ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DD220019		13.02.2024

Objet: Avis d'initiative concernant le traitement de données à caractère personnel de membres du personnel d'une entité de police aux fins de gestion des accès à l'armement – Traitement d'empreintes digitales de membres du personnel pour la même finalité

L'Organe de contrôle de l'information policière (ci-après dénommé en abrégé « Organe de contrôle » ou « COC ») ;

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. 5 septembre 2018, ci-après dénommée en abrégé « loi relative à la protection des données » ou « LPD »), et en particulier l'article 59, §1er, 2e alinéa, l'article 71 et le Titre VII, spécifiquement l'article 236 ;

Vu la loi du 5 août 1992 *sur la fonction de police* (ci-après dénommée « LFP »), et en particulier les articles 3, 6° et 25/1 à 25/7 inclus ;

Vu l'article 236, §2, premier alinéa de la LPD, prévoyant la possibilité, pour l'Organe de contrôle, d'émettre des avis d'initiative ;

Vu l'article 237 de la LPD ;

Vu le rapport de Monsieur Ronny Saelens, membre-conseiller *a.i.* de l'Organe de contrôle.

Émet le 13.02.2024 l'avis suivant.

Table des matières

REMARQUE PRÉALABLE AU SUJET DE 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 remanié en profondeur les tâches et 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 dénommée en abrégé « LAPD ») dispose qu'à l'égard des 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. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque les services de police traitent des données à caractère personnel en dehors du cadre des missions de police administrative et judiciaire, par exemple en vue de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. Le COC est en outre investi aussi d'une mission d'avis d'office, prévue à l'article 236 §2 de la LPD, et d'une mission de sensibilisation du public, des personnes concernées, des responsables du traitement et des sous-traitants à la matière du droit à la protection de la vie privée et des données, prévue à l'article 240 de la LPD.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet des 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 matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

---

[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 dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).
[3] Article 4 §2, 4e alinéa de la LAPD.
[4] Article 71 §1er, 3e alinéa de la LPD.
[5] Articles 59 §1er, 2e alinéa et 236, §2 de la LPD.

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé « 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 dénommée en abrégé « BELPIU ») visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/14 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[6].

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281, §4 de la loi générale sur les douanes et accises du 18 juillet 1977, telle que modifiée par la loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers.

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (M.B. du 8 août 2022), de la (non) validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] **G**eïntegreerde politie – **P**olice **I**ntégrée.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

OBJET ET CONTEXTE DE L'AVIS

8. Dans le cadre de l'exercice de ses missions, l'Organe de contrôle a reçu plusieurs demandes d'information relatives au traitement d'empreintes digitales de membres du personnel pour la gestion des accès à des locaux spécifiques de bâtiments de police.

9. Eu égard à l'intérêt grandissant de certaines entités de police pour le traitement de données biométriques – en particulier les empreintes digitales – de membres du personnel dans le cadre de politiques de gestion des accès, et au caractère particulièrement sensible des données biométriques, l'Organe de contrôle a décidé de rédiger un avis d'initiative.

10. Cet avis porte sur la question de la légalité du traitement d'empreintes digitales de membres du personnel d'une entité de police pour la gestion des accès à l'armement.

Pour toute clarté, l'Organe de contrôle précise que seul le terme "armement" sera utilisé, comme englobant toutes les armes, individuelles, collectives ou particulières, y compris les moyens incapacitants, dont sont dotés les membres du personnel de la police intégrée ainsi que leurs munitions et leurs accessoires tels que visés à l'article 1er de l'arrêté royal du 3 juin 2007 *relatif à l'armement de la police intégrée, structurée à deux niveaux, ainsi qu'à l'armement des membres des services d'enquêtes des comités permanents P et R et du personnel de l'inspection générale de la police fédérale et de la police locale*[9].

11. Le présent se limite strictement à la question du traitement de données à caractère personnel (empreintes digitales) de membres des services de police dans le cadre d'une politique interne de gestion des accès à l'armement (la prise, la remise et l'entreposage des armes). Cette question est examinée en deux temps : d'une part, la licéité du traitement de données à caractère personnel aux fins de la gestion des accès à l'armement, et, d'autre part, la licéité, la nécessité et la proportionnalité du traitement d'une catégorie particulière de données, à savoir les empreintes digitales qui constituent des données biométriques.

[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. »* ; article 71 §1er de la LPD.
[9] Des éventuelles règles spécifiques à l'exercice de certaines missions de police (p. ex. pour la Direction des Unités Spéciales) ne sont pas prises en compte pour le présent avis.

12. Le traitement de telles données dans le cadre d'une politique interne de gestion des accès à d'autres équipements ou locaux, comme par exemple les locaux réservés aux armes saisies ou à un autre type de matériel tel que les radios, est exclu du présent avis.
Le présent avis ne se prononce donc pas sur le traitement de données à caractère personnel aux fins de la gestion des accès aux bâtiments de police. L'Organe de contrôle a récemment remis un avis relatif à un projet d'arrêté royal relatif à la sécurisation des bâtiments et complexes de bâtiments policiers[10].

13. L'Organe de contrôle attire l'attention sur le fait que l'analyse, les développements et les réflexions de l'avis d'initiative se concentrent sur les aspects de protection des données liés à la gestion de l'accès à l'armement et sont formulés sans préjudice de l'application d'autres législations.

14. L'analyse fonctionnelle de la gestion de l'armement doit prendre en compte les objectifs organisationnels, stratégiques et opérationnels de l'entité de police[11], et intégrer différentes analyses de risques et perspectives telles que, sans volonté d'exhaustivité, le bien-être au travail, l'organisation et la logistique internes (p. ex. la gestion du matériel, la gestion des horaires, …), la sécurité des données à caractère personnel[12] et de l'information, etc.
Concrètement, l'armement en tant qu'actif (matériel) de l'organisation nécessite la mise en place d'une politique de gestion résultant de la conjonction d'obligations légales notamment en matière de fonctionnement et d'organisation internes, d'armement, et de gestion des risques et de protection des données.

15. Le COC rejoint sur ce point l'approche holistique encouragée par l'AIG dans son récent rapport faisant état du bilan des dernières années d'inspections relatives à l'armement de la police intégrée[13], qui, bien que principalement axé sur le contrôle de l'application de la circulaire GPI 62[14], encourage le développement d'approche méthodique et systémique pour parvenir à un niveau de sécurité optimal, prenant en compte la corrélation entre plusieurs risques, en particulier ceux liés à la sécurité des bâtiments et ceux liés à l'entreposage et la garde de l'armement.

[10] Une demande d'avis relative à un arrêté royal relatif à la sécurisation des bâtiments et complexes de bâtiments policiers a été soumise le 3 avril 2023 à l'Organe de contrôle (référence DA230015). Dans l'avis DA230015, l'Organe de contrôle se prononce sur les exigences d'une base légale relative au traitement d'empreintes digitales. Cet aspect est davantage développé dans le présent avis.
[11] Particulièrement : la Loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux*, la Loi du 5 août 1992 *sur la fonction de police*, les normes en matière de sécurité de l'information, la Loi du 4 août 1996 *relative au bien-être des travailleurs lors de l'exécution de leur travail* et le Code sur le bien-être au travail, la Circulaire CP3 du 29 mars 2011 *relative au 'système du contrôle interne' dans la police intégrée, structurée à deux niveaux*, le Plan National de Sécurité, les lettres de missions visées à l'article 72 de la loi du 26 avril 2002 *relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police*, etc. …
[12] Article 32 du RGPD.
[13] Inspection générale de la police fédérale et de la police locale, *GPI 62 relative à l'armement de la police intégrée – Bilan des dernières années d'inspections*, juillet 2022, p. 29, publié sur www.aigpol.be, consulté le 6 novembre 2023.
[14] Circulaire GPI 62 du 14 février *2008 relative à l'armement de la police intégrée, structurée à deux niveaux* telle que modifiée le 19 octobre 2017. Voir infra.

16. La gestion des risques liés à l'armement se doit d'être dynamique et évolutive en ce sens qu'elle doit être adaptée en fonction de l'expérience acquise, de l'évolution des méthodes de travail ou des conditions de travail et aussi des moyens technologiques.
Elle se traduira entre autres par la mise en place d'une conjugaison de mesures appropriées telles que, sans volonté d'exhaustivité, des infrastructures adéquates, des formations et le traitement de données à caractère personnel dans le respect des principes de nécessité et de proportionnalité.

LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL AUX FINS DE LA GESTION DES ACCÈS À L'ARMEMENT

CADRE JURIDIQUE - LICÉITÉ DU TRAITEMENT[15]

17. Dans les demandes d'information qu'il a reçues, l'Organe de contrôle a remarqué que les motifs principalement avancés pour justifier l'utilisation d'empreintes digitales dans le cadre de la gestion des accès à l'armement sont la sécurité (des membres du personnel et d'autrui) et le contrôle du respect des conditions de travail.
De manière générale, le COC est d'avis que l'utilisation des termes « *à des fins de sécurité* » est trop vague pour définir une finalité de traitement, certainement lorsque le traitement de données en question concerne des données particulières (sensibles)[16].

18. L'Arrêté royal du 3 juin 2007 relatif à l'armement de la police intégrée, structurée à deux niveaux[17] ('Arrêté Armement') et la circulaire GPI 62, qui exécutent et explicitent l'article 141 de la Loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux* (LPI), établissent des obligations et des responsabilités relatives à l'armement, sa détention, son port, son transport, son entreposage et sa garde.

19. La gestion et la dotation de l'armement représentent par conséquent un aspect particulier des obligations en matière d'organisation, de fonctionnement et de gestion internes incombant respectivement au commissaire général, aux directeurs généraux, aux directeurs coordonnateurs

[15] Article 6 du RGPD.
[16] Organe de contrôle de l'information policière, *Avis d'initiative concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail*, BD200007, 17 août 2020 ; Organe de contrôle de l'information policière, *Avis d'initiative suite aux constatations dans le cadre d'une enquête sur l'utilisation de bodycams*, CON190008, 8 mai 2020.
[17] Arrêté royal du 3 juin 2007 *relatif à l'armement de la police intégrée, structurée à deux niveaux, ainsi qu'à l'armement des membres des services d'enquêtes des comités permanents P et R et du personnel de l'inspection générale de la police fédérale et de la police locale*.

administratifs et judiciaires ainsi qu'aux chefs de corps vis-à-vis de leur direction ou de leur corps de police locale[18].

20. L'armement doit en effet être conservé dans un lieu sécurisé, hors de portée des tiers, conformément aux instructions, selon le cas, du Chef de corps, du Commissaire général, du Directeur général, du Directeur ou du Chef de service[19]. Lorsqu'il n'est pas emporté en missions, l'armement doit être entreposé dans un lieu sécurité dans une infrastructure abritant le lieu de travail[20].

21. La circulaire GPI 62 relative à l'armement de la police intégrée précise notamment que "*l'employeur doit prendre les mesures appropriées pour que seuls les membres du personnel qui ont reçu des instructions adéquates puissent être en contact avec l'armement et le manipuler et pour éviter le vol, la perte ou la détérioration*"[21] et que "l*es mesures mises en place doivent permettre que l'accès à l'armement soit limité au seul personnel autorisé et qu'un usage abusif par du personnel non autorisé soit impossible*"[22].

22. Dans ce cadre, une politique interne de gestion des accès à l'armement peut comprendre le traitement de données à caractère personnel ayant pour finalité que seuls les membres du personnel autorités puissent être en contact avec l'armement et le manipuler.

23. Le traitement mentionné ci-dessus ne constitue pas un traitement au sens de l'article 27 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (LPD). En d'autres termes, il n'est pas question dans ce cas de finalités de police administrative et judiciaire et les articles 44/1 et suivants de la LFP ne sont pas d'application.

24. Un tel traitement constitue un traitement de données à caractère personnel tombant sous le champ d'application du RGPD[23].
Le traitement de données à caractère personnel aux fins d'assurer la gestion des accès à l'armement constitue donc une obligation légale au sens de l'article 6.1, c) RGPD, qui résulte de la conjonction d'obligations légales en matière de fonctionnement et d'organisation internes, d'armement et de gestion des risques. Elle est issue d'une lecture combinée des dispositions suivantes :

- Loi du 7.12.1998 *organisant un service de police intégré, structuré à deux niveaux* (LPI) ;
    - Articles 44, 98 et 141 relatifs à la gestion et au fonctionnement internes ainsi qu'à l'équipement ;

[18] Articles 44 et 98 LPI.
[19] Article 19 de l'Arrêté Armement.
[20] Article 20 de l'arrêté Armement.
[21] Circulaire GPI 62, Chapitre Ier. Les mêmes règles sont d'application en ce qui concerne les munitions.
[22] Circulaire GPI 62, Chapitre VI, Section 2.
[23] Article 4, 2) du RGPD.

- L'Arrêté royal du 03.06.2007 *relatif à l'armement de la police intégrée, structurée à deux niveaux, ainsi qu'à l'armement des membres des services d'enquêtes des comités permanents P et R et du personnel de l'inspection générale de la police fédérale et de la police locale* (ci-après 'Arrêté armement') ;
    - Circulaire GPI 62 du 14.02.2008 *relative à l'armement de la police intégrée, structurée à deux niveaux* ;

25. Le traitement de données à caractère personnel de membres des services de police pour assurer la gestion des accès à l'armement est par conséquent fondé sur une obligation légale.
Le consentement[24] de la personne concernée (le membre du personnel de l'unité de police en l'espèce) ne saurait donc être invoqué comme base de licéité du traitement.
Comme l'Organe de contrôle l'a déjà développé dans plusieurs avis[25], cela s'explique par le déséquilibre (le lien hiérarchique) entre le membre du personnel (personne concernée) et l'autorité qui décide de mettre le traitement en œuvre (responsable du traitement)[26].

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

26. Le traitement de données à caractère personnel à des fins de gestion de l'accès à l'armement tombe donc sous le champ d'application du RGPD. Les principes et obligations du RGPD sont par conséquent également applicables à ce traitement. Il est renvoyé à cet égard aux articles pertinents du RGPD[27].
Le présent point insiste en particulier sur certains de ces aspects.

27. De manière générale, il incombe au responsable du traitement de s'assurer de la conformité du traitement et de la sécurité des données à caractère personnel traitées avant, au moment du traitement et pendant sa mise en œuvre[28]. Les mesures prises en réponse aux risques identifiés doivent être actualisées tout au long du traitement, selon un processus dynamique et continu de gestion des risques.
La documentation de toutes les étapes de la détermination du traitement (avis du DPO, analyses de risques, …) est importante et permet au responsable du traitement de démontrer la conformité du traitement à tout moment et donc aussi à la demande de l'autorité de contrôle.

[24] Article 6.1, a) du RGPD.
[25] Organe de contrôle de l'information policière, *Avis d'initiative concernant les situations dans lesquelles des citoyens filment des interventions de police et concernant la protection des données à caractère personnel et de la vie privée des fonctionnaires de police à l'égard de tiers pendant l'exécution de leurs missions policières*, DD200025, 22 novembre 2021 ; Organe de contrôle de l'information policière, *Avis d'initiative concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail*, BD200007, 17 août 2020 ; Organe de contrôle de l'information policière, *Avis d'initiative suite aux constatations dans le cadre d'une enquête sur l'utilisation de bodycams*, CON190008, 8 mai 2020 ; Organe de contrôle de l'information policière, *Avis relatif à une demande d'utilisation d'un système de badge par la zone de police de xxx*, DD200013, 1er avril 2020, consultables sur www.organedecontrole.be.
[26] Article 4.11 et considérants 32, 42 et 43 du RGPD.
[27] Complétés par le titre 1 de la LPD et l'article 145 LPI.
[28] Articles 5, 24 et suivants du RGPD.

PROTECTION DES DONNÉES DÈS LA CONCEPTION (*PRIVACY BY DESIGN*)

28. En vertu du cadre légal applicable, le responsable du traitement peut traiter des données pour la gestion de l'accès à l'armement mais il doit déterminer les modalités de ce traitement.

En application du principe de protection des données à caractère personnel dès la conception (*privacy by design*), le responsable du traitement doit veiller, dès la détermination des modalités du traitement, à l'évaluation de la nécessité et de la proportionnalité[29] du traitement des données au regard de la finalité visée.

A titre d'exemple et sans volonté d'exhaustivité :

- Quelles données sont nécessaires pour atteindre la finalité ?
- Quelles sont les opérations de traitement (collecte, conservation, effacement, etc. …) nécessaires ?
- Un coffre à arme individuel est-il utilisé ?
- Faut-il un traitement de données pour accéder au coffre à arme individuel ?
- Comment le coffre à arme individuel est-il accessible ? Par un badge ? Un Code ? Une clef ? etc. …
- Faut-il une armoire intelligente pour gérer le moyen d'accès (badge / clef / …) au coffre à arme individuel ?
- Comment accède-t-on au local d'armement ?
- Faut-il une armoire intelligente pour gérer le moyen d'accès au local d'armement (badge / clef / …) ?
- L'octroi de l'accès requiert-il une identification ou une authentification du membre du personnel ?
- Combien de temps les données devraient être conservées[30] ?
- Les accès sont-ils journalisés ? Dans l'affirmative, quelles données composent la journalisation ?
- Combien de temps la journalisation doit-elle être conservée ?
- Qui peut accéder à la journalisation et pour quelles finalités ?
- Mis à part les membres du personnel devant avoir accès à l'armement pour l'exercice de leurs missions, d'autres (catégories de) personnes doivent-elles pouvoir accéder au local et/ou aux armes (personnel d'entretien, armurier, prévention incendie, …) ? Dans l'affirmative, à quelles conditions ?
- …

[29] Article 5.1, b) et c) du RGPD (principes de minimisation des données et de limitation des finalités).
[30] Article 5.1, e) du RGPD.

29. A cet égard, les personnes clefs en lien direct ou indirect avec la mise en œuvre du traitement doivent être associées en temps utiles à la réflexion du responsable du traitement comme par exemple le Délégué à la protection des données (DPO) pour avis préalable et éclairé[31], un représentant des membres du personnel ayant accès à l'armement pour l'exercice de leurs missions, le membre du personnel compétent en matière de bien-être au travail, un membre du personnel chargé de l'infrastructure ICT, etc. …

30. Si le traitement de données à caractère personnel constitue une mesure – parmi d'autres – permettant de répondre au risque identifié inhérent à l'armement comme actif (matériel) de l'organisation, le responsable du traitement doit démontrer au moyen de l'évaluation de la nécessité et de la proportionnalité du traitement (principes de minimisation et de limitation) que le même résultat ne pourrait être obtenu autrement c'est-à-dire par des moyens moins invasifs sur le plan de la protection des données, comme par exemple le traitement d'autres (catégories de) données ou de moins de données[32].

ANALYSE D'IMPACT ET DE RISQUES (AIPD) ET SÉCURITÉ DU DONNÉES[33]

31. Outre les analyses de risques évoquées aux points précédents, une analyse d'impact et de risques du traitement envisagé sur la protection des données à caractère personnel (ci-après "AIPD" / *DPIA*[34]) est un préalable obligatoire lorsque le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques[35], comme par exemple lorsque des données biométriques sont concernées.

32. L'AIPD doit contenir *a minima*[36] une description systématique des opérations de traitement envisagées et des finalités du traitement, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, une évaluation des risques pour les droits et libertés des personnes concernées, et les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

[31] Articles 38 et 39 du RGPD.
[32] A toutes fins utiles, voir notamment les jurisprudences CEDH, BĂRBULESCU c. ROUMANIE, Requête no 61496/08, 5 septembre 2017 et CEDH, López Ribalda et autres c. Espagne, Requêtes nos 1874/13 et 8567/13, 17 octobre 2019, relatives aux critères auxquels les mesures des employés sur leur lieu de travail doivent se conformer pour ne pas enfreindre l'article 8.
[33] Article 32 du RGPD.
[34] *Data Protection Impact Assessment.*
[35] Article 35, §1er du RGPD.
[36] Article 35, §7 du RGPD.

33. C'est l'AIPD qui guidera le responsable du traitement[37] dans la détermination de modalités appropriées du traitement, et donc qui lui permettra de vérifier si les données qui sont appelées à être traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de minimisation des données)[38].

34. Le COC rappelle à cet égard que le Délégué à la protection des données (DPO) doit être sollicité dans le cadre de la réalisation de l'AIPD[39].

35. Les mesures[40] résultant de l'AIPD pour les droits et libertés des personnes concernées doivent permettre notamment de répondre aux points d'attention suivants (sans vouloir être complet) :

- Le traitement non autorisé ou illicite des données.
- La perte, la destruction ou les dégâts d'origine accidentelle des données.
- L'exécution d'activités de contrôle.
  Par exemple : le contrôle des accès à l'armement ; l'accès à la journalisation des accès à l'armement ; conditions et finalités de l'accès à la journalisation des accès à l'armement.
- Le retrait des droits.
  Par exemple : le retrait du droit d'accès à l'armement ; le contrôle de la conformité des droits d'accès octroyé.
- Confidentialité des données.
  Par exemple : méthode de cryptographie ; nécessité de la pseudonymisation des données ; nécessité de conservation de la donnée brute (p. ex. si conversion de la données en un code)
- Traçabilité / journalisation.
  Par exemple : données à caractère personnel et informations journalisées ; durée de conservation de la journalisation.
- Gestion des violations de données.
  Par exemple : répartition des rôles et responsabilités en cas de violation de données à caractère personnel ou d'incident de sécurité ; établissement et communication d'une procédure interne

[37] A toutes fins utiles, voir la Décision relative à l'adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement Général sur la Protection des données, 01/2019 du 16 janvier 2019, consultable sur https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf, consultée le 6 novembre 2023.
Recommandation d'initiative de l'Autorité de protection des données (APD) concernant l'analyse d'impact relative à la protection des données et la consultation préalable, 01/2018 du 28 février 2018, consultable sur https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf, consultée le 6 novembre 2023.
[38] Article 5, §1er, c) du RGPD.
[39] Article 35, §2 du RGPD et article 22 de la LPD.
[40] Article 5.1, f) du RGPD.

EXACTITUDE ET ACTUALISATION DES DONNÉES[41]

36. Il revient au responsable du traitement de mettre en place les mesures techniques et organisationnelles nécessaires et appropriées pour s'assurer du fait que les données permettant l'accès concernent uniquement les membres du personnel autorisés c'est-à-dire remplissant les conditions d'accès (formation, membre effectif de l'unité, autorisation, finalité, …).

Cela implique notamment les services directement ou indirectement liés à la mise en œuvre du traitement soient intégrés et communiquent à temps avec le responsable de la gestion des accès (responsables hiérarchiques, service de contrôle interne, etc. …).
A titre d'exemple, les données d'un membre du personnel à qui l'accès à l'armement doit être retiré en raison d'un changement d'unité ou d'une enquête (judiciaire / disciplinaire) en cours doivent pouvoir être immédiatement actualisées (interdiction temporaire d'accès, effacement des données, directives internes relatives à la communication au responsable de la gestion des accès, etc. …).

37. Toujours à titre d'exemple, l'accès à l'armement pourrait être conditionné à la conjonction de plusieurs conditions :

- être enregistré comme membre du personnel de l'unité dans l'application de gestion du personnel ;
- être en ordre en termes de formations obligatoires pour la possession d'armement ;
- accéder dans les heures de service ;
- etc. …

38. Des mesures techniques (p. ex. système d'alerte) et organisationnelles (p. ex. vérification a posteriori par le responsable hiérarchique compétent) devraient cependant permettre d'anticiper des situations exceptionnelles comme par exemple la non remise de l'armement après la fin du service ou la nécessité d'accéder à l'armement en dehors des heures de service (p. ex. si un membre du personnel doit reprendre du service en dehors des heures de services).

SOUS-TRAITANCE

39. Dans l'hypothèse où le responsable du traitement souhaite faire appel à un partenaire externe pour la mise en place du traitement, celui-ci doit s'assurer au préalable que le partenaire externe, sous-traitant au sens du RGPD[42], présente des garanties suffisantes quant à la mise en œuvre des mesures techniques, organisationnelles et de sécurité appropriées afin que les droits des membres du personnel

[41] Article 5.1, d) du RGPD.
[42] Article 4.8 du RGPD.

soient respectés[43]. Le cadre dans lequel le sous-traitant effectue le traitement doit être précisément défini avec le responsable du traitement. Sans volonté d'exhaustivité, les questions suivantes doivent être traitées :

- Quelles sont les (catégories de) données et les catégories de personnes concernées que le sous-traitant traite pour le responsable du traitement ?
- A quelles données le sous-traitant a-t-il accès ?
- Selon quelles modalités le sous-traitant a-t-il accès aux données ?
- Le sous-traitant a-t-il désigné un Délégué à la protection des données ?
- Quelles sont les obligations du sous-traitant ?

  Exemple : détection d'incidents de sécurité ; communication en cas d'incident de sécurité ; collaboration en cas d'exercice des droits par la personne concernée ; …
- Etc. …

LA FACILITATION DE L'EXERCICE DES DROITS DES PERSONNES CONCERNÉES[44]

40. Les informations relatives aux droits des personnes concernées (membres du personnel) doivent être formulées de manière qualitative et intelligible, par exemple dans un règlement, un ordre de service ou encore lors de la diffusion des directives internes applicables en matière d'armement[45], être compréhensibles et accessibles aux personnes concernées, membres du personnel bénéficiant d'un accès à l'armement selon les conditions applicables[46].
L'exercice des droits de la personne concernée est cependant sans préjudice des droits d'autrui[47].

41. L'Organe de contrôle est d'avis que la journalisation des accès à l'armement peut être utilisée à des fins disciplinaires. Il en va de même dans le cas où la commission d'une infraction pénale est soupçonnée ou constatée[48]. Il s'agit d'une finalité ultérieure, admissible à certaines conditions que l'Organe de contrôle a déjà évoquées dans d'autres avis[49].

[43] En particulier les articles 25, 28 et 29 du RGPD et articles 21 et 22 de la LPD.
[44] Articles 12 et suivants du RGPD.
[45] Circulaire GPI 62.
[46] Considérant 50 RGPD. Voir à cet égard les développements de l'Organe de contrôle dans son avis d'initiative BD200007 concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail du 17 août 2020, consultable sur www.organedecontrole.be ; Organe de contrôle de l'information policière, *Avis DD200013 relatif à une demande d'utilisation d'un système de badge par la zone de police de X*, 1er avril 2020, consultable sur www.organedecontrole.be.
[47] Article 15.4 du RGPD. A toutes fins utiles, voir la décision de la Chambre Contentieuse de l'Autorité de protection des données du 29 juillet 2020, *Plainte de x contre y (Droit d'accès auprès de l'ancien employeur)*, 41/2020, paragraphe 39 et CJUE, *arrêt Peter Nowak c. Data Protection Commissionner*, C-434/16, 20 décembre 2017.
[48] Voir notamment Cour de justice de l'Union européenne, Digi Távközlési és Szolgáltató Kft. c. Nemzeti Adatvédelmi és Információszabadság Hatóság, 20 octobre 2022, C-77/21, §§ 25 et suivants.
[49] A titre d'exemple, l'avis de l'Organe de contrôle de l'information policière BD200007 précité.

LE TRAITEMENT D'EMPREINTES DIGITALES AUX FINS DE LA GESTION DES ACCÈS À L'ARMEMENT

42. Pour rappel, le titre 2 de la LPD et l'article 44/1, §2 de la LFP ne sont pas d'application en l'espèce puisqu'il est question d'un traitement qui ne poursuit pas les finalités de l'article 27 de la LPD et qui tombe sous le champ d'application du RGPD complété par le titre 1 de la LPD.

43. L'article 9 RGPD entoure les données biométriques – considérées comme une catégorie particulière de données à caractère personnel – de garanties spécifiques. Le RGPD définit les données biométriques comme "*des données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques*"[50].

44. Le traitement des empreintes digitales aux fins que seuls les membres du personnel autorisés puissent être en contact avec l'armement et le manipuler (gestion des accès) constitue donc un traitement de données biométriques au sens de l'article 9 RGPD.
L'opération de conversion de ces empreintes en un code n'appelle pas de conclusion différente puisque ce code constitue la traduction numérique et la matérialisation des empreintes digitales du membre du personnel. Etant donné que le membre du personnel est identifiable par ce code et que le traitement a pour finalité de l'identifier de manière unique et certaine (authentification), il y a lieu de considérer que tant les empreintes digitales que le code qui les convertit constituent des données biométriques[51].

45. Les éléments qui suivent sont strictement limités à la question du traitement des empreintes digitales et/ou du code qui les convertit à des fins de gestion des accès à l'armement.

Le traitement d'autres sortes de données biométriques (par exemple la reconnaissance faciale, la reconnaissance par l'iris, …) est exclu du présent avis, de même que le traitement de données biométriques (en général) pour la gestion de l'accès à d'autres zones d'un bâtiment de police ou d'un bâtiment de police[52].

46. Le paragraphe 1er de l'article 9 RGPD pose une interdiction de principe de traitement des empreintes digitales.

[50] Article 4, 14) du RGPD.
[51] Rapport de l'Organe de contrôle de l'information policière (COC) concernant la visite effectuée auprès d'une zone de police de la province de Flandre occidentale par l'Organe de contrôle de l'information policière dans le cadre de ses compétences de contrôle et de surveillance, CON20008, 12 janvier 2021, version publique consultable sur www.organedecontrole.be.
[52] Voir l'avis DA230015 de l'Organe de contrôle précité.

Le paragraphe 2 du même article énumère de manière exhaustive une liste de conditions exceptionnelles dans lesquelles ces données peuvent toutefois être traitées. L'article 9 LPD fixe des conditions supplémentaires à respecter pour le traitement de telles données.

47. Comme développé plus haut, le traitement de données à caractère personnel aux fins de la gestion des accès à l'armement trouve une base de licéité dans la lecture conjointe de l'article 6.1, c) RGPD et des articles 44, 98, et 141 LPI, ainsi que dans l'Arrêté armement.
Le traitement de données particulières – en l'espèce les empreintes digitales – pour la même finalité doit **en outre** trouver une base parmi les conditions exceptionnelles reprises à l'article 9, §2 RGPD.
En vue de la gestion des accès à l'armement et partant des conditions énoncées à l'article 9, §2 RGPD, il y a lieu d'examiner trois hypothèses en l'espèce :

1) Le consentement (article 9, §2, a) RGPD) ;
2) L'exécution d'obligations ou l'exercice de droits en matière de droit du travail, de la sécurité sociale et de la protection sociale (article 9, §2, b) RGPD) ;
3) Le motif d'intérêt public important sur base du droit de l'Union ou du droit d'un Etat membre qui en outre doit être proportionné à l'objectif poursuivi (article 9, §2, g) RGPD).

LE CONSENTEMENT (ARTICLE 9, §2, A) RGPD)

48. Comme expliqué précédemment dans le présent avis, le **consentement** du membre du personnel de l'entité de police ne peut constituer une base de licéité au traitement en question en raison de l'absence du caractère 'libre' de ce consentement, étant donné que le membre du personnel se trouve dans une relation d'autorité avec le responsable du traitement.
En effet, le consentement ne constituera pas un fondement juridique valable pour le traitement dans le cas où il y a un déséquilibre entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique – ici l'entité de police – et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière[53].

49. Dans l'hypothèse où le consentement serait admissible - *quod non*, le traitement des empreintes digitales doit être strictement nécessaire. Le fait qu'une alternative au traitement des empreintes digitales soit *proposée* comme par exemple l'utilisation d'un badge ou d'un code pin personnel ne répond pas à cette condition.
D'ailleurs, le fait qu'une telle alternative au traitement des empreintes digitales puisse être proposée au membre du personnel démontre que le principe de minimisation (proportionnalité) des données n'est

[53] Considérant 43 du RGPD. A toutes fins utiles, voir *European Data Protection Board*, les Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, 4 mai 2020.

pas rencontré[54] : en émettant cette proposition à la personne concernée, le responsable du traitement identifie lui-même que le traitement d'autres données – qui ne sont pas des données particulières au sens de l'article 9 RGPD – permet d'atteindre la même finalité.

L'EXÉCUTION D'OBLIGATIONS OU L'EXERCICE DE DROITS EN MATIÈRE DE DROIT DU TRAVAIL, DE LA SÉCURITÉ SOCIALE ET DE LA PROTECTION SOCIALE (ARTICLE 9, §2, B) RGPD)

50. L'article 9, §2, b) RGPD renvoie à **l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée** en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée. Une telle disposition de droit interne ou base juridique n'existe pas en Belgique au moment de la rédaction du présent.

51. L'élaboration d'une convention collective de travail ou un équivalent ne serait de toute façon pas suffisante en l'espèce puisqu'il faudrait lui trouver une base légale dans une loi (formelle).
Dans ce cas, il y aurait lieu de prévoir des garanties appropriées pour les droits et intérêts fondamentaux des personnes concernées (membres du personnel), mais cela n'entre en jeu que s'il s'avère que les empreintes digitales peuvent être traitées dans ce contexte, *quod non* puisqu'un tel document ne peut combler l'absence de base légale (formelle) au traitement.

LE MOTIF D'INTÉRÊT PUBLIC IMPORTANT (ARTICLE 9, §2, G) RGPD)

52. L'article 9, §2, g) RGPD renvoie quant à lui au **motif d'intérêt public important** sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.
Une telle disposition de droit interne ou base juridique n'existe pas en Belgique au moment de la rédaction du présent avis d'initiative.
L'Organe de contrôle a d'ailleurs encore récemment rappelé dans son avis DA230015 "*qu'il n'existe pas dans l'ordre juridique belge de base légale nationale générale encadrant le traitement de données à caractère personnel biométriques. La base légale potentielle devra établir clairement quelles finalités sont considérées comme un 'intérêt public important'*"[55].

[54] Voir infra.
[55] Organe de contrôle de l'information policière, Avis DA230015 précité, §12.

53. La recommandation de l'Autorité de protection des données (APD) relative au traitement de données biométriques le confirme en les termes suivants : "*le législateur belge n'a pas opté pour une base légale générale autorisant le traitement de données biométriques dans le cadre de l'identification ou de l'authentification unique d'une personne à des fins de sécurité. L'absence d'une telle base légale implique qu'actuellement et à l'exception du traitement des données biométriques dans le cadre de l'eID (carte d'identité électronique) et du passeport, le traitement de données biométriques ne peut pas s'appuyer, de manière valable en droit, sur des motifs d'intérêt public important.*"[56] et conclut que "*cela signifie concrètement que vu l'article 9.2.g) du RGPD, le législateur belge doit régir les modalités du traitement de données biométriques explicitement par une loi dans la mesure où il veut (continuer à) autoriser une telle utilisation de données biométriques*"[57].

54. L'Organe de contrôle doit donc constater, à la lumière des règles et principes établis par le RGPD, que le traitement des empreintes digitales de membres du personnel de la police intégrée aux fins de la gestion des accès à l'armement qui permette que seul les membres du personnel de la police intégrée autorisés puissent y accéder et le manipuler est pour le moins très problématique, par absence de base légale qui permettrait explicitement le traitement de telles données particulières pour une finalité déterminée et qui fournirait les garanties appropriées pour les droits fondamentaux et les intérêts des personnes concernées (membres du personnel de la police intégrée).

RÉFLEXIONS

55. Au-delà des considérations purement juridiques reprises ci-dessus, l'Organe de contrôle remarque qu'il existe au niveau de la police intégrée[58] une certaine propension au traitement d'empreintes digitales des membres du personnel dans le cadre d'une politique de gestion des accès à l'armement, et une préoccupation sérieuse quant à la sécurité des infrastructures policières au niveau politique, qui a notamment résulté en une circulaire et un projet d'arrêté royal récemment soumis pour avis au COC[59].

[56] Comme indiqué précédemment, l'Organe de contrôle est d'avis que l'utilisation des termes « *à des fins de sécurité* » est trop vague pour définir une finalité, certainement dans le cadre du traitement de données particulières telles que des empreintes digitales.
[57] Autorité de protection des données, *Recommandation relative au traitement de données biométriques*, version du 1er décembre 2021, p. 26. Voir à titre d'exemple l'Avis de l'Autorité de protection des données du 9 mars 2022 *relatif à un avant-projet de loi modifiant le Code belge de la Navigation concernant la sûreté maritime*, 51/2022, consultable sur www.autoriteprotectiondonnees.be.
[58] Notamment de par les différentes demandes d'information reçues.
[59] Voir entre autres : Demande d'avis relative à un arrêté royal relatif à la sécurisation des bâtiments et complexes de bâtiments policiers soumise le 3 avril 2023 à l'Organe de contrôle (référence DA230015) ; Circulaire ministérielle GPI 91 du 30 avril 2019 relative aux normes minimales de sécurisation des accueils ; Question parlementaire n° 308 du 4 février 2021 (Fr.) à la Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, référencée DO 2020202107872 à propos des mesures de protection des infrastructures policières ; Question parlementaire n° 632 du 25 mai 2021 (Fr.) à la Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, référencée DO 2020202110214 relative aux mesures de protection physique supplémentaires aux abords des commissariats.

56. Par anticipation d'une éventuelle initiative législative, le COC souhaite partager ci-après quelques considérations générales quant aux exigences minimales de la base légale qui encadrerait explicitement le traitement d'empreintes digitales de membres de la police intégrée aux fins de la gestion de l'accès à l'armement.

57. L'Organe de contrôle est d'avis qu'une modification de la LPI serait plus adéquate. L'Organe de contrôle rappelle que toute initiative législative doit lui être soumise pour avis.
Avant toute chose, si le législateur souhaitait adopter une position plus générale vis-à-vis du traitement d'empreintes digitales à des fins de gestion d'accès (pas uniquement concernant l'armement policier et par exemple, pour l'accès à des infrastructures policières, nucléaires, militaires, …), il est évident qu'une loi à part entière ou au moins un chapitre dans la LPI serait préférable[60].

58. La jurisprudence[61] a rappelé à maintes reprises que pour ne pas enfreindre l'article 8 de la Convention européenne des droits de l'Homme (CEDH), une ingérence doit être « *prévue par la loi* », poursuivre un but légitime au regard du paragraphe 2 et, de surcroît, être nécessaire dans une société démocratique pour atteindre ce but. Les éléments essentiels du traitement doivent être fixés dans la loi elle-même (voir art. 22 de la Constitution) et ce dans des termes clairs et suffisamment précis.

59. Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute éventualité – dépend naturellement du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires[62] : l'adoption de directives pratiques à diffusion restreinte est envisageable. Ainsi par exemple, la Cour européenne des droits de l'homme a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines[63].

60. Comme il l'a déjà formulé par rapport à la sécurisation des bâtiments et complexes de bâtiments policiers[64], l'Organe de contrôle insiste sur le fait qu'un traitement tel que celui dont question ne peut être réglé par arrêté royal et que la simple adaptation de l'Arrêté Armement et/ou d'une circulaire comme la GPI 62 serait en l'occurrence insuffisante.
Dans l'hypothèse d'une initiative législative, le caractère obligatoire ou non du recours à un tel traitement pour la finalité de gestion des accès à l'armement devrait être identifié.

[60] A cet égard, il est renvoyé aux considérations émises dans l'avis DA230015 du COC précité.
[61] Notamment : Cour européenne des droits de l'Homme, Nuh Uzun et autres c. Turquie, requête n° 49341/18, 29 mars 2022 ; Cour européenne des droits de l'Homme, Rotaru c. Roumanie, Requête n° 28341/95, 4 mai 2000 ; Cour constitutionnelle, arrêt n° 33/2022 du 10 mars 2022.
[62] Cour européenne des droits de l'Homme, Grande Chambre, 4 décembre 2008, S. et Marper c. Royaume-Uni.
[63] Cour européenne des droits de l'Homme, 26 mars 1987, Leander c. Suède ; Cour européenne des droits de l'Homme, 4 juillet 2006, Lupsa c. Roumanie ; Cour constitutionnelle, arrêt n° 33/2022 du 10 mars 2022.
[64] Organe de contrôle de l'information policière, Avis DA230015 précité.

61. Eu égard au caractère particulièrement sensible des empreintes digitales, les ministres compétents devraient évaluer la plus-value de l'implémentation d'un tel traitement de manière intégrée, c'est-à-dire via l'application de mesures techniques, organisationnelles et de sécurité uniformes au sein des entités de police mettant en œuvre ce traitement. A titre d'exemple et sans volonté d'exhaustivité :

- catégories de données biométriques traitées (empreintes digitales, …) ;
- type de données traitées (empreintes digitales brutes ou leur traduction en un code (le gabarit)) ;
- taux du seuil pour la validation de l'identification[65] ;
- type de comparaison (identification simple ou authentification)[66] ;
- détection, signalement et suivi des incidents de sécurité ;
- contenu minimal des directives internes ;
- données devant être enregistrées dans la journalisation ;
- durée de conservation minimale de la journalisation ;
- …

62. Dans cette optique, l'implication des services ayant un rôle général ou d'appui en matière de logistique[67] par rapport au responsable du traitement devrait être examinée.
Les avis circonstanciés du Comité de coordination de la police intégrée[68] et du Comité d'avis en charge de la stratégie en matière d'information[69] présenteraient sans conteste une valeur ajoutée en la matière.

63. Quoi qu'il en soit, l'Organe de contrôle insiste sur le fait que l'existence d'une base légale au sens de l'article 9, §2, b) ou g) RGPD ne suffirait pas pour que le traitement dont question, pour la finalité visée, soit conforme au RGPD. En effet, en sus de la base légale, des garanties appropriées adaptées et supplémentaires au sens de l'article 9 de la LPD ainsi que le respect des principes généraux et des autres règles du RGPD doivent être assurés.

64. A cet égard, le COC souhaite aborder en particulier le principe de la proportionnalité: il incombe au responsable du traitement de vérifier et d'être en mesure de démontrer au préalable et pendant toute la durée du traitement sa conformité à toutes les règles et conditions applicables, en ce compris le fait

[65] Pour plus d'informations, voir Autorité de protection des données, *Recommandation relative au traitement de données biométriques* précitée.
[66] *Ibidem*.
[67] Sans volonté d'exhaustivité : le Commissariat général (article 100*bis*, §1er LPI), la Direction générale de la gestion des ressources et de l'information (article 93, §1er, 2° LPI et article 6 de l'Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale), les Directions de coordination et d'appui (article 104 LPI et article 4 de l'Arrêté royal du 14 novembre 2006 relatif à l'organisation et aux compétences de la police fédérale).
[68] Eu égard à sa mission d'avis inscrite à l'article 8*ter*, §2 LPI.
[69] Eu égard à sa mission d'avis inscrite à l'article 8*sexies*, §2 LPI.

que les données traitées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité pour laquelle elles sont traitées (principe de minimisation)[70].

65. La Circulaire GPI 62[71] prévoit que les locaux d'armement ne soient accessibles que moyennant l'application d'une procédure spécifique qui doit être définie par le responsable local, de sorte qu'un nombre limité de personnes spécialement désignées par lui peuvent y avoir accès. Accès, par exemple, via un badge ou un code d'accès.
Une procédure adéquate doit être mise au point pour la prise et la remise des armes, le cas échéant via un registre d'utilisateur mentionnant le nom de l'utilisateur de l'arme, la date d'entrée et de sortie. Cette procédure doit être adaptée en fonction des circonstances locales (nombre d'armes, effectif en personnel, configuration des lieux, ...). Dans tous les cas, elle doit être conçue de sorte que l'accès à l'endroit de stockage soit limité au seul personnel autorisé, que les accès soient contrôlés, qu'un contrôle du nombre d'armes entreposées puisse facilement être opéré, qu'un usage abusif par du personnel non autorisé soit impossible et que les clés ne restent pas sur la porte de la chambre forte le cas échéant.

66. Considérant que l'utilisation d'un badge ou d'un code d'accès évoquée dans la circulaire GPI 62 est une suggestion, l'évaluation de la proportionnalité doit naturellement prendre en compte les évolutions technologiques ainsi que la possibilité de combiner plusieurs méthodes pour la gestion des accès, toujours en ayant égard à l'évaluation des risques actualisée et l'analyse fonctionnelle réalisée[72].

67. L'expérience du responsable du traitement voire même d'autres entités de la GPI (p. ex. la survenance d'un incident) est également un point d'attention[73]. Un traitement de données à caractère personnel fondé principalement (voire exclusivement) sur des arguments plutôt 'émotionnels' et/ou sur une anticipation non documentée du risque jugé le plus grave est toutefois insuffisant.

A cet égard par exemple, l'Organe de contrôle ne voit pas dans quelle mesure le traitement des empreintes digitales des membres du personnel à l'entrée du local d'armement comme moyen unique de gestion des accès serait proportionné, certainement si l'armement en tant que tel n'est pas rangé dans des casiers individuels dont l'accès est bloqué ou en tous cas si, une fois l'accès au local ouvert,

[70] Concernant l'exigence de proportionnalité et à titre informatif, l'APD prend dans sa recommandation de 2021 précitée comme exemple un jugement du tribunal d'Amsterdam qui a considéré que l'utilisation d'un scan d'empreintes digitales permettant d'accéder au système de caisse dans un magasin, afin de garantir la sécurité et l'intégrité de données particulières et d'empêcher toute fraude était disproportionnée. Comme le souligne l'APD, le magasin n'a pas suffisamment démontré qu'il n'existait pas d'alternative moins radicale pour réaliser les mêmes finalités. L'accès à la caisse d'un magasin ne représente évidemment pas les mêmes risques que l'accès de membres de la police intégrée à l'armement pour l'exercice de leurs missions.
[71] Circulaire GPI 62, Chapitre VI, Section 2.
[72] Sur ce point, le traitement de données biométriques à des fins d'authentification (comprendre la validation de l'identification) est reconnu comme étant un moyen d'authentification fort au même titre que l'authentification à plusieurs facteurs (*Multi-Factor Authentification - MFA*) (Commission vie privée, *Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes*, n° 17/2008, 9 avril 2008, p. 10, consultable sur https://www.autoriteprotectiondonnees.be/publications/avis-n-17-2008.pdf, consulté le 6 novembre 2023).
[73] A titre d'information, concernant l'usage de caméras de surveillance à des fins de contrôle du respect des conditions de travail, la jurisprudence a déjà indiqué qu'il n'est pas non plus exigé que le responsable du traitement ait d'abord subi un préjudice avant de pouvoir introduire la surveillance par caméra (Cour de Justice, 11 décembre 2019, TK, C-708/18, considérant 44).

le membre du personnel a la possibilité de prendre possession d'une ou plusieurs arme(s) qui ne lui est/sont pas destinées.

68. En tous les cas, c'est le caractère inévitable du traitement des empreintes digitales plutôt que d'autres mesures et le traitement (éventuellement combiné) d'autres données tels que l'intervention d'un armurier, l'utilisation d'un badge, d'un code pin, de casiers individuels sécurisés, de caméras de surveillances, de moyens *MFA*, etc. … pour atteindre la finalité visée que le responsable du traitement doit démontrer, cela en tenant compte des intérêts, des droits et des libertés des personnes concernées et des finalités visées ainsi que des éventuels risques identifiés.

69. De même, les analyses de risques et l'analyse fonctionnelle liées à l'armement devraient mettre en évidence qu'une distinction doit être faite entre l'accès au local d'armement et à chaque arme : est-il envisagé que du personnel logistique puisse pénétrer dans le local pour des missions particulières (par exemple le ménage, le remplacement d'une ampoule, …) sans pouvoir accéder à l'armement parce que ce personnel n'y est pas autorisé ? Il est évident que l'accès à l'armement moyennant le traitement des empreintes digitales ne pourra pas être justifié à tous égards.

CONCLUSION

70. Le traitement de données à caractère personnel de membres du personnel d'une entité de police aux fins de gérer les accès à l'armement tombe sous le champ d'application du RGPD.
Ce traitement trouve une base légale dans la conjonction d'obligations légales en matière de fonctionnement et d'organisation internes, d'armement, et de gestion des risques[74].

71. Les empreintes digitales – de même que le code (gabarit) qui les convertit – constituent des données dites particulières en ce sens qu'elles bénéficient de garanties et de protections particulières.
Le traitement d'empreintes digitales de membres du personnel de la police intégrée aux fins de la gestion des accès à l'armement doit donc trouver une base parmi les conditions exceptionnelles reprises à l'article 9, §2 RGPD.

72. Bien que l'Organe de contrôle puisse comprendre l'intérêt de la police intégrée pour le traitement d'empreintes digitales dans le cadre d'une politique interne de gestion des accès aux fins que seuls les membres du personnel autorisés puissent être en contact avec l'armement et le manipuler, le COC doit constater, à la lumière des règles et principes établis par le RGPD et en l'état actuel de la législation belge, qu'un tel traitement est **très problématique**, par absence de base légale qui permettrait explicitement le traitement de telles données particulières pour cette finalité, et qui fournirait les garanties appropriées pour les droits fondamentaux et les intérêts des personnes concernées[75].

73. L'Organe de contrôle rappelle que le consentement de la personne concernée[76] ne peut constituer une base au traitement étant donné que le consentement ne pourrait être considéré comme libre et éclairé. Le fait que le responsable du traitement propose à la personne concernée de choisir entre le traitement via empreintes digitales ou un code par exemple est sans incidence sur l'absence du caractère libre du consentement. En outre, l'offre d'une telle alternative est la preuve en soi de l'absence du caractère inévitable du traitement de cette catégorie de données.

74. En outre, il y a lieu de rappeler que la base légale du traitement n'induit pas systématiquement ou *ipso facto* sa proportionnalité : il y a lieu de démontrer le caractère inévitable du traitement et de ses modalités, en l'occurrence de la catégorie et des données choisies.

75. Le COC rappelle que dans son évaluation, le responsable du traitement doit également tenir compte de la conjonction des obligations légales qui lui incombent et du résultat de la gestion dynamique des risques qu'il aura mise en place. Il s'agit, sans volonté d'exhaustivité, notamment : analyse d'impact et

[74] En particulier : Article 6.1, c) du RGPD, articles 44, 98 et 141 de la LPI, l'Arrêté royal Armement et la Circulaire GPI 62.
[75] Voir notamment : Cour européenne des droits de l'Homme, Rotaru c. Roumanie, Requête n° 28341/95, 4 mai 2000, §52.
[76] Au sens de l'article 9, §2, a) du RGPD.

de risques en matière de protection des données ; politique et plan de sécurité de l'information ; approche planifiée, structurée et évolutive du bien-être au travail matérialisée par une politique dont l'application est répartie aux différents niveaux de compétence et de responsabilité de l'entité de police ; mesures résultants du management des risques (contrôle ; sensibilisation ; …) ; formation[77] et conditions d'accès préalable ; information et prévention vis-à-vis des membres de l'organisation ; plan de sécurité techno préventif ; etc. …

Une approche globale est donc à privilégier[78] pour la détermination des mesures et de la proportionnalité des données traitées.

La démonstration du caractère inévitable du traitement des empreintes digitales au regard de la finalité visée inclut la comparaison avec le traitement d'autres données prises individuellement mais également, à lumière du principe de subsidiarité, de l'avis de l'Organe de contrôle, avec une combinaison de traitements de données moins invasifs.

76. Dans l'hypothèse d'une initiative législative ayant pour but de permettre le traitement de données biométriques pour la gestion des accès à l'armement, le législateur devrait évaluer la plus-value de l'implémentation d'un tel traitement de manière intégrée, c'est-à-dire via l'application de mesures techniques, organisationnelles et de sécurité uniformes au sein des entités de police.

[77] A titre d'information, voir les conditions reprises dans l'Arrêté Armement et la circulaire GPI 62, ainsi que les obligations découlant de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail, à charge des travailleurs de respecter la formation et les instructions dispensées par l'employeur (article 6).

[78] Une telle approche est d'ailleurs explicitement encouragée dans la Circulaire GPI 62 (Chapitre 6, Section 6). L'AIG l'encourage également dans son récent rapport (Inspection générale de la police fédérale et de la police locale, *op. cit.*, notamment pp. 9, 10, 14 et 15).

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière,

émet d'initiative le présent avis

Conformément aux articles 237 et 240, 1° et 2° de la LPD, porte le présent avis d'initiative à la connaissance :

- du Ministre de l'Intérieur et du Ministre de la Justice
- du Commissaire général de la Police fédérale
- de la Commission Permanente de la Police Locale
- du Comité Information et ICT (art. 8*sexies* LPI)

Avis d'initiative adopté par l'Organe de contrôle de l'information policière le 13.02.2024

Pour l'Organe de contrôle,

Frank SCHUERMANS
Président *a.i.* (SIGNÉ)