Autorité de protection des données

Recommandation relative au traitement de données biométriques

EXECUTIVE SUMMARY

Les données biométriques sont des données à caractère personnel déduites des caractéristiques physiques, physiologiques ou comportementales d'une personne physique et permettant d'identifier ou d'authentifier cette personne. Les citoyens sont de plus en plus souvent confrontés au traitement de données biométriques sur leurs smartphones ou leurs tablettes mais aussi par les autorités publiques et par des entreprises privées. Conformément à l'article 9.1 du 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* (ci-après le "RGPD"), les données biométriques constituent une catégorie particulière de données à caractère personnel, et ce contrairement à la situation antérieure à l'entrée en vigueur du RGPD. Ce sont des données à caractère personnel qui, par leur nature, sont particulièrement sensibles car leur traitement peut comporter des risques significatifs pour les libertés et droits fondamentaux des personnes. En vertu de l'article 9.1 du RGPD, le traitement de données biométriques est donc interdit, à moins que le responsable du traitement puisse légitimement invoquer l'un des motifs d'exception énumérés de manière limitative à l'article 9.2 du RGPD.

Ce sont notamment ce changement de qualification juridique de la notion de données biométriques et l'augmentation considérable de processus de traitement biométriques dans le quotidien qui ont incité l'Autorité de protection des données (ci-après "l'Autorité") à s'exprimer sur ce sujet.

La recommandation vise principalement à accompagner les responsables du traitement et les sous-traitants afin de leur permettre d'interpréter et d'appliquer correctement les règles du RGPD en matière de traitement de données biométriques. Il convient toutefois de faire remarquer dans ce contexte que la recommandation ne s'applique pas au traitement de données biométriques réalisé par des autorités compétentes au sens de la 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 à tout autre traitement de données qui n'est pas couvert par le RGPD. En outre, la présente recommandation entend inviter le législateur à prévoir une base légale pour le traitement de données biométriques.

Dans un premier temps, l'Autorité explique en détail au Chapitre II le cadre juridique du traitement visé. Une attention particulière est notamment accordée aux notions de 'données à caractère personnel', 'traitement de données à caractère personnel', 'responsable du traitement' et 'sous-traitant'.

La recommandation fournit ensuite des explications sur la portée concrète de la notion de 'traitement de données biométriques'. Une bonne compréhension de la terminologie utilisée est en effet fondamentale avant de pouvoir appliquer les principes de protection des données au traitement de données biométriques.

Le Chapitre III traite ensuite des principes pertinents de protection des données dans le cadre du traitement de données biométriques. Dans ce cadre, une attention particulière est consacrée au choix d'une base juridique correcte (motif d'exception), à la définition correcte des finalités du traitement, à l'exigence de proportionnalité, à la sécurité du traitement, au principe de limitation de la conservation, à l'obligation de transparence et à l'obligation (éventuelle) de réaliser une analyse d'impact relative à la protection des données.

Cette analyse, en particulier en ce qui concerne le recours à une base juridique ou à un motif d'exception qui justifie le traitement de données biométriques, nous apprend qu'actuellement, il existe une lacune en droit belge de sorte que tout traitement de données biométriques dans le cadre de l'authentification de personnes, dans la mesure où l'on ne peut pas recourir au consentement explicite et à l'exception du traitement de données biométriques dans le cadre de l'eID (carte d'identité électronique) et du passeport, a lieu sans base juridique. Cela signifie concrètement que le législateur belge devra définir dans la loi les modalités du traitement de données biométriques dans la mesure où il veut (continuer à) autoriser l'utilisation de données biométriques dans un contexte déterminé. Toutefois, l'Autorité admet que cette exigence déroge dans une large mesure au régime antérieur à l'entrée en vigueur du RGPD. Dès lors, compte tenu des principes de bonne gouvernance, dès la publication de la présente recommandation, il est prévu une période transitoire d'un an pendant laquelle le traitement de données biométriques sera toléré conformément à l'ancienne norme et l'Autorité n'interviendra pas de manière proactive. Cette période d'un an doit permettre aux responsables du traitement et au législateur de prendre les mesures nécessaires afin de mettre les traitements visés en conformité avec les dispositions du RGPD, comme expliqué dans la présente recommandation.

I. Introduction

1. Avant-propos

Le RGPD est entré en vigueur le 25 mai 2018. Il abroge la Directive du Parlement européen et du Conseil du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (ci-après "la Directive 95/46/CE") et confirme et consolide la jurisprudence telle qu'appliquée par la Cour de justice de l'Union européenne et par le Groupe de travail Article 29[1] (ci-après le "Groupe 29") au moyen de points de vue officiels et de lignes directrices. En passant d'une directive à un règlement, le législateur européen a voulu rendre applicable, directement et de manière uniforme dans les États membres, la protection des données à caractère personnel qui est définie en tant que droit fondamental à l'article 8 de la Charte des droits fondamentaux de l'Union européenne[2].

L'un des principaux objectifs du RGPD consiste à renforcer les droits des personnes concernées. Le RGPD confère en effet aux autorités de contrôle des pouvoirs importants de manière à ce qu'elles puissent également infliger des sanctions en cas de non-respect des règles qui y sont définies. L'Eurobaromètre de mai 2019 sur le RGPD révèle que les connaissances des personnes concernées relatives aux règles de protection des données applicables et à leurs droits augmentent nettement[3]. Ainsi, elles exercent leurs droits plus qu'auparavant. C'est notamment le cas pour le retrait de leur consentement ou l'opposition au traitement de leurs données à des fins commerciales[4].

C'est à la lumière de ces droits renforcés que de nombreuses associations de défense des droits des consommateurs et des citoyens s'accordent à dire que le RGPD contribue considérablement à une société numérique juste, basée sur la confiance mutuelle entre les personnes concernées et les acteurs qui interviennent dans le traitement de leurs données.

Afin de réaliser cet objectif, le RGPD met l'accent sur la responsabilisation des différents acteurs qui traitent des données à caractère personnel, qu'il s'agisse de particuliers, de professionnels, de personnes morales ou d'autorités publiques, et ce lors de chaque phase du traitement, tant au niveau national qu'européen ou international.

---

[1] Le Groupe 29 a été remplacé par le Comité européen de la protection des données (souvent désigné par l'abréviation anglaise "EDPB") qui reprend les différents points de vue adoptés par le Groupe 29. Dès lors, dans la présente recommandation, il sera fait référence aux points de vue de l'EDPB.

[2] Avec, à quelques exceptions près, une certaine marge de manœuvre pour les législateurs nationaux, que nous n'approfondirons pas dans la présente recommandation.

[3] https://europa.eu/eurobarometer/screen/home et voir également : https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_2956.

[4] Voir le rapport du "*Multistakeholder Group on the General Data Protection Regulation*" qui a été créé dans le sillon de la Commission européenne et dans lequel sont impliqués la société civile et des représentants des secteurs professionnels, des universitaires et des gens de terrain, disponible via le lien suivant : https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3537&lang=fr.

Dès lors, le rôle des autorités de contrôle ne se limite pas simplement à une action répressive. Vu les sanctions conséquentes auxquelles s'exposent les contrevenants et le fait que les données à caractère personnel sont devenues indispensables pour l'exercice de la plupart des activités socio-économiques, la prévention et la sensibilisation occupent une place importante dans la stratégie de protection des données.

2. Contexte et champ d'application de la recommandation

Conformément à l'article 9.1 du RGPD, les données biométriques constituent une catégorie particulière de données à caractère personnel, et ce contrairement à la situation antérieure à l'entrée en vigueur du RGPD. Ce sont des données à caractère personnel qui, par leur nature, sont particulièrement sensibles car leur traitement peut comporter des risques significatifs pour les libertés et droits fondamentaux des personnes. Les caractéristiques corporelles biométriques peuvent être uniques ou presque et peuvent dès lors presque toujours être reliées à un seul individu. En outre, elles contiennent souvent plus d'informations que ce qui est strictement nécessaire au regard des finalités poursuivies, peuvent contenir des données sensibles sur l'état de santé et sont permanentes ou évoluent lentement, ce qui implique qu'une fuite de données a de graves conséquences à long terme. En vertu de l'article 9.1 du RGPD, le traitement de données biométriques est donc interdit, à moins que le responsable du traitement puisse légitimement invoquer l'un des motifs d'exception énumérés de manière limitative à l'article 9.2 du RGPD. Ce changement de qualification implique toutefois que les lignes directrices de la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, en matière de traitement de données biométriques dans le cadre de l'authentification de personnes, conformément à l'avis n° 17/2008, ne sont plus pertinentes.

En outre, grâce au caractère de plus en plus fiable et bon marché des méthodes d'authentification biométrique, l'Autorité a constaté que des individus, tant dans leurs relations avec les autorités publiques qu'avec des entreprises privées, sont de plus en plus souvent confrontés au traitement de leurs données biométriques.

Ce sont notamment ce changement de qualification juridique de la notion de données biométriques et l'augmentation considérable de processus de traitement biométriques dans le quotidien qui ont incité l'Autorité à s'exprimer à nouveau sur ce sujet.

La recommandation vise principalement à accompagner les responsables du traitement et les sous-traitants afin de leur permettre d'interpréter et d'appliquer correctement les règles du RGPD en matière de traitement de données biométriques. Une méthode conforme au RGPD constitue en effet un allié indispensable et utile dans leurs relations avec les personnes concernées. C'est en communiquant de manière transparente avec la personne concernée sur la manière dont certaines données à caractère

personnel sont traitées et en démontrant que des mesures appropriées ont été prises pour veiller à ce que le traitement soit conforme à la réglementation qu'une relation de confiance pourra être établie, relation nécessaire pour réaliser et défendre les objectifs poursuivis. La présente recommandation ne remplace donc pas les obligations générales qui découlent du RGPD et de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, mais entend uniquement les compléter ou les spécifier. Les entreprises et instances qui effectuent un traitement visé dans la présente recommandation devront toujours respecter tous les actes légaux et réglementaires concernant le traitement de données à caractère personnel. Dans ce cadre, l'Autorité veut toutefois souligner que la portée de la présente recommandation se limite au traitement de données biométriques dans le champ d'application du RGPD. Les lignes directrices reprises dans la présente recommandation ne s'appliquent donc pas au traitement de données biométriques réalisé par des autorités compétentes[5] au sens de la Directive Police-Justice[6] ou à tout autre traitement de données qui n'est pas couvert par le RGPD.

Enfin, il conviendra d'adapter/de compléter la présente recommandation en temps opportun, en tenant compte des nouvelles évolutions en matière de traitement de données biométriques.

3. Cadre juridique

La réglementation relative au traitement de données biométriques figure dans le RGPD. L'analyse des règles du RGPD se base, le cas échéant, sur les points de vue du Comité européen de la protection des données (ci-après l' "EDPB") et de son prédécesseur, le Groupe 29. Certaines des lignes directrices de ce dernier ont déjà été revues et actualisées par l'EDPB, alors que d'autres ont été adoptées en l'état. L'EDPB doit également se prononcer sur des questions ou des thèmes qui n'ont pas encore fait l'objet de prises de position antérieures. Cela vaut notamment pour les lignes directrices attendues concernant le traitement de données biométriques. Les points de vue adoptés par l'Autorité dans la présente recommandation ne portent toutefois pas préjudice à la future position de l'EDPB dans ce cadre. L'Autorité fait en effet partie de l'EDPB et est tenue par les points de vue de ce dernier. Une modification de la présente recommandation afin de la mettre en conformité avec la vision européenne n'est dès lors pas exclue. Dès lors, l'Autorité recommande de consulter régulièrement son site Internet qui reprendra toujours la dernière version de la présente recommandation.

[5] L'article 3.7 de cette directive dispose qu' *aux fins de la présente directive, on entend par "autorité compétente" :*
" *"a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou*
b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;""
[6] La Directive telle que visée en note de bas de page 1.

II. Traitement de données biométriques : de quoi s'agit-il ?

1. Cadre juridique

1.1 Données à caractère personnel[7]

L'article 4.1) du RGPD définit les 'données à caractère personnel' comme suit : "*toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*."

Les termes 'identifiée' et 'identifiable' sont fondamentaux pour comprendre ce qu'est une donnée à caractère personnel. Alors que les données permettant d'identifier directement une personne sont souvent évidentes (par exemple une combinaison du nom de famille, du prénom et de l'adresse ou de la date de naissance ou d'un numéro d'identification unique, comme un numéro de client), il est parfois plus difficile de savoir ce qu'il y a lieu d'entendre par 'données permettant d'identifier une personne indirectement' (par exemple des données pseudonymisées).

Conformément à l'article 4.5) du RGPD, les données pseudonymisées sont des données à caractère personnel traitées de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. En d'autres termes, chaque élément d'information qui a été attribué à une personne, aussi insignifiant semble-t-il quand vous le considérez de manière isolée (par exemple un âge, un domicile, la couleur des yeux ou le sexe, voire un numéro d'enregistrement), constitue une donnée à caractère personnel dès que, combiné à une ou plusieurs autres données, il permet d'identifier une personne physique. Tant que de telles informations supplémentaires sont disponibles, et quelle que soit la qualité des mesures techniques et organisationnelles mises en œuvre, les données pseudonymisées relèvent du champ d'application du RGPD.

[7] Pour de plus amples informations sur ce sujet, consulter l'avis 4/2007 (WP 136) *sur le concept de donnée à caractère personnel*, adopté le 20 juin 2007 par le Groupe 29 et disponible via le lien suivant : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf.

Les données 'anonymisées' par contre ne sont pas qualifiées de données à caractère personnel car l'identification d'une personne physique à l'aide de telles données n'est plus possible, même pas avec des informations supplémentaires. Bien que pour cette raison, le RGPD exclut de telles données de son champ d'application, la pratique nous apprend que la distinction entre données pseudonymisées et données anonymisées est de plus en plus difficile à établir. Dans ce contexte, on peut signaler que l'EDPB est actuellement occupé à rédiger les lignes directrices concernant l'anonymisation des données.

Retenez enfin que - en principe - seules les données de personnes physiques en vie sont des données à caractère personnel.

1.2 Traitement de données à caractère personnel

L'article 4.2) du RGPD définit le 'traitement' comme suit : "*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel*".

Tout comme pour les finalités de son traitement, chaque responsable du traitement doit également être transparent à l'égard des traitements qu'il effectue avec les données d'une personne concernée. Le degré de détail dépend notamment du type de personnes concernées (enfants, professionnels, experts, etc.), de la manière dont leurs données à caractère personnel sont traitées et de la mesure dans laquelle de tels traitements impliquent une ingérence dans leur droit au respect de la vie privée. Définir les traitements qui sont réalisés pour chaque finalité distincte constitue également un élément fondamental lors de l'évaluation de la proportionnalité (entendez : l'admissibilité) du traitement en question. En ce sens, il est improbable que l'installation d'un capteur d'empreintes digitales pour accéder à une cafétéria réussisse le test de proportionnalité.

Afin d'avoir un aperçu des activités de traitement, il est également obligatoire, en vertu de l'article 30 du RGPD, de tenir un registre des activités de traitement lorsqu'une entreprise ou une organisation occupe plus de 250 personnes ou lorsque le traitement qu'elle effectue est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou **s'il porte notamment sur des catégories particulières de données**. Dès lors, s'agissant d'un traitement de données biométriques, il sera toujours obligatoire de tenir un tel registre.

Outre une liste des activités de traitement réalisées, ce registre contient également d'autres informations comme les données à caractère personnel ou les catégories de données à caractère personnel qui sont traitées. Ce registre doit être établi par écrit ou par voie électronique et doit être clair et compréhensible.

Le registre contribue donc également à l'inventaire précis des données traitées et constitue dès lors un outil indispensable pour comprendre l'écosystème des traitements de données pour lesquels un responsable du traitement déterminé est responsable. Un registre tenu correctement permet d'économiser du temps dans le cadre du respect de vos obligations en vertu du RGPD et permet aussi que toutes les personnes travaillant au sein de votre organisation et impliquées dans le traitement de données utiles pour votre organisation soient, au besoin, consultées et/ou informées concernant les traitements réalisés au sein de l'organisation, ce qui contribue également, à tous les niveaux, à une plus grande prise de conscience en matière de protection des données. Le registre vous aidera aussi dans la rédaction d'une analyse d'impact relative à la protection des données (voir ci-dessous la rubrique III.7) et dans la collaboration avec l'Autorité si celle-ci a des questions concernant une de vos activités de traitement.

1.3 Responsable du traitement[8]

Vous êtes 'responsable du traitement' lorsque vous déterminez, seul ou conjointement avec d'autres, les finalités et les moyens du traitement de données à caractère personnel.

Il importe de retenir qu'une organisation n'est pas "par nature" un responsable du traitement ou un sous-traitant. Tout dépend de la manière dont l'organisation se comporte dans les faits. Pour chaque opération que vous réalisez avec des données biométriques, vous devez vous demander qui a déterminé les finalités du traitement ainsi que le mode de traitement de ces données.

Afin de préciser votre rôle et celui des autres parties (comme les prestataires de services techniques ou les tiers qui vous fournissent des données), posez-vous les questions suivantes :

- Qui décide en premier lieu de procéder à la collecte de données (biométriques) ?
- Qui définit les personnes concernées ou les catégories de personnes concernées ?
- Qui détermine les catégories de données qui doivent être collectées ?
- Qui détermine la/les finalité(s) pour laquelle (lesquelles) les données sont utilisées ?
- Qui détermine la base juridique du traitement ?
- Qui détermine si les données doivent être transmises et si oui, à qui ?

[8] Pour un aperçu complet relatif à la fonction de responsable du traitement, voir : EDPB Guidelines 07/2020 *on the concepts of controller and processor in the GDPR* (actuellement, uniquement disponible en anglais). Consultable via le lien suivant : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

- Qui détermine le contenu des informations fournies aux personnes concernées au sujet du traitement ou des activités de traitement appliqué(es) à leurs données ?
- Qui détermine le délai de conservation des données ? et
- Qui détermine la manière de réagir quand des personnes concernées exercent leurs droits ?

Toutes ces décisions ne peuvent être prises que par le responsable du traitement dans le contexte de son contrôle général du traitement de données. Si vous prenez l'une de ces décisions, vous êtes plus que probablement responsable du traitement.

L'article 26 du RGPD prévoit également la situation dans laquelle deux responsables du traitement ou plus coexistent, ce qu'on appelle des 'responsables conjoints du traitement'. C'est le cas lorsque plusieurs entités déterminent conjointement les finalités et les moyens du traitement. L'article 26 du RGPD établit que dans ce cas, les responsables conjoints du traitement doivent définir de manière transparente leurs obligations respectives par voie d'un accord qui reflète correctement leurs rôles respectifs vis-à-vis des personnes concernées.

1.4 Sous-traitant[9]

Lorsqu'une autorité publique ou une instance privée ou une personne physique traite des données à caractère personnel pour votre compte, sur la base de vos instructions, dans le seul but de vous permettre de réaliser vos finalités, il s'agit d'une relation de sous-traitance.

Le recours à un sous-traitant implique que les exigences de l'article 28 du RGPD doivent être respectées.

Retenez tout d'abord que quelle que soit la situation et quel que soit le sous-traitant, dès que vous agissez en tant que responsable du traitement, vous êtes lié aux obligations que vous impose le RGPD et que, le cas échéant, vous devez répondre des violations de ces obligations. C'est pour cette raison que l'article 28.1 du RGPD dispose que vous ne pouvez faire appel qu'à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Cela découle également de l'article 24 du RGPD qui vous oblige à mettre en œuvre des mesures techniques et organisationnelles appropriées pour vous assurer et être en mesure de démontrer que votre traitement de données est effectué conformément au RGPD. Faire appel à un sous-traitant certifié ou à un sous-traitant qui a adhéré à un code de conduite approuvé constitue un élément pouvant démontrer l'existence de garanties suffisantes comme le requièrent les articles 28.1 et 28.4 du RGPD.

[9] Pour un aperçu complet relatif à la relation responsable du traitement - sous-traitant, voir : EDPB Guidelines 07/2020 *on the concepts of controller and processor in the GDPR*, voir la note de bas de page 8.

Alors que dans une situation idéale, le responsable du traitement donne des instructions complètes relatives au traitement qui a été confié au sous-traitant, dans la réalité, c'est souvent moins évident et il se peut que certains éléments ne soient pas déterminés par le responsable du traitement mais par son sous-traitant sur la base de son expertise concernant les technologies appliquées lors du traitement et/ou les mesures de sécurité des données les plus appropriées. Le fait qu'un sous-traitant dispose de plus d'expertise que vous quant aux moyens techniques à utiliser lors du traitement de données ne conduit pas, en soi, à une requalification de sa position de sous-traitant en celle de responsable du traitement. Certains sous-traitants proposent des solutions prêtes à l'emploi sans que cela porte préjudice à votre obligation, en tant que responsable du traitement, de prendre les décisions requises concernant les données traitées, les finalités poursuivies et/ou les moyens pour les réaliser.

En outre, il convient encore de faire remarquer qu'une même instance peut à la fois remplir le rôle de sous-traitant et de responsable du traitement mais pas pour le même traitement de données à caractère personnel. Un sous-traitant qui agit de la sorte doit veiller à ce que ses systèmes et procédures fassent une distinction entre les données à caractère personnel qu'il traite en sa qualité de responsable du traitement et les données à caractère personnel qu'il traite en sa qualité de sous-traitant. Si certaines données sont identiques, ces systèmes doivent pouvoir établir une distinction entre ces deux situations, de manière à ce que différents processus et différentes mesures puissent être appliqué(e)s à chaque situation.

Si toutefois une organisation intervient simultanément en tant que responsable du traitement et en tant que sous-traitant pour différentes activités de traitement sur la base des mêmes données à caractère personnel, les personnes concernées doivent être correctement informées par l'organisation, aussi bien en sa qualité de responsable du traitement qu'en sa qualité de sous-traitant, et ce évidemment dans la mesure où les activités de traitement sont licites. Cela s'applique notamment pour les concepteurs d'un logiciel de reconnaissance faciale qui d'une part interviennent en tant que sous-traitant vis-à-vis d'une entité qui utilise ce logiciel pour des finalités déterminées (le responsable du traitement) mais d'autre part vont également traiter les données collectées pour des finalités personnelles. Les informations à fournir doivent dans ce cas mentionner les différents traitements ainsi que les données collectées, les destinataires des données et leurs finalités propres.

Exemple

Dans un restaurant chinois de la chaîne KFC, un logiciel de reconnaissance faciale (conçu par Baidu, l'homologue chinois de Google) est utilisé afin de prédire les préférences du client. Dans cette relation, KFC est le responsable du traitement (cette société détermine en effet les finalités du traitement) et Baidu est le sous-traitant, étant donné que son logiciel assure le traitement effectif. Si toutefois Baidu

utilise les données à caractère personnel en question pour établir des profils biométriques de clients et les communiquer à des entreprises tierces, elle agit en sa qualité de responsable du traitement[10].

Enfin, l'Autorité veut souligner que vos employés ne sont pas vos sous-traitants. Tant que ces employés agissent sous votre autorité dans le cadre d'un lien de subordination, ils font partie intégrante de votre organisation.

2. Définition des données biométriques

2.1 Contexte

L'article 4.14) du RGPD définit les 'données biométriques' comme étant "*les 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* ". Lorsque les données ne sont pas traitées en vue de l'identification unique de personnes mais que cela est toutefois possible, compte tenu de la nature des données, il s'agira donc également d'un traitement de données biométriques au sens du RGPD.

Afin d'éviter toute confusion à cet égard et de favoriser la sécurité juridique, il importe de faire remarquer que la notion de données biométriques a une autre signification dans le contexte scientifique que dans le contexte de protection des données (européen). La définition scientifique se retrouve dans la Norme internationale ISO/IEC 2382-37[11] et est libellée comme suit : "*biometric sample or aggregation of biometric samples at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property.*" La norme ISO/IEC considère dès lors ce qui suit comme des données biométriques : (1) l'enregistrement de données (`*biometric sample*'), (2) l'extraction de données provenant d'échantillons (`*biometric feature*'), (3) l'attribution d'échantillons biométriques à des individus déterminés (`*biometric reference*') et (4) la comparaison entre les différents échantillons *biometric probe*'). On remarque d'emblée que la notion dans le contexte scientifique ne concerne pas nécessairement le lien entre un individu et ses données biométriques, ce alors que l'identification ou plutôt l' "**identifiabilité**" d'un individu est fondamentale pour la notion de 'données biométriques' dans le contexte de la protection des données. Le traitement de données biométriques au sens scientifique sans possibilité d'identifier les individus ne relève donc pas du champ d'application du RGPD. Les données biométriques ne peuvent en effet être classées en tant que données à caractère personnel

[10] Pour de plus amples informations, voir : https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition.
[11] La Norme internationale ISO/IEC 2382-37 est le texte de référence scientifique en matière de biométrie et elle harmonise le vocabulaire international au niveau de la biométrie https://www.iso.org/standard/55194.html.

que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique (même lorsque ce n'est pas le but de prime abord)[12]. Une telle conclusion est conforme à l'article 4.1) du RGPD d'où il découle que la notion de données à caractère personnel se rapporte uniquement à **une personne physique identifiée ou identifiable**.

Néanmoins, il y a lieu de constater que la notion de données biométriques a été définie en des termes assez généraux, ce qui implique que le RGPD reconnaît que la technologie biométrique est encore en plein développement et continuera à évoluer.

Enfin, en vertu de l'article 9.1 du RGPD, les données biométriques sont une catégorie particulière de données à caractère personnel. Le traitement de telles catégories particulières est en principe interdit, à moins que les conditions d'un des motifs d'exception à l'interdiction de traitement énumérés à l'article 9.2 du RGPD soient remplies. Les implications de cette qualification sur le traitement sont expliquées de manière circonstanciée dans le Chapitre III de la présente recommandation.

2.2 Interprétation concrète de la notion de données biométriques

Le RGPD distingue deux catégories d'informations pouvant être considérées comme des données biométriques. La première catégorie concerne des propriétés physiques - à savoir les caractéristiques physiques ou physiologiques d'une personne. Le contenu de cette catégorie est assez simple et correspond à ce que la plupart des gens comprennent par données biométriques, comme par exemple des informations relatives au visage, les empreintes digitales et les scans de l'iris.

La deuxième catégorie, des informations comportementales, est considérablement plus large. Chaque caractéristique comportementale permettant l'identification unique d'une personne est logiquement censée être une donnée biométrique. Les possibilités de traitement en matière d'informations comportementales évoluent toutefois rapidement. Par conséquent, il n'est pas possible d'établir une liste exhaustive de tels traitements. Il sera donc toujours nécessaire de vérifier à l'aide d'éléments concrets s'il s'agit ou non d'un traitement de données comportementales permettant l'identification unique de personnes.

Exemples de données biométriques comportementales
L'utilisation de modèles de claviers, d'écrans tactiles et de souris afin d'authentifier des personnes (qui suscite un vif intérêt dans le secteur bancaire[13].
L'identification à l'aide de la démarche unique de personnes (en anglais *gait recognition*)[14].

[12] Considérant 51 du RGPD.
[13] Voir : https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/inspired/behavioral-biometrics.
[14] Voir : https://www.biometricupdate.com/201311/explainer-gait-recognition.

2.3 Gabarits biométriques

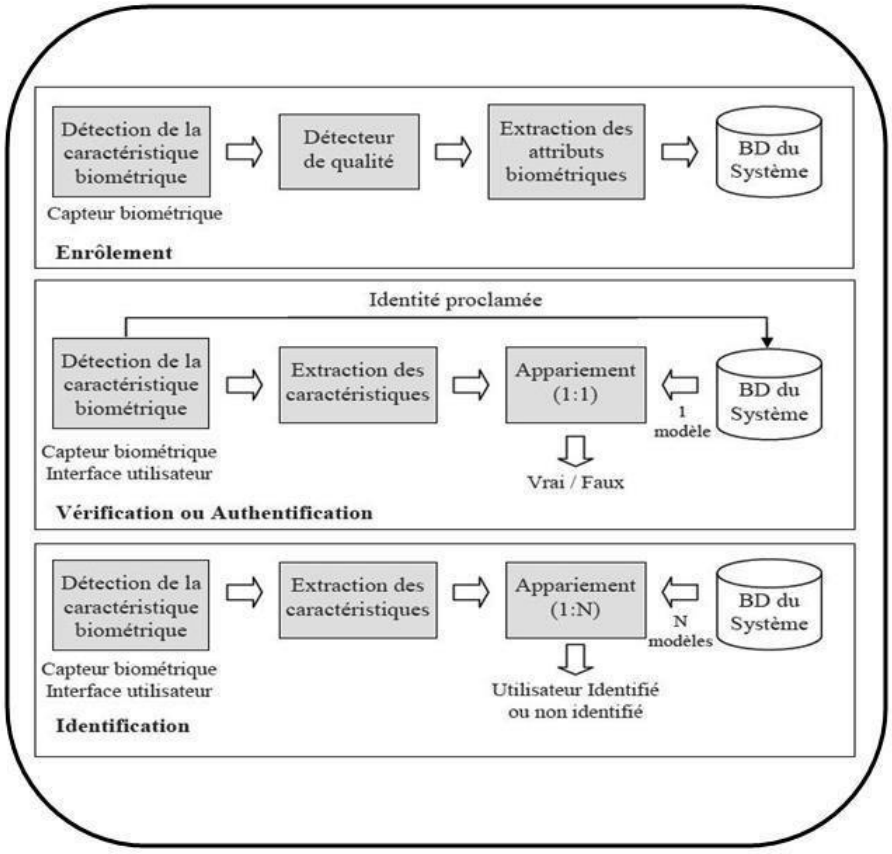
Le fonctionnement d'un système biométrique est scindé en deux phases de collecte des informations et deux manières de comparer les informations collectées (les deux fonctions des systèmes biométriques).

PHASES DE COLLECTE

La première phase de collecte, ce qu'on appelle l'inscription (ou l'enregistrement), est le moment où une caractéristique biométrique de la personne concernée est collectée et enregistrée sur un support pour stocker des informations (soit un support individuel comme un badge ou un token, soit dans une base de données). Ces informations de référence seront soit la donnée biométrique brute (comme par exemple l'image du visage, de la main, de l'iris ou l'empreinte digitale), soit l'ensemble d'informations codées, obtenu au départ des caractéristiques individuelles et uniques de la donnée brute dans le but de vérifier ou d'établir l'identité d'un individu (un gabarit). Bien que ces gabarits soient distincts des données biométriques brutes, ils relèvent incontestablement du champ d'application du RGPD. En outre, l'Autorité fait remarquer que conformément à l'article 5.1.f) *juncto* l'article 32 du RGPD et compte tenu du principe de '*privacy by design*[15]', il ne sera plus possible de recourir licitement à un système qui enregistre les informations de référence sous leur forme brute (entendez : la donnée biométrique brute). Au cours de la première phase de collecte, les données biométriques brutes devront toujours être converties en gabarits. Après quoi, les données brutes devront immédiatement être supprimées.

Lors de la deuxième phase de collecte, l'individu montre à nouveau ses caractéristiques biométriques au système qui doit l'authentifier. À ce moment, un deuxième échantillon biométrique est prélevé (une personne tient par exemple son doigt devant le capteur) et ces informations (la donnée brute ou le gabarit) sont ensuite comparées aux informations de référence pour vérifier si elles correspondent. Si les informations collectées au cours de la deuxième collecte correspondent aux informations de référence (association positive), le système considère que la personne qui se présente est celle qui a été enregistrée préalablement lors de la phase d'inscription.

[15] Voir l'article 25 du RGPD.



Modèle schématique d'un système biométrique pour la vérification de l'*identité* consistant en une phase d'enregistrement et de vérification.

Selon la manière dont le gabarit est enregistré, des conditions strictes s'appliquent. La recommandation distingue trois possibilités :

- (type 1) Maîtrise du gabarit par la personne concernée elle-même : le seul support de stockage durable du gabarit est exclusivement conservé par la personne concernée ou, le cas échéant, dans l'appareil dans lequel le capteur biométrique est installé sans l'association possible avec d'autres systèmes informatiques. Il suffit de penser à un badge, à un token ou à un enregistrement local dans le capteur à l'entrée du bâtiment. Il faut en principe utiliser cette méthode et on ne peut y déroger que dans des cas exceptionnels ;
- (type 2) Maîtrise partagée : Il existe une base de données centrale des gabarits sous maîtrise du responsable du traitement sans que ce dernier puisse toutefois l'utiliser sans le consentement de la personne concernée. Comme par exemple lorsque l'accès à un gabarit déterminé n'est accordé que moyennant l'introduction d'un mot de passe choisi par la personne concernée.
- (type 3) Maîtrise exclusive par le responsable du traitement : le gabarit est enregistré sous une forme exploitable dans une base de données des gabarits sous maîtrise exclusive du responsable du traitement. Dans ce cas, les conditions les plus strictes doivent être respectées et la réalisation préalable d'une analyse d'impact relative à la protection des données sera toujours nécessaire.

L'Autorité souligne que l'enregistrement de gabarits conformément aux types 2 et 3 ne sera possible que dans des circonstances exceptionnelles. Il suffit de penser par exemple à l'authentification dans des environnements critiques où la perte d'un token ou d'un badge (maîtrise exclusive par la personne concernée) aurait des conséquences particulièrement graves (par exemple : l'accès à un centre opérationnel d'une centrale nucléaire).

Enfin, l'Autorité souhaite souligner dans ce contexte que la présente recommandation ne concerne en principe pas l'usage tout à fait local par l'utilisateur d'une authentification à l'aide de systèmes biométriques. De tels traitements de données biométriques relèvent en effet de l'exception domestique conformément à l'article 2.2.c) du RGPD. Il suffit de penser dans ce cadre à l'authentification personnelle au moyen de smartphones ou d'autres appareils électroniques dans lesquels un logiciel de reconnaissance faciale et des capteurs d'empreintes digitales sont de plus en plus souvent proposés comme alternative au code PIN traditionnel. Les conditions et modalités de l'exception domestique sont expliquées en détail dans la rubrique III.1.3.3 ci-dessous.

PHASE COMPARATIVE

Il existe deux manières de comparer les informations qui ont été obtenues lors des phases de collecte et elles constituent les deux principales fonctions de la biométrie : la fonction d'identification et la fonction de vérification. Bien que ces deux fonctions puissent être utilisées dans le cadre de l'authentification, la fonction de vérification est incontestablement préférable (étant donné que les informations de référence biométriques ne doivent pas nécessairement être enregistrées dans une base de données centrale) et la fonction d'identification ne pourra être utilisée que dans des cas exceptionnels et motivés.

La fonction d'identification consiste à comparer les informations de la deuxième phase avec toutes les informations biométriques disponibles dans le système biométrique et enregistrées par définition dans une base de données (`*one-to-many comparison*'). Cette fonction permettra tout d'abord d'identifier l'utilisateur parmi toutes les personnes enregistrées et pourra servir à l'authentifier lors d'une phase ultérieure.

La fonction de vérification consiste à comparer les informations de la deuxième phase aux informations enregistrées au préalable appartenant à une seule personne (`*one-to-one comparison*'). Cette fonction se prête en particulier à des situations dans lesquelles la personne souhaite s'authentifier et est donc disposée à faire connaître volontairement un élément permettant de l'identifier sur la base de la comparaison entre les informations de référence définies au préalable et l'échantillon de la nouvelle collecte.

III. Application des principes de protection des données au traitement de données biométriques

1. Base juridique

1.1 Pourquoi une base juridique ?

Le traitement de données à caractère personnel est en principe uniquement autorisé s'il se fonde sur une des six bases juridiques prévues à l'article 6 du RGPD. Lorsqu'il est question d'un traitement de catégories particulières de données à caractère personnel, il faudra aussi recourir à un des motifs d'exception prévus à l'article 9.2 du RGPD. La présence d'un motif d'exception tient lieu dans ce cas de base juridique pour le traitement. Vous ne pouvez pas traiter de données sans base juridique, vous devez donc veiller à disposer d'une telle base avant d'entamer votre traitement.

Il est également essentiel de vous demander quelle est votre base juridique, étant donné que les conditions de chacune des bases juridiques sont différentes. Le choix de votre base juridique a des conséquences pour les droits des personnes concernées, dont vous devez connaître les particularités, pas uniquement pour pouvoir les informer correctement mais également pour garantir l'exercice effectif de leurs droits.

La qualification de la notion de 'données biométriques' en tant que catégorie particulière de données à caractère personnel au sens de l'article 9.1 du RGPD a des conséquences importantes pour la détermination de la base juridique et implique que les lignes directrices *en matière de traitement de données biométriques dans le cadre de l'authentification de personnes* de la Commission de la protection de la vie privée ne sont plus d'application. Cet aspect est expliqué de manière circonstanciée dans la rubrique III.1.3. ci-dessous.

1.2 La base juridique peut-elle être modifiée ?

La base juridique ne peut pas être modifiée lors du traitement. Cela signifie que si le responsable du traitement invoque une base juridique inappropriée ou que celle-ci "n'est plus valable" parce que les conditions ne sont pas ou plus remplies, le traitement ne peut pas se poursuivre.

Si un traitement se base par exemple sur le consentement (explicite), dès que la personne retire son consentement, vous devez cesser tous les traitements de données fondés sur cette base juridique, à moins que vous ne continuiez à traiter les mêmes données dans le cadre d'une autre finalité pour laquelle vous disposez d'une autre base juridique valable.

1.3 Quelle base juridique utiliser pour le traitement de données biométriques ?

Il n'existe pas de hiérarchie entre les bases juridiques prévues par le RGPD. Il vous appartient de démontrer que votre traitement se fonde valablement sur un des motifs d'exception conformément à l'article 9.2 du RGPD, étant donné que les traitements visés dans la présente recommandation concernent toujours des catégories particulières de données à caractère personnel, à savoir des données biométriques. À cet égard, il faut toutefois signaler qu'il ressort des lignes directrices du Groupe 29 et de l'EDPB qu'une double base juridique n'est requise que si le motif d'exception mentionné à l'article 9.2 du RGPD offre moins de protection que les bases juridiques mentionnées à l'article 6 du RGPD. Ce sera par exemple le cas lorsque le responsable du traitement invoque l'article 9.2.e) du RGPD : pour des données sensibles rendues publiques par la personne concernée elle-même, il faut recourir à une base juridique de l'article 6 du RGPD. Toutefois, lorsque le traitement repose sur l'article 9.2.a) du RGPD (le consentement explicite) ou l'article 9.2.g) du RGPD (un intérêt public important), ce n'est pas nécessaire.

De plus, comme mentionné dans le considérant 132 du RGPD, certaines lois spécifiques précisent la base juridique sur laquelle les responsables du traitement doivent se fonder pour pouvoir traiter des données. Il est donc de votre responsabilité de vérifier si, sur la base d'une loi spécifique, vous êtes obligé d'utiliser une base juridique spécifique.

N'oubliez pas, conformément aux exigences de l'article 13 ou de l'article 14 du RGPD, d'informer en tout état de cause les personnes concernées de la base juridique de vos traitements. Quelle que soit la base juridique sur laquelle vous vous fondez, vous devez la communiquer aux personnes concernées.

Enfin, malgré l'absence de toute hiérarchie, certaines bases juridiques s'avèrent plus adaptées que d'autres à la réalité du traitement de données biométriques en vertu du RGPD. En d'autres termes, vu les conditions qui y sont liées, il sera difficile de s'appuyer dans ce contexte sur certaines bases juridiques. En ce qui concerne les traitements visés dans la présente recommandation, deux bases juridiques méritent d'être davantage précisées, vu leur intérêt pratique. Il s'agit plus particulièrement du consentement explicite (art. 9.2.a) du RGPD) et de l'intérêt public important (art. 9.2.g) du RGPD).

L'article 9.4 du RGPD laisse aux États membres la possibilité de maintenir ou d'introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques,

des données biométriques ou des données concernant la santé. De telles dispositions peuvent ensuite servir de base juridique pour le traitement[16]. Ce sera notamment nécessaire lorsque le responsable du traitement veut s'appuyer sur l'intérêt public important. Ceci est expliqué de manière circonstanciée dans la rubrique III.1.3.2. ci-dessous.

1.3.1. Consentement explicite

Le consentement explicite doit être scindé en deux éléments. Tout d'abord, il faut un consentement **valable** pour le traitement et ensuite, ce consentement doit être **explicite**[17].

CONSENTEMENT VALABLE

L'article 4.11) du RGPD précise qu'il ne peut être question d'un consentement de la personne concernée que s'il s'agit d'une manifestation de volonté (1) libre, (2) spécifique, (3) éclairée et (4) univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Les sections suivantes préciseront brièvement la manière dont ces éléments doivent être évalués.

Premièrement, l'élément 'libre' implique qu'il doit y avoir un véritable choix pour la personne concernée. En règle générale, si la personne concernée n'a pas de véritable choix, se sent obligée de donner son consentement ou risque de subir des préjudices en l'absence de consentement, il ne peut pas s'agir d'un consentement valable au sens du RGPD. Un tel consentement n'est pas considéré comme ayant été donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice. Le RGPD accorde aussi une attention au concept - important dans ce contexte - d'un déséquilibre entre le responsable du traitement et la personne concernée.

Un déséquilibre survient notamment dans le cadre de la relation de travail. Vu la subordination résultant de la relation entre employeur et employé, il est improbable que la personne concernée puisse refuser son consentement au traitement de données sans crainte ou réelle menace de conséquences négatives découlant de ce refus. Il est improbable que l'employé puisse réagir librement à une demande de consentement de son employeur par exemple pour l'activation de systèmes d'authentification avec

[16] Voir par ex. l'article 29 de la loi néerlandaise du 16 mai 2018 *houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (Uitvoeringswet Algemene verordening gegevensbescherming (ci-après UAVG) (loi d'exécution du RGPD)) (Pays-Bas) et l'article 8.II.9 de la Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés* (France).

[17] Pour des informations complètes sur le consentement, nous vous renvoyons aux Lignes directrices 5/2020 de *l'EDPB sur le consentement au sens du règlement (UE) 2016/679*, disponibles via le lien suivant : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fr.pdf.

empreinte digitale pour accéder à des locaux ou à des données sensibles. Pour cette raison, l'Autorité estime qu'il est problématique, pour des employeurs, de traiter des données à caractère personnel (biométriques) d'employés sur la base du consentement (explicite), étant donné qu'il est improbable que celui-ci soit donné librement.

Les déséquilibres entre la personne concernée et le responsable du traitement ne se limitent toutefois pas aux relations de travail. Comme déjà précisé ci-dessus, il est question d'un déséquilibre chaque fois que le rapport de force entre le responsable du traitement et la personne concernée compromet le caractère libre du consentement. Le traitement de données effectué par les autorités publiques en est un exemple important mais il ne relève pas du cadre de la présente recommandation. En outre, on peut également penser à la relation entre une école et ses élèves ou à des situations dans lesquelles le prestataire d'un service ou le fournisseur d'un bien détient le (quasi) monopole. Dans ces cas aussi, il s'agit effectivement d'un rapport de force factuel étant donné qu'il est improbable que la personne concernée refuse de donner son consentement sans crainte de conséquences négatives.

Concrètement, le responsable du traitement qui veut traiter des données biométriques au sens du RGPD devra toujours vérifier s'il est question d'un rapport de force en tenant compte de la situation factuelle. En d'autres termes, l'absence d'un rapport de force officiel n'exclut pas *de facto* l'existence de celui-ci. En la matière, il faut toujours réaliser une évaluation concrète.

Exemple

Le 22 août 2019, l'autorité de contrôle suédoise (*Datainspektionen*) a infligé une amende de 200 000 SEK (environ 20 000 EUR) à une école pour l'utilisation d'un logiciel de reconnaissance faciale dans le cadre du contrôle de la présence des élèves. Bien que l'école ait basé son traitement sur le consentement, l'autorité de contrôle suédoise a estimé que ce consentement n'était pas valable vu le rapport de force entre le responsable du traitement et les personnes concernées[18].

En outre, au moment de déterminer si le consentement a été donné librement, il y a lieu de tenir compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat[19]. L'article 7.4 du RGPD vise à garantir que les finalités du traitement de données à caractère personnel ne soient pas dissimulées en associant le consentement à

[18] Voir : https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_fr.

[19] Article 7.4 du RGPD : "*Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat*". Voir également le considérant 43 du RGPD qui *est libellé comme suit : "[...] Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.*"

ce traitement à l'exécution d'un contrat pour lequel ces données à caractère personnel ne sont pas nécessaires. Le RGPD assure ainsi que le traitement de données à caractère personnel pour lequel le consentement est demandé ne peut pas être directement ou indirectement la contrepartie d'un contrat. Contraindre à consentir à l'utilisation de données à caractère personnel, outre ce qui est strictement nécessaire à la réalisation des finalités, restreint en effet le choix de la personne concernée et empêche un consentement libre.

La charge de la preuve pour démontrer qu'il ne s'agit pas d'une telle conditionnalité incombe au responsable du traitement. Cette preuve peut par exemple être fournie en démontrant que son organisation offre aux personnes concernées un véritable choix entre un service comprenant un consentement pour l'utilisation de données à caractère personnel pour des finalités complémentaires d'une part, et un service équivalent offert par le même responsable du traitement qui ne comprend pas de consentement pour l'utilisation de données pour des finalités complémentaires d'autre part[20].

Deuxièmement, le consentement doit être spécifique. En vertu de l'article 6.1.a) du RGPD, cette spécificité concerne la (les) finalité(s) du traitement. Cette exigence vise à offrir un certain contrôle et une certaine transparence à la personne concernée et est étroitement liée à l'exigence d'un consentement 'éclairé'.

Conformément à l'article 5.1.b) du RGPD, l'obtention d'un consentement licite est toujours précédée de la définition d'une finalité déterminée, explicite et légitime pour l'activité de traitement poursuivie (voir ci-dessous la rubrique III.2). "*Combinée à la notion de limitation de la finalité, la nécessité d'obtenir un consentement spécifique sert de garantie contre l'élargissement ou l'estompement progressif des fins auxquelles les données* (biométriques) *sont traitées après qu'une personne concernée a donné son consentement à la collecte initiale de ses données. Ce phénomène, également connu sous le terme de détournement d'usage, constitue un risque pour les personnes concernées dès lors qu'il peut entraîner une utilisation imprévue de leurs données à caractère personnel par le responsable du traitement ou par de tierces parties*"[21]. C'est surtout lorsque le traitement concerne des catégories particulières de données, dont font partie les données biométriques, qu'il est pertinent d'exclure le détournement d'usage. Les personnes concernées accordent leur consentement dans l'idée qu'elles peuvent exercer un contrôle et que leurs données sont exclusivement traitées pour la (les) finalité(s) mentionnée(s). Si un responsable du traitement traite des données sur la base d'un consentement (explicite) et qu'il veut également traiter les données pour d'autres finalités, il doit demander un consentement supplémentaire pour ces autres finalités, à moins qu'il n'existe une autre base juridique mieux adaptée à la situation.

[20] Lignes directrices 5/2020 de l'EDPB *sur le consentement au sens du règlement (UE) 2016/679*, p. 10-12 et voir également l'avis 06/2014 du Groupe 29 *sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE* (http://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2014/wp217_fr.pdf).
[21] Lignes directrices 5/2020 de l'EDPB *sur le consentement au sens du règlement (UE) 2016/679*, point 56.

Troisièmement, le RGPD requiert que le consentement soit éclairé, ce qui implique que la personne qui donne son consentement doit parfaitement comprendre ce à quoi elle consent et à quelles fins. La transparence est un des principes fondamentaux du RGPD et est étroitement liée aux principes de loyauté et de licéité. Il est nécessaire de fournir des informations aux personnes concernées avant d'obtenir leur consentement pour leur permettre de prendre des décisions éclairées, de comprendre ce à quoi elles consentent et par exemple d'exercer leur droit au retrait du consentement. Si le responsable du traitement ne fournit pas d'informations compréhensibles, le contrôle de la personne concernée n'est qu'illusion et le consentement n'est pas une base licite pour le traitement.

Il découle des lignes directrices de l'EDPB qu'il faut au moins prévoir les informations suivantes afin d'obtenir un consentement valable :

- l'identité du responsable du traitement ;
- la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité ;
- les (types de) données collectées et utilisées ;
- l'existence du droit de retirer son consentement ;
- des informations concernant l'utilisation des données pour la prise de décision automatisée conformément à l'article 22.2.c) du RGPD, le cas échéant ; et
- des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées telles que décrites aux articles 45 du et 46 du RGPD.

Ces informations doivent être fournies en des termes clairs et simples : il convient d'exclure de longues déclarations de confidentialité formulées dans un jargon juridique qui n'est pas à la portée de tous[22].

En outre, la demande de consentement doit être présentée distinctement de toutes les autres demandes.

Une quatrième et dernière condition est que le consentement doit être univoque. Le RGPD précise explicitement que pour un consentement, une déclaration ou un acte positif clair de la personne concernée est requis(e). En d'autres termes, il ne peut y avoir aucun doute raisonnable quant à l'intention de la personne concernée de donner son consentement pour le traitement envisagé de ses données à caractère personnel. Le silence, l'utilisation de cases cochées par défaut ou l'inactivité ne peuvent dès lors pas avoir valeur de consentement. Le consentement donné doit valoir pour toutes les

[22] Pour de plus amples informations, voir ci-dessous la rubrique III.6 ainsi que les lignes directrices du Groupe 29 *sur la transparence au sens du règlement (UE) 2016/679* (à télécharger via : https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227).

activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement doit être donné pour chacune d'entre elles[23].

L'univocité du consentement implique également que les personnes concernées doivent pouvoir comprendre clairement les options dont elles disposent et, si plusieurs options sont disponibles, le choix de consentir au traitement de leurs données biométriques doit être clairement distinct de tout autre choix.

CONSENTEMENT EXPLICITE

Conformément à l'article 9.2.a) du RGPD, un consentement explicite est requis dans certaines situations dans lesquelles il existe un risque grave pour la protection des données et dès lors dans lesquelles un niveau élevé de contrôle individuel des données à caractère personnel est jugé approprié.

Le terme 'explicite' renvoie à la manière dont le consentement est exprimé par la personne concernée. Cela signifie que la personne concernée doit rédiger une déclaration explicite de consentement. Une manière évidente de veiller à ce que le consentement soit explicite est de le confirmer dans une déclaration écrite. Le cas échéant, le responsable du traitement pourrait veiller à ce que la déclaration écrite soit signée par la personne concernée afin de dissiper tout doute éventuel et d'exclure une éventuelle absence de preuve dans le futur.

Une telle déclaration signée ne constitue toutefois pas la seule manière d'obtenir un consentement explicite et le RGPD ne précise pas que dans toutes les circonstances nécessitant un consentement explicite valable, une déclaration écrite et signée est requise. Dans le contexte numérique ou en ligne par exemple, une personne concernée peut fournir la déclaration requise en complétant un formulaire électronique, en envoyant un e-mail, en téléchargeant un document scanné sur lequel figure sa signature ou au moyen d'une signature électronique. En théorie, l'utilisation de déclarations verbales peut également suffire pour obtenir un consentement explicite valable mais il peut être difficile pour un responsable du traitement de prouver que lors de l'enregistrement de la déclaration, toutes les conditions d'un consentement explicite valable étaient remplies.

[23] Considérant 32 du RGPD.

Exemple

Le 4 décembre 2019, l'autorité de contrôle néerlandaise (ci-après l' "Autoriteit Persoonsgegevens") a infligé une amende administrative de 725 000 EUR à une entreprise pour traitement illicite des empreintes digitales de ses employés. L'Autoriteit Persoonsgegevens a constaté à cet effet que le responsable du traitement avait invoqué à tort le consentement explicite comme motif d'exception. Les collaborateurs sont en effet subordonnés à leur employeur et en tant que tels, il est toujours question d'un rapport de force qui exclut un consentement valable en droit. En outre et à titre secondaire, l'Autoriteit Persoonsgegevens a jugé qu'en tout état de cause, il ne s'agissait pas d'un consentement libre, spécifique, éclairé et univoque conformément à l'article 4.11) du RGPD.

CONSENTEMENT VALABLE CONFORMÉMENT À L'ARTICLE 7 DU RGPD

Même lorsqu'il s'agit d'un consentement libre, spécifique, éclairé, univoque et explicite, le responsable du traitement devra également respecter les conditions de l'article 7.1 et de l'article 7.3 du RGPD.

L'article 7.1 du RGPD[24] dispose que le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. Pour répondre à cette exigence, le responsable du traitement est libre d'opter pour la méthode la plus appropriée. Ainsi, en cas de plainte de la personne concernée ou d'un contrôle par l'autorité de contrôle, le responsable du traitement peut simplement démontrer qu'il a agi conformément aux dispositions du RGPD.

L'obligation de pouvoir démonter le consentement s'applique aussi longtemps que le traitement a lieu. Au terme de ce traitement, la preuve du consentement ne peut pas être conservée au-delà du temps nécessaire au respect de cette obligation légale ou à la constatation, à l'exercice ou à la défense de droits en justice, comme le prévoit l'article 17.3.b) et e) du RGPD.

En outre, conformément à l'article 7.3 du RGPD, la personne concernée a le droit de retirer son consentement à tout moment. Avant que la personne concernée donne son consentement, elle doit être informée du fait qu'elle peut retirer son consentement gratuitement et sans subir de préjudice[25] (comme par exemple une diminution du niveau de service accordé jusqu'alors ou même le refus de celui-ci).

Bien que le RGPD accorde une place de premier plan au retrait du consentement, il ne prescrit pas sous quelle forme ce retrait doit ou peut être effectué. L'EDPB affirme à cet égard : "*Toutefois, lorsque le consentement est obtenu par voie électronique uniquement par un clic, une frappe ou en balayant l'écran, les personnes concernées doivent, en pratique, pouvoir retirer ce consentement par le même*

[24] Voir également le considérant 42 du RGPD.
[25] Voir le considérant 42 du RGPD.

biais."[26]. Obliger les personnes concernées à suivre un cheminement complexe via des liens vers des documents électroniques ou les contraindre à saisir un mot de passe ne respecte pas l'exigence de pouvoir retirer son consentement de manière aussi simple qu'on l'a donné. En outre, le responsable du traitement doit veiller à ce que le consentement d'un autre utilisateur ne puisse pas être retiré à son insu ou sans son consentement.

Lorsque le consentement est retiré, il faut cesser toutes les activités de traitement qui concernent cette personne. Toutefois, cela n'a pas d'incidence sur la licéité du traitement (sur la base de ce consentement) avant le retrait du consentement. Le responsable du traitement devra également vérifier si la conservation des données utilisées pour le traitement en question est justifiée ou non, même si la personne concernée n'a pas introduit de demande de suppression. En effet, conformément à l'article 5.1.e) du RGPD, la conservation des données à caractère personnel doit être limitée à la finalité poursuivie (voir ci-dessous la rubrique III.5).

Ce n'est que lorsque les données de la personne concernée sont nécessaires lors de l'exécution d'un traitement pour d'autres finalités pour lesquelles il existe également une base juridique valable que les données peuvent éventuellement être conservées. Si tel n'est pas le cas, elles doivent être supprimées.

1.3.2. Intérêt public important

Conformément à l'article 9.2.g) du RGPD, les données biométriques ne peuvent être traitées que lorsque ce "*traitement est nécessaire pour des motifs 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*". Ce motif d'exception joue un rôle important notamment lorsque - par exemple, en raison de l'existence d'un rapport de force entre le responsable du traitement et la personne concernée - on ne peut pas invoquer le consentement explicite, conformément à l'article 9.2.a) du RGPD. Cela implique en effet qu'il faut toujours préférer le consentement explicite et qu'un responsable du traitement ne pourra invoquer l'intérêt public important en tant que base juridique du traitement de données biométriques que dans des cas déterminés, spécifiés par la loi.

Exemple

La seule loi qui prévoit actuellement explicitement le traitement de données biométriques est la loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour*, exécutée par l'arrêté royal du 25 mars 2003 *relatif aux cartes d'identité*.

[26] Lignes directrices 5/2020 de l'EDPB *sur le consentement au sens du règlement (UE) 2016/679*, p. 25.

Dans ce cadre, on peut faire référence au niveau européen au Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres*. Ce règlement prévoit également le traitement d'une photo faciale et d'une empreinte digitale.

Contrairement à plusieurs de nos voisins, le législateur belge n'a pas choisi de prévoir 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.

Exemple

L'article 29 de l'UAVG, la loi néerlandaise d'exécution du RGPD, dispose qu'en raison de l'article 9.2.g) du RGPD, l'interdiction de traiter des données biométriques en vue de l'identification unique d'une personne ne s'applique pas si le traitement est nécessaire à l'authentification ou à des fins de sécurité.

Cela implique toutefois que dans la mesure où l'on ne peut pas invoquer le consentement explicite et à l'exception du traitement des données biométriques dans le cadre de l'eID (carte d'identité électronique) et du passeport, chaque traitement de données biométriques à des fins d'authentification de personnes a lieu actuellement sans base juridique. Faire reposer un traitement sur des motifs d'intérêt public important, sans qu'aucune disposition du droit de l'Union ou d'un l'État membre ne le prévoie, semble en effet incompatible avec l'esprit de l'article 9.2.g) du RGPD.

Dès lors, l'Autorité estime qu'une obligation formulée de manière générale dans le chef du responsable du traitement de 'prévoir des mesures de sécurité suffisantes' ne peut pas être considérée comme étant de nature à justifier l'utilisation de données biométriques. Bien que l'Autorité admette que le traitement de données biométriques pour l'identification ou l'authentification de personnes puisse être justifié dans certains cas, il faudra toujours prévoir une disposition légale (générale ou sectorielle) qui permet le traitement de données biométriques dans certains cas, vu l'article 9.2.g) du RGPD. En ce sens, l'Autorité veut souligner que la simple existence d'une disposition légale n'est pas un sauf-conduit pour le traitement de données biométriques et qu'elle ne dispense nullement le responsable du traitement de son obligation d'étayer la nécessité et la proportionnalité du traitement de données. En d'autres termes, le responsable du traitement devra vérifier si les finalités qu'il poursuit sont de nature à ce que l'utilisation de la biométrie soit **inévitable**.

Exemple

Le 12 août 2019, le magasin de chaussures Manfield a été condamné par le tribunal d'Amsterdam pour l'utilisation d'un système de caisse fonctionnant sur la base d'un scan de l'empreinte digitale. Manfield a avancé que cela était permis en vertu de l'article 24 de l'UAVG *juncto* l'article 9.2.g) du RGPD, étant donné que l'utilisation d'un système d'autorisation par scan de l'empreinte digitale était nécessaire pour sécuriser des informations sensibles, à savoir des informations financières et des données à caractère personnel tant des employés que de la clientèle. En outre, un tel système était censé empêcher la fraude avec les caisses. Le juge a rejeté ces arguments et a affirmé que l'utilisation de la biométrie pour des finalités d'authentification ou de sécurité ne réussissait le test de proportionnalité que dans des cas exceptionnels. En l'occurrence, Manfield n'a pas suffisamment démontré qu'il n'existait pas d'alternative moins radicale pour réaliser les mêmes finalités[27].

Il sera toujours requis de mettre en balance les intérêts (importants) poursuivis avec les risques pour les droits et libertés des personnes concernées. À cet effet, on peut par exemple vérifier de quelle manière le traitement envisagé influence la société, tant 'en profondeur' (l'ampleur de l'avantage ou du préjudice ressenti en raison du traitement) qu' 'en largeur' (le nombre de personnes qui perçoivent un avantage ou un préjudice). Ainsi, dans l'exemple susmentionné, il s'agit d'un préjudice relativement grand (le recours obligatoire aux empreintes digitales) pour un groupe (proportionnellement) relativement grand de personnes concernées (tous les employés du magasin de chaussures) qui n'est pas proportionnel à l'avantage perçu par une seule personne (le propriétaire du magasin). Comparons cela à l'utilisation de l'authentification biométrique en vue d'accorder un accès aux locaux d'une centrale nucléaire. Le préjudice perçu par les employés (proportionnellement un groupe relativement petit de personnes concernées) ne contrebalance pas l'avantage dont bénéficie l'ensemble de la population (la sécurité d'une infrastructure critique).

Tout 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. À cet effet, les secteurs, organisations ou instances professionnelles concerné(e)s peuvent introduire une demande motivée dont il ressort que le traitement est proportionné et nécessaire dans le cadre des finalités visées, que le contenu intrinsèque du droit à la protection des données à caractère personnel est respecté et que des mesures appropriées et spécifiques sont prises afin de protéger les droits et intérêts fondamentaux de la personne concernée. L'Autorité souligne qu'en vertu de l'article 23 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, des initiatives législatives dans ce cadre doivent toujours être soumises pour avis au Centre de Connaissances de l'Autorité. Dans ce contexte, on

[27] L'intégralité du jugement peut être consultée via le lien suivant : https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005.

vérifiera si la disposition légale est conforme au RGPD, et plus spécialement si le traitement envisagé est effectivement nécessaire pour des raisons d'intérêt public important.

Ces nouvelles exigences donnent lieu à une fracture avec le régime antérieur à l'entrée en vigueur du RGPD. Dès lors, compte tenu des principes de bonne gouvernance, dès la publication de la présente recommandation, il est prévu une période transitoire d'un an pendant laquelle le traitement de données biométriques sera toléré conformément à l'ancienne norme et l'Autorité n'interviendra pas de manière proactive. Cette période d'un an doit permettre aux responsables du traitement et au législateur de prendre les mesures nécessaires afin de mettre les traitements visés en conformité avec les dispositions du RGPD, comme expliqué dans la présente recommandation.

1.3.3. L'exception domestique

Il existe une application très spécifique, bien qu'omniprésente, de l'utilisation de données biométriques dans le cadre de l'authentification personnelle via des smartphones et d'autres appareils électroniques dans lesquels un logiciel de reconnaissance faciale et des capteurs d'empreintes digitales sont de plus en plus souvent proposés comme alternative au code PIN traditionnel. Vu l'importance que prennent de telles applications et l'ambiguïté qui les entoure souvent, ce sujet mérite quelques explications.

L'Autorité fait remarquer qu'il faut faire une distinction entre d'une part les données biométriques enregistrées sur l'appareil lui-même et d'autre part les données biométriques enregistrées à d'autres endroits. L'impact de cette distinction est considérable étant donné que pour la première catégorie, l'exception domestique de l'article 2.2.c) du RGPD peut s'appliquer. Lorsque les données biométriques ne sont toutefois pas (uniquement) conservées sur l'appareil ou lorsqu'elles sont également communiquées à des tiers, cette exception n'est plus valable et le responsable du traitement devra donc démontrer qu'il existe un des motifs d'exception énumérés à l'article 9.2 du RGPD.

L'article 2.2.c) du RGPD stipule que le règlement ne s'applique pas "*au traitement de données à caractère personnel effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique*". Lorsque les données biométriques (entendez : les gabarits créés qui permettent l'authentification par reconnaissance faciale ou au moyen d'une empreinte digitale) sont exclusivement conservées sur l'appareil, cela a pour conséquence que le processus d'authentification biométrique peut se dérouler localement et de manière autonome sans accès externe. Un traitement de données en ce sens - initié par la personne concernée et réalisé sous son contrôle - peut relever, sous certaines conditions, de l'exception domestique, ce qui implique que les règles du RGPD ne sont pas d'application[28].

Avant de pouvoir invoquer l'exception domestique, le fournisseur d'un appareil ou d'un service déterminé devra toutefois démontrer que les cinq conditions suivantes sont remplies :

- la personne concernée utilise cet appareil de manière privée - ses données biométriques ne peuvent être utilisées que par elle-même pour déverrouiller l'appareil ou pour accéder aux applications qu'elle a elle-même téléchargées ;
- c'est la personne concernée qui décide en toute indépendance d'utiliser la possibilité d'une authentification biométrique qui est intégrée dans son appareil. Cela implique que :

[28] Ce point de vue est partagé par l'autorité de protection des données française (la CNIL), voir : https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees.

    - des employeurs qui imposent des procédures d'authentification biométrique à leurs employés, par exemple via des appareils fournis dans le cadre de leur activité professionnelle, ne peuvent pas invoquer l'exception domestique ;
    - les fournisseurs d'un appareil ou d'un service déterminé doivent toujours, sans la moindre restriction, prévoir une alternative à l'authentification biométrique (comme par exemple l'utilisation d'un code PIN traditionnel). Si ce n'est pas le cas, le fournisseur concerné est pleinement considéré comme responsable du traitement, conformément à l'article 4.7) du RGPD, à l'égard des données biométriques traitées ;
- après avoir été créé par la personne concernée, le gabarit biométrique doit être enregistré sur l'appareil, dans un environnement partitionné offrant un niveau élevé de sécurité contre l'envoi d'informations au départ de cet environnement. Dès lors, lorsque le gabarit est enregistré en dehors de l'appareil ou si le gabarit est accessible à des tiers (par exemple le fournisseur de l'appareil ou du service ou le concepteur d'une application), il ne peut pas être question d'une exception domestique ;
- le gabarit biométrique doit être crypté conformément à l'état des connaissances ;
- la seule information pouvant être communiquée lors du contrôle d'accès est celle de savoir si l'authentification biométrique a réussi ou échoué.

Dans la mesure où les conditions précitées sont remplies, le fournisseur de l'appareil ou du service ne sera pas tenu responsable du traitement de données biométriques en question. Néanmoins, l'applicabilité de l'exception dans ce contexte n'implique nullement que le fournisseur soit purement et simplement dispensé de toutes ses obligations en vertu du RGPD. Logiquement, le fournisseur reste responsable du traitement de données à caractère personnel qui a lieu par le biais de son appareil ou de son service. Étant donné que l'accès à l'appareil ou au service s'effectue le cas échéant au moyen d'une authentification biométrique, la sécurité de l'application en question est extrêmement importante. À ce titre, le fournisseur devra démontrer la fiabilité de ses technologies d'authentification biométrique, notamment en garantissant que :

- le pourcentage de résultats faux positifs[29]/ faux négatifs[30] soit adapté au niveau de sécurité requis d'un service déterminé (par exemple, en ce qui concerne des applications particulièrement sensibles, comme l'accès à un smartphone, à des données bancaires ou à des documents cryptés, un pourcentage bas de résultats faux positifs devra être démontré) ;
- les technologies biométriques soient au moins à l'épreuve d'attaques qui, conformément à l'état des connaissances, doivent être considérées comme banales (par exemple l'utilisation d'une photo afin de tromper un logiciel ou un dispositif de reconnaissance faciale) ;

[29] Une situation dans laquelle un accès est accordé à tort à l'appareil ou au service.
[30] Une situation dans laquelle l'accès à l'appareil ou au service est refusé à tort.

- le nombre de tentatives d'authentification biométrique autorisées soit limité (par exemple après trois essais infructueux, la personne concernée ne peut plus accéder à l'application qu'en introduisant un code PIN).

Il va de soi que si les cinq conditions précitées ne sont pas remplies ou si la sécurité du système d'authentification biométrique ne peut pas être démontrée, le traitement de données biométriques relèvera incontestablement du champ d'application du RGPD.

2. Limitation des finalités[31]

Le principe de limitation des finalités est défini à l'article 5.1.b) du RGPD et établit que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Il faut distinguer deux éléments : (1) spécifier une (des) finalité(s) déterminée(s), explicite(s) et légitime(s) pour le traitement visé et (2) un élément de compatibilité qui implique qu'un traitement ultérieur n'est autorisé que dans la mesure où il n'est pas incompatible avec la (les) finalité(s) pour laquelle (lesquelles) les données ont été collectées initialement. Étant donné que la (les) finalité(s) choisie(s) déterminera (détermineront) dans une large mesure la base juridique sur laquelle il faudra fonder le traitement, il va de soi que la (les) finalité(s) doi(ven)t être définie(s) avant que le traitement ne puisse débuter[32].

Les données à caractère personnel ne peuvent être traitées que pour des finalités réelles ou existantes ou pour des finalités qui, à la lumière de l'activité effective du responsable du traitement, sont réalisables dans un avenir proche.

2.1 Finalité(s) initiale(s)

Pour chaque traitement de données qu'il envisage, le responsable du traitement doit définir la (les) finalité(s). Cela signifie qu'il faut définir ce qu'il veut concrètement atteindre en utilisant certaines données à caractère personnel.

Cette définition des finalités du traitement est essentielle pour le test de proportionnalité obligatoire concernant le traitement (afin de garantir que les données traitées et le traitement concret de celles-ci

[31] Pour de plus amples explications en la matière, voir : Groupe 29, *Opinion 03/2013 on purpose limitation* (avis sur la limitation des finalités), consultable via le lien suivant : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (uniquement disponible en anglais).
[32] Ceci ressort notamment de l'obligation du consentement 'éclairé' (voir ci-dessus) et voir également l'article 6.1.a) du RGPD.

soient proportionnés aux finalités poursuivies). Ces finalités du traitement doivent être clairement délimitées et permettre au responsable du traitement de choisir les activités de traitement les plus appropriées. En d'autres termes, la simple définition d'une finalité, pas plus que par exemple l'identification d'un intérêt important, n'implique pas automatiquement que le traitement de données biométriques envisagé soit légitime.

Ci-dessous, quelques exemples de finalités pour le traitement de données biométriques :

- Authentification de personnes pour des finalités de sécurité ;
- Authentification de personnes dans le cadre de paiements ou pour un accès à des appareils privés ou à des applications ;
- Enregistrement du temps dans un contexte professionnel ;
- Marketing direct[33] ;
- Screening (à l'aide d'un logiciel de reconnaissance faciale ou d'individualisation) de lieux publics dans le cadre de la prévention de la criminalité[34] ;
- Analyse ADN dans le secteur médical ;
- Analyse ADN commerciale dans le but d'établir le patrimoine ethnique et/ou la spécificité génétique d'une personne[35].

Une fois définies, les finalités doivent être inscrites avec précision dans le registre des activités de traitement (voir ci-dessus la rubrique II.1.2) ainsi que dans le document utilisé pour fournir les informations requises aux personnes concernées (la communication exacte des finalités du traitement est en effet essentielle pour pouvoir répondre à l'obligation de transparence conformément aux articles 13 et 14 du RGPD dont il ressort que les personnes concernées doivent être informées des finalités du traitement).

2.2 Finalité(s) ultérieure(s)

La deuxième obligation qui découle de l'article 5.1.b) du RGPD implique que les données à caractère personnel qui ont été collectées et traitées pour une finalité déterminée et explicite ne peuvent pas être traitées ultérieurement d'une manière incompatible avec cette finalité. Cela signifie que pour toute

[33] Le marketing direct proprement dit, en tant que finalité, est particulièrement large et doit incontestablement être spécifié dans chaque cas concret. Étant donné que cela ne relève toutefois pas du cadre de la présente recommandation, l'Autorité renvoie en la matière à la recommandation n° 01/2020 *relative aux traitements de données à caractère personnel à des fins de marketing direct* (consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf).
[34] Les traitements de données biométriques qui ont lieu dans ce cadre ne relèveront toutefois que rarement du champ d'application du RGPD étant donné qu'ils sont généralement réalisés par des services de police et/ou de renseignements.
[35] L'analyse ADN privée a évolué vers une industrie représentant des milliards. Malgré son interdiction en France (voir : https://www.statnews.com/2019/11/14/france-consumer-genetic-testing-ban/), l'on s'attelle actuellement au sein de l'Union européenne à élaborer un cadre éthique et des directives concernant l'utilisation de kits de test privés et la publicité de ceux-ci (projet SIENNA, voir : https://www.sienna-project.eu/).

nouvelle finalité qui n'est pas compatible avec la finalité initiale, une base juridique propre doit être identifiée.

En la matière, le considérant 50 du RGPD dispose ce qui suit : "*Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres : de tout lien entre ces finalités et les finalités du traitement ultérieur prévu ; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données ; la nature des données à caractère personnel ; les conséquences pour les personnes concernées du traitement ultérieur prévu ; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.*"

Cette analyse de la compatibilité doit être réalisée par le premier responsable du traitement, aussi bien pour ses activités de traitement que pour les activités de traitement visées par des tiers, responsables du traitement, auxquels le responsable du traitement initial a l'intention de transmettre les données. Une telle situation peut par exemple se présenter lorsqu'un employeur qui utilise un logiciel de reconnaissance faciale pour l'accès à ses locaux transmet les données biométriques traitées à cet effet au concepteur du logiciel en question qui les utilise à son tour pour améliorer ses technologies ou lorsque le fournisseur de tests ADN commerciaux utilise également les résultats des personnes concernées pour des recherches génétiques ou ethnographiques.

Vu les conditions particulièrement strictes qui s'appliquent à l'égard du traitement de données biométriques, il s'avérera toutefois très difficile dans la pratique de démontrer une telle compatibilité. Le traitement ultérieur de données biométriques devra donc presque toujours s'appuyer sur une base juridique spécifique propre.

Si le traitement ultérieur est quand même compatible avec la (les) finalité(s) initiale(s), l'article 13.3 du RGPD spécifie que : "*Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.*"

3. Proportionnalité

La proportionnalité, sans toutefois être mentionnée explicitement dans le texte du RGPD, est un des principes fondamentaux du droit (à la protection des données) européen. Le test obligatoire de

proportionnalité ressort indirectement de l'article 5.1.a) (loyauté) et c) (minimisation des données) du RGPD et implique la proportionnalité lors de la mise en balance des intérêts respectifs du responsable du traitement d'une part et des personnes concernées d'autre part. À cet effet, le responsable du traitement doit toujours se demander si les activités de traitement qu'il envisage sont (1) appropriées (la mesure est-elle pertinente pour la réalisation des finalités ?), (2) nécessaires (la mesure est-elle nécessaire pour la réalisation des finalités ?) et (3) non excessives (la mesure va-t-elle plus loin que ce qui est nécessaire à la réalisation des finalités ?).

Plus concrètement, le test obligatoire de proportionnalité s'inscrit dans le respect des obligations imposées par le RGPD. Ce n'est que lorsque le responsable du traitement peut efficacement démontrer que tous les principes de la protection des données ont été respectés que l'on peut parler d'un traitement de données licite et donc proportionné. Pensons par exemple à l'identification d'une base juridique appropriée, à la définition claire des finalités, à la garantie que seules les données nécessaires à ces finalités sont traitées, au choix des activités de traitement spécifiques, au respect de l'obligation de transparence, au fait de veiller à ce que les données ne soient pas traitées et conservées plus longtemps que le temps nécessaire, à la garantie de l'intégrité du traitement de données, au respect des principes de '*privacy by design*' et '*privacy by default*', …

En ce qui concerne en particulier le traitement de données biométriques, la notion de proportionnalité joue un rôle important. En effet, conformément à l'article 5.1.c) du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Le traitement de données à caractère personnel ne peut donc avoir lieu que dans la mesure où les finalités du traitement ne peuvent raisonnablement pas être atteintes d'une autre manière. Dans le contexte du traitement de données biométriques, cela signifie que même si une base juridique a été identifiée et que les finalités ont été clairement définies, le traitement ne peut pas avoir lieu sans condition. Il faut en effet vérifier s'il n'existe pas de solutions moins radicales (le traitement de données biométriques sera toujours la dernière solution).

Exemple

En août 2019, l'école gantoise Saint-Bavon a annoncé que les élèves et les membres du personnel pourraient, dans un avenir proche, effectuer divers paiements (cafétéria, photocopieuses, ...) avec un scan de leur paume. Pour ce faire, l'école s'appuyait sur le consentement explicite des parents et des élèves et visait la suppression des justificatifs de repas en version papier et de l'argent liquide (afin d'éviter que les enfants doivent circuler avec trop d'argent sur eux). Ceux qui refuseraient pourraient utiliser les méthodes de paiement alternatives. Toutefois, à la suite d'un avis négatif, l'idée a été abandonnée étant donné qu'il existait un déséquilibre manifeste entre le traitement risqué de données biométriques et le paiement de petits montants dans un contexte scolaire. En l'occurrence, on peut estimer que bien que la mesure soit appropriée pour atteindre les finalités visées, il n'a pas

été suffisamment démontré qu'elle était effectivement nécessaire et qu'il n'existait pas de solution moins radicale[36].

Si le responsable du traitement peut démontrer que le traitement de données biométriques constitue le moyen le plus approprié pour garantir la sécurité, il devra également documenter et justifier l'utilisation d'une caractéristique biométrique déterminée. En ce qui concerne en particulier l'authentification biométrique de personnes, l'Autorité souligne que le responsable du traitement doit se limiter à l'authentification sur la base de caractéristiques morphologiques des personnes concernées (par exemple la reconnaissance faciale, le scan de la paume ou de l'empreinte digitale, la reconnaissance de l'iris), en tenant compte toutefois du fait que l'utilisation de caractéristiques morphologiques qui ne laissent pas de trace (par exemple la reconnaissance faciale ou de l'iris) comporte moins de risques que l'utilisation par exemple de scans de l'empreinte digitale ou de la paume. Quant au traitement d'échantillons biologiques (par exemple salive, urine ou sang), ce seront toujours les conditions les plus strictes qui seront d'application[37].

Le mode d'enregistrement du gabarit biométrique dans le cadre de l'authentification de personnes (voir ci-dessus la rubrique II.2.3) joue également un rôle important dans le cadre du test de proportionnalité. En effet, comme cela a déjà été expliqué ci-dessus, l'enregistrement de gabarits sous maîtrise partagée ou sous maîtrise exclusive du responsable du traitement n'est possible que dans des cas exceptionnels. L'enregistrement du gabarit sous maîtrise exclusive de la personne concernée (par exemple : dans un token ou un badge) reste d'application en tant que règle de principe.

Enfin, si l'authentification doit absolument être réalisée à l'aide d'un système biométrique, l'utilisation de celui-ci doit toujours se limiter aux espaces/services qui justifient de telles mesures particulières. En ce qui concerne par exemple le contrôle d'accès, un site peut comprendre plusieurs espaces qui sont librement accessibles et d'autres espaces qui justifient l'utilisation de la biométrie. L'accès à l'aide de systèmes biométriques doit, en tant que tel, être limité à ces espaces et les données biométriques traitées doivent rester limitées aux personnes autorisées à pénétrer dans ces espaces. En outre, afin de limiter l'accès à un espace à un certain groupe d'individus, il n'est pas toujours nécessaire de traiter des données permettant une identification directe (comme le nom) des personnes qui disposent d'un droit d'accès. Par conséquent, tant qu'une personne dispose d'un droit d'accès et que la biométrie permet de contrôler cet aspect, il est inutile d'associer les informations biométriques à des moyens d'identification supplémentaires.

[36] Voir notamment : https://tweakers.net/nieuws/156660/belgische-school-laat-leerlingen-hun-lunch-afrekenen-met-scan-van-handpalm.html et https://www.nieuwsblad.be/cnt/dmf20190911_04603325.
[37] Le traitement d'échantillons biologiques a lieu principalement dans le secteur médical ou dans le cadre de tests ADN commerciaux.

4. Sécurité du traitement

Conformément à l'article 5.1.f) *juncto* l'article 32 du RGPD, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. De telles mesures peuvent notamment comprendre des :

a. Mesures relatives aux données biométriques[38] :

- crypter les données biométriques, y compris les gabarits, à l'aide d'un algorithme cryptographique conformément à l'état des connaissances ;
- associer un code d'intégrité aux données biométriques (par exemple avec une signature électronique) ;
- intégrer des mesures de détection de fraude ;
- interdire l'accès externe aux données biométriques ;
- veiller à ce que la copie des données collectées au cours de la phase de collecte ne soit pas conservée plus longtemps que le temps nécessaire à la comparaison des données collectées avec les informations de référence ;
- mettre en œuvre un système efficace pour la suppression et la destruction des données biométriques après échéance du délai de conservation ;

b. Mesures organisationnelles :

- délimiter clairement et former les personnes au sein d'une entreprise qui ont accès aux systèmes/données biométriques ;
- responsabiliser les personnes concernées quant à l'utilisation et à l'application de systèmes biométriques ;
- mettre gratuitement à disposition des procédures d'authentification alternatives pour les personnes pour lesquelles l'enregistrement ou la lecture des données biométriques est impossible ou sérieusement compliqué(e) en raison d'un handicap ou d'une autre circonstance ;
- tester la sécurité, la fiabilité et la résilience du système avant la mise en œuvre et après toute modification ;
- définir un système de sauvegarde et des procédures de récupération en cas de défaillance du système ;
- définir une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises pour assurer la sécurité du traitement ;

[38] Concernant l'authentification biométrique de personnes, il a déjà été spécifié en ce sens qu'actuellement, on ne pourra pas justifier de travailler avec un système dans lequel les informations de référence sont enregistrées sous leur forme brute (obligation de travailler avec des gabarits biométriques) et qu'il faut préférer la fonction de vérification à celle d'identification, étant donné qu'avec cette dernière, il sera toujours nécessaire d'enregistrer les informations de référence dans une base de données centrale (voir ci-dessus la rubrique II.2.3).

c. Mesures concernant le dispositif et le logiciel :

- tenir à jour les systèmes biométriques afin de les protéger contre un accès non autorisé et/ou de réduire les faux résultats négatifs/positifs (cela implique également qu'il relève de la responsabilité du responsable du traitement de vérifier que les modifications apportées par le concepteur du dispositif ou du logiciel ne compromettent pas la sécurité du système) ;
- prévoir une procédure d'avertissement ou la suppression automatique des données si le système constate un accès non autorisé (ou une tentative d'accès non autorisé) ;
- veiller à ce que les données biométriques soient enregistrées séparément et à ce que l'environnement d'exécution de l'application biométrique soit séparé des autres réseaux.

Dans ce cadre, il faut également faire référence à l'article 25 du RGPD concernant la protection des données dès la conception (`*privacy by design*') et la protection des données par défaut (`*privacy by default*').

Privacy by design signifie concrètement que les principes en matière de protection des données conformément à l'article 5 du RGPD sont déjà intégrés dans le processus de traitement de données avant le début des activités de traitement[39]. En d'autres termes, *Privacy by design* doit être compris comme étant l'approche par laquelle ces principes essentiels sont appliqués en tant que principes de conception fondamentaux tout au long du processus de conception du système de manière à réduire au maximum les risques pour les personnes concernées, dès le début. Ainsi, il convient d'inciter les fabricants de systèmes biométriques à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels systèmes et, compte tenu de l'état des connaissances, à s'assurer que les responsables du traitement sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données[40].

Privacy by default implique que le responsable du traitement mette en œuvre les mesures techniques et organisationnelles appropriées pour garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées. Cette obligation s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité et vise à empêcher le traitement illicite, imprévu ou injustifié de données.

[39] Le Contrôleur européen de la protection des données (souvent désigné par l'abréviation anglaise "EDPS") définit la `*privacy by design*' comme suit : "*Le concept de respect de la vie privée et de protection des données dès la conception a pour but d'intégrer le respect de la vie privée et la protection des données dans les spécifications de conception et l'architecture des systèmes et des technologies d'information et de communication.*" Voir l'avis n° 7/2015 de l'EDPS "Relever les défis des données massives", p. 17 (consultable via le lien suivant : https://edps.europa.eu/sites/default/files/publication/15-11-19_big_data_fr.pdf).
[40] Voir le considérant 78 du RGPD.

Dans ce contexte, il est indispensable que le responsable du traitement suive attentivement les évolutions technologiques en la matière afin d'adapter les mesures de sécurité à ces évolutions. L'Autorité veut dès lors attirer l'attention sur le fait qu'en vertu de l'article 5.2 du RGPD, le responsable du traitement est responsable et donc peut être tenu pour responsable des dommages qui seraient dus au non-respect des mesures de sécurité[41].

5. Limitation de la conservation

Conformément à l'article 5.1.e) du RGPD, "*les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées*". Concrètement, cela signifie qu'une fois que la finalité du traitement a été réalisée, ou lorsque la base juridique n'est plus valable (par exemple en raison du retrait du consentement par les personnes concernées ou de la disparition de l'intérêt public important), les données biométriques en question doivent être supprimées[42]. Toutefois, cela n'exclut pas que les données soient conservées plus longtemps en vertu d'une obligation légale ou lorsque ces données sont nécessaires dans le cadre d'une procédure judiciaire.

Lorsque le traitement de données biométriques a lieu en vertu d'une obligation légale dans le chef du responsable du traitement, le délai de conservation repris dans la loi doit être respecté.

Concernant l'authentification biométrique, comme déjà expliqué ci-dessus dans la rubrique II.2.3, l'Autorité souhaite préciser que les données biométriques brutes collectées dans le cadre de la première phase de collecte d'un système biométrique (phase d'enregistrement) doivent immédiatement être supprimées dès que le gabarit biométrique a été créé. En outre, les données collectées lors de la deuxième phase de collecte ne peuvent pas être conservées plus longtemps que le temps nécessaire pour comparer les données collectées avec les informations de référence.

6. Obligation de transparence[43]

Le considérant 38 du RGPD dispose que : "*Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant*

[41] Voir le considérant 74 du RGPD.
[42] Ainsi, par exemple, les données utilisées pour gérer l'accès à un lieu de travail doivent être supprimées dès que l'utilisateur perd son droit d'accès à cet espace.
[43] Pour un exposé général concernant le principe de transparence, voir le Groupe 29, Lignes directrices *sur la transparence au sens du règlement (UE) 2016/679.* À télécharger via le lien suivant : https://ec.europa.eu/newsroom/article29/items/622227/en.

à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement. Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement. En particulier, les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées lors de la collecte des données à caractère personnel."[44].

Les principaux articles du RGPD qui concernent la transparence, car s'appliquant aux droits des personnes concernées, figurent dans le Chapitre III (Droits de la personne concernée). L'article 12 du RGPD contient les prescriptions générales qui s'appliquent à : la communication d'informations aux personnes concernées (articles 13 - 14 du RGPD), la communication avec les personnes concernées au sujet de l'exercice de leurs droits (articles 15 - 22 du RGPD) et la communication concernant les violations de données à caractère personnel (article 34 du RGPD).

Il va de soi qu'en ce qui concerne le traitement de données à caractère personnel, les obligations en matière de transparence doivent être scrupuleusement respectées.

7. Analyse d'impact relative à la protection des données

Conformément à l'article 35.1 du RGPD, le responsable du traitement devra effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsque le traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

L'article 35.4 du RGPD dispose complémentairement que chaque autorité de contrôle est tenue d'établir et de publier une liste des activités de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise. Dans l'attente de la création de l'Autorité, la Commission de la protection de la vie privée a adopté la recommandation n° 01/2018 sur les modalités d'exécution d'une analyse d'impact relative à la protection des données, en tenant compte des dispositions de l'article 35 du RGPD et des lignes directrices du Groupe 29. Cette recommandation a ensuite été complétée par la décision n° 01/2019[45] du Secrétariat Général de l'Autorité qui comprend une liste des activités de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

[44] Considérant 38 du RGPD.
[45] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf.

Comme il ressort du point 6 de la décision n° 01/2019, il faudra toujours réaliser une analyse d'impact relative à la protection des données lorsque le traitement utilise des données biométriques en vue de l'identification unique des personnes concernées se trouvant dans un lieu public ou dans un lieu privé accessible au public. L'Autorité souhaite toutefois souligner que le traitement de données biométriques pour d'autres finalités que celles reprises explicitement dans la décision est également soumis à l'obligation de réaliser une analyse d'impact relative à la protection des données. Qui plus est, vu le risque inhérent élevé pour les droits et libertés des personnes concernées qu'implique le traitement de données biométriques, ne pas réaliser une analyse d'impact relative à la protection des données ne sera justifié que dans des cas exceptionnels.

En la matière, en ce qui concerne les modalités de l'exécution d'une analyse d'impact relative à la protection des données, l'Autorité renvoie à la recommandation n° 01/2018[46], à la décision n° 01/2019 et au Guide AIPD[47].

[46] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf.
[47] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf.