ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DD200013		1er avril 2020

Objet : avis relatif à une demande d'utilisation d'un système de badge par la zone de police de xxx

L'Organe de contrôle de l'information policière (ci-après 'le COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 *relative* à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (M.B. du 5 septembre 2018, ci-après la "LPD"), en particulier l'article 59, § 1er, 2e alinéa, l'article 71 et le titre VII, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, en particulier l'article 4, § 2, quatrième alinéa.

Vu la loi du 5 août 1992 sur la fonction de police (ci-après la 'LFP'), en particulier l'article 44/6.

Vu la demande d'avis du Délégué à la protection des données de la zone de police de xxx ;

Vu le rapport de Monsieur Frank Schuermans, membre-conseiller à l'Organe de contrôle ;

Émet, le 1er avril 2020, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a profondément modifié les tâches et les missions de l'Organe de contrôle. L'article 4 § 2, quatrième alinéa de la loi organique du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après la 'LCA') dispose que pour les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle.

2. Cela signifie notamment que l'Organe de contrôle est également compétent lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socio-économiques ou de traitements de ressources humaines. L'Organe de contrôle doit être consulté dans le cadre de la préparation d'une législation ou d'une mesure réglementaire liée au traitement de données à caractère personnel par les services de police de la police intégrée (voir l'article 236 § 2 de la loi sur la protection des données[3], l'article 36.4 du RGPD et l'article 28.2 de la Directive Police-Justice). Dans ce cadre, l'Organe de contrôle a pour mission d'examiner si l'activité de traitement envisagée par les services de police est conforme aux dispositions des Titres 1er (pour les traitements non opérationnels)[4] et 2 (pour les traitements opérationnels) de la loi sur la LPD[5]. En outre, le COC a également une mission d'avis d'initiative, prévue à l'article 236 § 2 de la LPD, et une mission d'information générale du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

3. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou de police judiciaire, l'Organe de contrôle émet un avis, soit d'initiative, soit à la demande du gouvernement ou de la Chambre des représentants, d'une autorité administrative ou judiciaire ou d'un service de police concernant toute question relative à la gestion de l'information policière, telle que régie dans la section 12 du chapitre 4 de la loi sur la fonction de police[6].

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données ou 'RGPD'*).*

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après la 'Directive Police-Justice' ou *LED* (*Law Enforcement Directive*)).

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après la 'LPD')

[4] Article 4, § 2, quatrième alinéa de la LCA.

[5] Article 71, § 1er, troisième alinéa de la LPD.

[6] Article 236, § 2 de la LPD.

4. Enfin, l'Organe de contrôle est également chargé du contrôle de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel telles que visées aux articles 44/1 à 44/11/13 de la loi sur la fonction de police et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois vis-à-vis des services de police, de l'Inspection générale de la police fédérale et de la police locale (ci-après l' 'AIG'), telle que visée dans la loi du 15 mai 2007 sur l'Inspection générale, et de l'Unité d'information des passagers (ci-après 'BELPIU'), telle que visée dans le Chapitre 7 de la loi du 25 décembre 2016[7].

II. Objet de la demande

5. L'Organe de contrôle de l'information policière a reçu une demande d'avis de la zone de police de xxx concernant l'utilisation d'un système de badges par la zone ainsi que l'utilisation et l'analyse des logs de ces badges.

Ces badges nominatifs doivent être utilisés pour pénétrer dans l'hôtel de police de la zone, pour utiliser les multicopieurs, pour la distribution et la réception ponctuelle de matériel logistique nécessaire à l'accomplissement des missions de police et pour entrer dans le parking. Seuls les membres du personnel peuvent accéder audit parking.

En outre, la demande d'avis indique que l'utilisation des badges nominatifs sera contrôlée, notamment pour le stationnement dans le parking.

6. La zone souhaite mettre à jour une directive interne relative à l'utilisation des badges eu égard aux règles en vigueur en matière de protection des données.

Le Délégué à la protection des données (ci-après le *DPO*) produit deux raisonnements. Le premier renvoie au contrôle pur et simple par le chef de corps de l'accès des membres de la zone au parking sur base d'une banque de données (ci-après la 'banque de données des badges') qui reprend les plaques d'immatriculation déclarées par les membres du personnel.

Le *DPO* demande plus précisément des éclaircissements quant à la notion de consentement qui peut constituer une base de licéité d'un traitement de données effectué pour des finalités autres que des finalités opérationnelles.

[7] Article 71 § 1er, troisième alinéa *juncto* article 236, § 3 de la LPD.

Celui-ci se réfère à une FAQ de la police fédérale qui indique que «*l'utilisation, à des fins de contrôle (y compris disciplinaire), de données à caractère personnel issues du système de badge est autorisée si les membres du personnel y ont consenti*».

7. Le second raisonnement renvoie aux missions de police administrative qui incombent aux services de police, par lesquelles ceux-ci sont tenus de contrôler les lieux qui leurs sont accessibles et d'opérer une surveillance générale. Sur cette base, une première vérification dans la banque de données des badges aurait lieu ainsi qu'une deuxième vérification dans la banque carrefour des véhicules (ci-après la 'DIV') afin que les véhicules qui ne seraient pas identifiés via la première consultation puissent l'être.

Ces contrôles pourraient mener à des sanctions disciplinaires.

8. Les traitements de données qui sont envisagés ci-dessus tombent sous la compétence de l'Organe de contrôle. En effet, celui-ci est compétent[8] pour tous les traitements de données à caractère personnel effectués par les services de police au sens de l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégrée, structurée à deux niveaux (ci-après la 'LPI'), que ceux-ci soient exercés dans le cadre du RGPD ou dans le cadre du Titre II de la loi de la LPD.

Eu égard aux questions posées ci-dessus, il y a lieu de déterminer dans un premier temps si un(des) traitement(s) de données à caractère personnel existe(nt) au sens des règles en matière de protection des données, et si oui, lesquels, et dans un deuxième temps de déterminer qui est responsable du traitement ainsi que la(es) base(s) de licéité du(es) traitement(s).

III. <u>Analyse</u>

III.1. Traitement de données à caractère personnel

9. L'utilisation d'un système de badging nominatif requiert la collecte de données à caractère personnel afin de gérer les accès à certains lieux ou services, en l'occurrence au bâtiment, au parking et à la distribution/réception de matériel ainsi qu'aux multicopieurs.

Cette collecte de données constitue un traitement de données à caractère personnel au sens du RGPD[9]. Ces données alimentent une banque de données des badges, créée pour la gestion des accès.

De plus, la consultation des logs afin d'opérer un contrôle des accès opérés avec les badges nominatifs constitue un autre traitement de données à caractère personnel.

[8] Articles 71 de la LPD et 4, §2, alinéa 4 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.
[9] Art. 4 du RGPD.

Mais encore, la demande d'avis fait référence à la consultation de la DIV dans le cadre du contrôle des accès aux parkings : les véhicules stationnés seraient d'abord contrôlés au moyen de la banque de données des badges et ensuite, s'ils ne peuvent être identifiés, via la DIV. Cette consultation d'une autre banque de données constitue un traitement de données à caractère personnel.

10. Trois traitements différents de données à caractère personnel sont donc identifiés. Ces traitements doivent obéir à certaines règles et principes selon les finalités pour lesquelles ils sont réalisés.

III.2. Utilisation d'un système de badging

III.2.1. Finalités des traitements et base(s) légale(s) applicable(s)

11. Dans le cadre de la présente demande et afin de respecter les principes généraux des traitements de données[10], il y a lieu d'identifier les finalités des traitements identifiés afin que la(es) base(s) légale(s) applicables soient déterminées.

De la demande d'avis, il apparaît que le premier traitement à savoir l'utilisation d'un système de badging nominatif serve à :

- entrer dans l'hôtel de police de la zone de xxx ;
- utiliser des multicopieurs ;
- distribuer et recevoir de manière ponctuelle du matériel logistique nécessaire à l'accomplissement des missions de police ;
- accéder au parking non accessible au public géré par la zone de police.

Ces finalités de traitements ne constituent pas des finalités de police administrative ou judiciaire définies à l'article 27 de la LPD (traitements à des fins opérationnelles).

12. Le deuxième traitement identifié consiste en un contrôle et une vérification des accès via la consultation des logs des badges avec la banque de données des badges :

- contrôle des entrées dans l'hôtel de police de la zone de xxx ;
- contrôle des utilisations des multicopieurs ;
- contrôle de la distribution et de la réception ponctuelles de matériel logistique nécessaire à l'accomplissement des missions de police ;
- contrôle des accès au parking non accessible au public géré par la zone de police ;
- contrôle des véhicules présents pour s'assurer que ceux-ci appartiennent aux membres du personnel de la zone ;

[10] Art. 5 du RGPD et 28 de la LPD.

- contrôle des véhicules présents pour identifier les propriétaires des véhicules éventuellement mal stationnés.

Ces finalités ne constituent pas non plus des finalités de police administrative ou judiciaire.

Ces deux traitements, bien qu'ayant chacun des finalités différentes, tombent sous le champ d'application du RGPD.

Dès lors, le second raisonnement présenté par le *DPO,* basé sur les missions de police administrative des services de police ne peut s'appliquer en l'espèce: le RGPD s'applique à l'utilisation d'un système de badges par la zone ainsi qu'à la consultation des logs et de la banque de données des badges à des fins de contrôle.

13. En ce qui concerne le troisième traitement à savoir le contrôle des véhicules stationnés dans le parking de la zone via la DIV, la demande d'avis indique qu'il s'agit d'une consultation qui vise l'efficacité des contrôles d'accès. Cette consultation de la DIV ne serait effectuée que pour la gestion du stationnement du parking interne et lorsque la banque de données des badges ne suffit pas.

Cette consultation est justifiée dans la demande d'avis par référence aux missions de police administrative dans le cadre desquelles une surveillance générale et des contrôles des lieux accessibles aux services de police sont exercés. Le parking intérieur de la zone est assimilé dans la demande d'avis à un lieu accessible aux services de police.

Néanmoins, comme l'indique le raisonnement du présent point, les finalités exposées au paragraphe 12 ne tombent pas sous le champ de l'article 27 de la LPD et il ne peut donc être renvoyé aux missions de police administrative pour justifier un contrôle dans la DIV pour des finalités non opérationnelles de gestion du parking interne de la zone de police de xxx.

14. L'Organe de contrôle rappelle que l'accès à la DIV par les services de police est expressément prévu dans le cadre de l'exécution de leurs missions légales de police administrative et judiciaire[11], parmi lesquelles ne figure pas la gestion du stationnement dans un parking interne à la zone de police.

La demande d'avis indique qu'une telle consultation serait utile par exemple, si une plaque d'immatriculation contrôlée ne figure pas dans la banque de données des badges.

[11] Loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules ; Décision du Comité sectoriel pour l'Autorité Fédérale AF n°53/2016 du 15 décembre 2016.

Toutefois, les données qui sont traitées doivent être tenues à jour[12], ce qui implique notamment que le responsable du traitement, veille à ce que les données comprises dans sa banque de données soient exactes et complètes. Ainsi, une organisation et une communication interne efficaces doivent permettre de tenir les données de la banque de données des badges à jour et de, par exemple, permettre aux membres du personnel qui disposent de plusieurs véhicules qu'ils utilisent indifféremment de tous les déclarer, ou encore de déclarer un véhicule de remplacement occasionnel.

La délimitation claire des finalités d'utilisation des badges nominatifs et des contrôles qui en découlent rendent le contrôle des véhicules dans la DIV incompatible avec le principe de proportionnalité ainsi qu'avec les conditions d'accès des services de police à cette banque de données.

15. L'Organe de contrôle demande par conséquent que la possibilité de consultation de la DIV dans le cadre des contrôles de l'utilisation des badges par les membres du personnel de la zone de police de xxx soit retirée du projet de la nouvelle directive interne eu égard à son incompatibilité avec les finalités de traitement énoncées.

III.2.2. Responsable du traitement

16. Dans le cadre de la présente demande, il y a lieu de déterminer qui décide de recourir à l'utilisation d'un système de badging et donc d'identifier le responsable du traitement. Le responsable du traitement est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* » par le RGPD[13].

En l'espèce, c'est le chef de corps de la zone de police de xxx qui a décidé de recourir au système de badging nominatif et de procéder à certains contrôles de l'utilisation des badges.

Le chef de corps de la zone de police de xxx est donc le responsable du traitement pour le badging et pour les contrôles des logs qui en découlent.

17. Dans l'hypothèse où le chef de corps fait appel à un partenaire externe afin de mettre en place le système de badging, ce partenaire externe doit être considéré comme un sous-traitant du chef de

[12] Art. 5 du RGPD.
[13] Art. 4, 7° du RGPD.

corps[14]. En effet, dans la mesure où seul le chef de corps détermine les finalités du traitement, le partenaire externe se limite à traiter des données à caractère personnel pour le compte de celui-ci.

III.2.3. Base de licéité du traitement

18. Vu les conclusions du point précédent, le présent point se concentrera sur les bases de licéité des deux traitements suivants : l'utilisation d'un système de badging nominatif et la consultation des logs et de la banque de données des badges pour le contrôle des accès réalisés par badge.

L'article 6 du RGPD prévoit différentes bases de traitement et indique qu'au moins une de celles-ci doit être remplie afin qu'un traitement soit licite.

Le premier raisonnement du *DPO* faisait référence au consentement des membres du personnel.

Le consentement des personnes concernées[15], en l'occurrence des membres du personnel de la zone de police, ne peut constituer une base de licéité pour la mise en place d'un système de badges nominatifs et pour la vérification des logs à des fins de contrôle. En effet, les membres du personnel se trouvent dans une relation de travail avec le responsable du traitement (le chef de corps), une relation hiérarchique même, ce qui a pour conséquence que leur consentement ne peut être considéré comme libre et spécifique tel que le RGPD le requiert[16]. Cette base de traitement n'est donc pas applicable.

19. Les bases de l'article 6, §1er, b), d), e) et f) du RGPD sont également à écarter en l'espèce.

En effet, l'installation d'un système de badging et la consultation des logs à des fins de contrôle renvoient, comme cela a déjà été exposé au point II.2.1., à des finalités autres que des finalités de police administrative ou judiciaire (finalités opérationnelles) : il est question de gestion et d'administration du personnel, de dotation en matériel et de gestion du stationnement à l'intérieur du parking accessible uniquement aux membres de la zone disposant d'un badge[17].

Dès lors, le chef de corps a recours aux badges à des fins de bonne gestion de la zone, ce qui entre dans le cadre de ses obligations légales en termes de direction et d'organisation de la zone[18]et ce qui signifie que l'article 6, §1er, c) du RGPD constitue la base légale.

---

[14] Article 4, alinéa 1er, 8° du RGPD.
[15] Article 6, §1er, alinéa 1er, a) du RGPD.
[16] Articles 4, 11) et 7 du RGPD et Considérants 32, 33, 42 et 43.
[17] Zone de police de xxx, *Demande d'avis juridique relative à l'utilisation d'un système de badge*, CS-1708/2020, 06 mars 2020, p. 2 – 3.
[18] Art. 44 de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (LPI).

20. Toutefois, étant donné que les contrôles sur base des logs des badges peuvent donner lieu à des sanctions disciplinaires, l'Organe de contrôle rappelle que la zone de police est tenue d'organiser au préalable un comité de concertation avec les organisations syndicales représentées au sein de la zone[19] afin de déterminer notamment : comment les membres du personnel vont être notifiés *a priori* de la possibilité d'utilisation des logs des badges à des fins de contrôle ; de la manière dont vont se dérouler ces contrôles ; de leur étendue ; des raisons qui peuvent justifier un contrôle ; des périodes qui peuvent être visées ; des conséquences qui peuvent découler des contrôles (sanctions disciplinaires, pénales, contrôles ponctuels de qualité, …) ; …

III.2.4. Information et droits des personnes concernées

21. L'Organe de contrôle rappelle que des droits de la personne concernée sont prévus par le RGPD.

Ainsi, les informations visées à l'article 13 du RGPD doivent être mises en toute exhaustivité à la disposition des membres du personnel de la zone, dans le respect du principe de transparence[20].

Parmi ces informations doivent entre autres figurer l'identité et les coordonnées du responsable du traitement, les coordonnées du Délégué à la protection des données de la zone de police[21], les finalités du traitement et les intérêts légitimes poursuivis par le chef de corps et l'identification des données collectées. Eu égard aux finalités annoncées, il convient dès lors dans un souci de proportionnalité[22] de collecter soit le matricule du membre du personnel, soit son nom/prénom, ainsi que son/ses numéro(s) de plaque d'immatriculation.

Si pour la création de la banque de données des badges, la zone de police utilise des données dont elle dispose déjà dans d'autres banques de données, il y a lieu de vérifier si les finalités énoncées dans le présent sont compatibles avec les finalités pour lesquelles les données ont été collectées initialement.

De plus, les informations concernant le droit d'accès doivent également être disponibles[23].

III.2.5. Obligations du responsable du traitement

22. Conformément à l'article 24 du RGPD, le chef de corps est tenu, en tant que responsable du traitement, de mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour

[19] Loi du 24 mars 1999 organisant les relations entre les autorités publiques et les organisations syndicales du personnel des services de police.
[20] Art. 5 du RGPD.
[21] Art. 144 de la LPI.
[22] Art. 5 du RGPD.
[23] Art. 13 du RGPD.

que les traitements de données effectués soient conformes aux règles en vigueur en matière de protection des données.

23. Le fichier qui va associer le badge au membre du personnel constitue une banque de données qui doit être déclarée dans le registre de traitements REGPOL[24]. La durée de conservation des données doit également être définie au préalable, ou à défaut, les critères permettant de définir cette durée doivent être clairement indiqués (et communiqués aux membres du personnel).

24. Le chef de corps est également chargé de mettre en place toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité[25] suffisant comme par exemple la gestion des accès à la banque de données des badges.

Mais encore, le Délégué à la protection des données doit être averti de l'utilisation d'un système de badging ainsi que des traitements de données à caractère personnel qui en découlent et avoir accès à la banque de données[26].

25. Dans l'hypothèse où le chef de corps a fait appel à un partenaire externe pour la mise en place du système de badging, celui-ci doit s'assurer au préalable que le partenaire externe, sous-traitant, présente des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées afin que les droits des membres du personnel soient respectés.

La zone et le partenaire externe doivent être liés par un contrat écrit qui répond à toutes les exigences inscrites à l'article 28 du RGPD, et qui définit notamment l'objet du traitement, le type de données et les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement. Les modalités d'accès par la zone aux données traitées par le partenaire externe doivent également être prévues dans le contrat entre les deux parties.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière,

invite le demandeur à tenir compte des remarques susmentionnées,

demande qu'il soit tenu compte des paragraphes 15 et 18 à 20.

Avis approuvé par l'Organe de contrôle de l'information policière le 1er avril 2020.

[24] Art. 145 de la LPI.
[25] Art. 32 du RGPD.
[26] Art. 63 à 65 de la LPD et 144 de la LPI.

Pour l'Organe de contrôle,

Frank SCHUERMANS (sé.)
Membre-conseiller