de rectification

Aux termes de l'article 13 du règlement, *«(l)a personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement (...) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données»*. L'article 14 garantit aux personnes concernées le droit de rectifier des données inexactes ou incomplètes.

La notification et déclaration de confidentialité contiennent ces informations (voir ci-dessus "point 2 les faits"). De plus, la notification prévoit également la politique de verrouillage/effacement de données sur demande légitime et motivée des personnes concernées.

Dans les cas où l'article 20 s'appliquerait (par exemple dans le cas d'enquêtes), le CEPD souligne au Parlement qu'il convient de l'appliquer de manière restrictive et au cas par cas.

En conclusion, le CEPD estime que les conditions visées aux articles 13 et 14 du règlement sont remplies moyennant une application au cas par cas dans le cadre de l'application de l'article 20 du règlement.

3.8. Information des personnes concernées

En vertu des articles 11 et 12 du règlement, les responsables de la collecte des données à caractère personnel doivent informer les personnes de la collecte de leurs données. Par ailleurs, ces personnes sont en droit d'être informées, notamment, des finalités du traitement, des destinataires des données et de leurs droits spécifiques en tant que personnes concernées.

Le Parlement a transmis au CEPD un projet de déclaration de confidentialité destinée aux personnes concernées (les agents) qui utiliseront le système de vérification biométrique. Le

[5] Voir l'avis sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Commission européenne à propos de la «mise en œuvre du Flexitime spécifique à la DG INFSO», 19 octobre 2007 (2007-218).

Parlement n'a pas précisé cependant à quel moment et comment cette déclaration sera rendue disponible aux personnes concernées.

L'information se fera également via une formation aux agents nouvellement recrutés à laquelle le DPD du Parlement participe.

En ce qui concerne la déclaration de confidentialité, le CEPD a également examiné le contenu des informations fournies afin de vérifier s'il satisfaisait aux exigences des articles 11 et 12 du règlement. Le CEPD note que les données relatives aux prestations horaires et aux absences médicales sont transférées aux unités "droits individuels et rémunération", "gestion du personnel et des carrières" et "gestion des absences médicales" le cas échéant (voir point 3.5). Ces trois unités sont donc destinataires de données qui ont toute leur importance pour les personnes concernées. Afin d'assurer un traitement de données loyal, la déclaration de confidentialité doit mentionner de quelles données chaque unité est destinataire et ce, pour quelles finalités.

Il s'ensuit que cette information sur l'origine des données traitées dans le cadre des traitements connexes mentionnés ci-dessus doit aussi apparaitre dans les déclarations de confidentialité correspondantes (gestion des prestations, gestion des congés, gestion des absences médicales, etc.). Les notifications correspondantes doivent être mises à jour le cas échéant.

3.9. Sécurité

En vertu de l'article 22 du règlement, le responsable du traitement doit mettre 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.

Dans le cas présent, et comme mentionné précédemment, le choix de la solution spécifique est aussi lié au fait que cette solution est actuellement utilisée par la société de gardiennage externe sous contrat avec le Parlement. Etant donné les changements de responsabilités, il serait opportun pour le Parlement de revoir l'analyse de risques de façon à déterminer quels sont les contrôles à mettre en œuvre pour diminuer les risques à un niveau acceptable pour le Parlement.

[…]

De plus, le CEPD attire l'attention du Parlement sur les considérations techniques suivantes, […]:
[…]

Conclusion

Le traitement proposé ne paraît pas entraîner de violations des dispositions du règlement (CE) n°45/2001 pour autant qu'il soit tenu compte des recommandations faites ci-dessus. Cela implique, en particulier, que le Parlement :

- mette tout en œuvre afin d'effectuer des modifications du système actuel […], et de fournir au CEPD un échéancier pour ces modifications ;
- informe clairement le personnel concerné des destinataires des différentes catégories de données personnelles et mettent à jour l'information donnée aux personnes concernées dans le cadre des traitements connexes (voir point 3.8) ;

- informe le CEPD sur la manière et sur le moment où la déclaration de confidentialité sera fournie aux personnes concernées.

De plus, en ce qui concerne les aspects de sécurité de la solution, le CEPD recommande que le Parlement :

- […]

Finalement, en ce qui concerne le transfert de données vers Securitas, le CEPD recommande au Parlement :

- […]

Fait à Bruxelles, le 15 mai 2014