Votre carte d'identité comme carte de fidélité RGPD

Nathanaël Pascal, le 19 mai 2025

L'autorité de protection des données belge s'est intéressée au recours à la carte d'identité nationale électronique en tant que substitut à la carte de fidélité. Dans ce cadre, le recueil d'un consentement valide, la garantie de la transparence des traitements de données ainsi que le respect des principes de minimisation et de responsabilité revêtent une importance cardinale.

Autorité belge de protection des données, décision de la Chambre contentieuse 146/2024 du 28 novembre 2024

À la suite de la publication d'un article portant sur la mutualisation de la gestion des données de consommateurs dans un journal belge, l'autorité de protection des données de Belgique (ci-après : APD) a ouvert un dossier contre la société mentionnée dans l'article en question (ci-après : la Société). Cette société propose une technologie visant à simplifier la collecte et la mise à jour de données personnelles en utilisant notamment des données contenues dans la puce de la carte d'identité électronique belge (ci-après : eID). Les services que proposent la Société permettent de centraliser des avantages commerciaux offerts par différentes enseignes aux consommateurs, ainsi que les cartes de fidélité ou preuves d'achat de ces derniers.

I. De la collecte à la mutualisation des données personnelles : un cas de responsabilité conjointe

L'APD débute son analyse en qualifiant la collecte des données personnelles (art. 4 par. 2 RGPD). Ces dernières sont directement fournies par les consommateurs par divers moyens, dont la lecture de leur eID ou manuellement sur une borne dédiée, sur le site Internet d'un partenaire commercial, mais également par la Société via sa plateforme ou son application.

Cette collecte a pour finalité d'alimenter un fichier mutualisé détenu par la Société. Ce traitement de données de données personnelles est inextricablement lié à la mutualisation de ces dernières. En effet, les partenaires commerciaux qui ont préalablement une relation commerciale avec le consommateur peuvent accéder aux données mises à jour par le biais de cette mutualisation. En d'autres termes, si le partenaire commercial A détient des données plus

récentes sur un consommateur qui a également une relation commerciale avec le partenaire commercial B, ces données à jour seront transférées à ce dernier.

Forte de ce constat, l'APD retient une responsabilité conjointe au sens de l'art. 26 RGPD de la Société et de ses partenaires commerciaux pour la collecte et la mutualisation des données d'identité. Pour arriver à une telle qualification, l'APD se fonde sur les lignes directrices du CEPD concernant les notions de responsable du traitement et de sous-traitant qui rappellent que la participation conjointe englobe tant la détermination des finalités que la détermination des moyens. Ces lignes directrices précisent qu'une telle participation peut être retenue en présence d'une infrastructure créée par l'une des parties en vue de son utilisation par d'autres parties, permettant ainsi aux parties de traiter les mêmes données personnelles.

En l'espèce, les données personnelles sont collectées par le biais de dispositifs fournis par la Société et proposés, notamment sous la forme de bornes, par ses partenaires commerciaux. Ces données font l'objet d'une centralisation dans une infrastructure technique développée, soit le fichier, par la Société, leur mutualisation étant le fruit des contributions continues des consommateurs. De la sorte, la mutualisation réalisée par la Société n'est possible que grâce à la collaboration de ses partenaires commerciaux. En outre, l'infrastructure technique préalablement configurée par la Société et intégrée dans l'environnement de ses partenaires commerciaux démontre une convergence des moyens du traitement et des finalités mis en œuvre pour le réaliser.

Par conséquent, l'APD retient que la finalité poursuivie – tant par la collecte que par la mutualisation des données personnelles – est l'alimentation du fichier mutualisé. En effet, cette finalité est cardinale pour l'enrichissement dudit fichier, et ce, en vue d'attirer de nouveaux partenaires commerciaux désireux d'obtenir une identification fiable et à jour de leurs consommateurs.

Enfin, et à l'appui de la jurisprudence de la CJUE (C-210/16 du 5 juin 2018), l'APD met en exergue le fait que les traitements intervenant subséquemment ne remet pas en cause la qualification de responsable conjoint du traitement.

II. Des manquements ayant trait au consentement

La loi belge du 19 juillet 1991 relative aux registres de la population aux cartes d'identité, aux cartes des étrangers et aux documents de séjour conditionne la lecture ou l'utilisation de l'eID au consentement libre, spécifique et éclairé de son titulaire (art. 6 §4). L'APD indique que le recours au consentement, tel que prévu à l'art. 6 par. 1 let. a RGPD, est donc la base

juridique appropriée pour les traitements concernés. L'autorité retient que, quand bien même les lignes directrices du CEPD relatives au consentement ont été adoptées postérieurement à l'enquête dirigée contre la Société, ces dernières lui sont opposables selon l'APD car elles reprennent en substances celles adoptées par le Groupe de travail « article 29 » en 2017. Dès lors, il convient d'analyser si le consentement des consommateurs est libre, spécifique, éclairée et univoque (art. 4 par. 11 RGPD).

L'APD constate que, indépendamment du mécanisme de recueil du consentement concerné, les consommateurs sont tenus d'accepter les conditions générales de la Société pour bénéficier des avantages commerciaux offerts par les partenaires commerciaux de cette dernière. En procédant de la sorte, les consommateurs voient l'obtention desdits avantages conditionnée au traitement de leurs données personnelles. Partant, l'APD réfute le caractère libre du consentement recueilli.

Pour ce qui est du caractère spécifique de ce dernier, il apparait que sur le site internet de la Société, la demande de consentement est globale et n'opère pas de distinction entre le consentement portant sur la création d'un compte et celui portant sur l'utilisation ultérieure de ces données en vue d'alimenter le fichier mutualisé. L'absence de caractère spécifique des demandes de consentement se retrouve également dans celles formulées par les partenaires commerciaux de la Société.

Les lignes directrices du CEPD relatives au consentement indiquent que pour qu'un consentement puisse être considéré comme éclairé, notamment lorsqu'il constitue la base juridique du traitement à divers responsables conjoints du traitement ou lorsque les données doivent être traitées par d'autres responsables souhaitant se fonder sur le consentement original, l'ensemble de ces organisations doivent être nommées. Or, l'APD constate que les personnes concernées sont renvoyées vers la charte « vie privée » de la Société où il est fait mention des catégories de destinataires en l'absence de toute nomination individuelle, ce qui est selon elle insuffisant et constitue une obligation distincte qui découle de l'obligation de transparence (art. 13 et 14 RGPD). En conséquence, l'APD réfute le caractère éclairé du consentement recueilli.

Afin que le consentement exclût toute ambiguïté, l'action par laquelle la personne concernée consent doit se distinguer de manière nette des autres actions possibles. L'APD constate que la simple navigation d'une page à l'autre, quand bien même en présence d'une option de retour, n'équivaut pas à une expression claire de consentement.

Par conséquent, la Société n'a pas obtenu de consentement valable auprès des personnes

concernées.

En outre, et à teneur de l'art. 7 par. 3 RGPD, la personne concernée a le droit de retirer son consentement à tout moment et il doit être aussi simple de le retirer que de le donner. L'APD constate que les options offertes par la Société ne remplissent pas l'exigence de simplicité évoquée en raison de la nécessité pour les personnes concernées de naviguer dans de multiples onglets ou interfaces. Cela est agrémenté par l'absence d'une option de retrait explicite et immédiate. De tels éléments sont considérés comme porteurs du risque de décourager les personnes concernées de procéder au retrait de leur consentement.

De plus, l'APD met en exergue le lien entre cette obligation et celle de protection des données par défaut (art. 25 RGPD), obligation qui aurait dû conduire la Société à prévoir des mécanismes de retrait du consentement directement sur les bornes mises en place par ses partenaires commerciaux, et ce, avant même la mise en place du traitement.

En outre, le considérant 42 du RGPD fait écho à son art. 5 par. 2 en indiquant que lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement doit être en mesure de démontrer que ladite personne a consenti au traitement concerné. L'APD retient à cet égard que des mesures contractuelles telles que l'obligation supportée par les partenaires commerciaux de la Société d'indemniser cette dernière en cas de collecte de consentement non-valable, ainsi que la présence d'un registre reprenant bonnement et simplement des informations quant à la présence d'un mécanisme de consentement sont insuffisants.

Vu les faits de l'espèce, l'APD a tranché que la Société n'a pas mis en place les mesures nécessaires lui permettant de démontrer que le consentement collecté est conforme au RGPD et n'a pas respecté ses exigences de documentation et de responsabilité en matière de retrait de consentement.

III. De la minimisation et de la protection par défaut des données personnelles

Invoquant une mise en balance du principe de minimisation (art. 5 par. 1 let. c RGPD) et de celui d'exactitude (art. 5 par. 1 let. d RGPD), la Société indique que le volume important de données collectées est justifié par le fait qu'elle doit rapidement limiter le risque de confusion entre les consommateurs, éviter les doublons et identifier d'éventuelles fraudes. L'APD balaie cette position en se prévalant notamment de la recommandation 03/2011 émise par la Commission de la Protection de la Vie Privée (CPVP). Cette dernière indique que dans le cadre du recours à l'eID à titre de carte de fidélité, il n'est pas possible, et ce indépendam-

ment des circonstances, de traiter les éléments suivants qui figurent sur l'eID : la photo du titulaire, le numéro de la carte, le numéro d'identification au Registre national, la nationalité et le lieu de naissance. Or la Société collecte certaines de ces données, lesquelles ne revêtent aucune pertinence eu égard au traitement concerné, comme peut en attester l'absence de collecte de telles informations dans le formulaire de collecte manuel. L'APD soulève le fait que – plus le nombre de données personnelles collectées est important – plus il est difficile de respecter concomitamment les principes d'exactitude et de minimisation. L'autorité belge précise en l'espèce que le risque d'avoir des données obsolètes ne justifie pas la collecte d'une dizaine d'informations supplémentaires et facultatives.

Au surplus, l'APD estime qu'une centralisation massive de données d'une grande partie de la population et de leurs données collectées directement sur leur eID, comme en l'espèce, constitue un risque élevé pour la vie privée de millions de consommateurs.

De ce fait, la Société a manqué aux principes de minimisation et de protection des données par défaut.

IV. De la durée de conservation

Les données personnelles doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (art. 5 par. 1 let. e RGPD). La Société se prévaut d'un intérêt économique légitime, de considérations tant comptables que fiscales, ainsi que de la garantie légale des biens de consommation de deux ans (art. 1649*quater* du Code civil belge), laquelle peut faire l'objet d'une prolongation, de sorte à fixer une durée de conservation des données dans le cadre du fichier mutualisé de huit ans dès la dernière activité de la personne concernée. Or, l'APD constate que les arguments de la Société s'appliquent principalement à d'autres finalités que celle relative à la gestion du fichier mutualisé, dites finalités qui concernent surtout les relations entre le consommateur et ses partenaires commerciaux. Ainsi, la Société ne peut se fonder sur ces prescriptions et l'APD estime qu'une durée de conservation d'un maximum de trois ans à compter de la dernière activité du consommateur est suffisante.

Par conséquent, l'APD retient une violation du principe de limitation de la conservation des données personnelles en raison de la durée excessive de conservation de huit ans pour le fichier mutualisé par la Société.

L'APD impose une série de mesures correctrices à la Société et somme cette dernière de se mettre en conformité dans un délai de quatre mois sous peine d'astreintes pouvant atteindre

EUR 5’000.-/jour.

V. Conclusion

Cette décision met en lumière les exigences rigoureuses pesant sur les responsables conjoints du traitement en matière de licéité, de transparence, de minimisation, de protection par défaut et de limitation de la conservation des données à caractère personnel. La Société, en s’appuyant sur une infrastructure technique mutualisée et en centralisant les données issues des eIDs de manière systématique, a méconnu ces obligations et principes fondamentaux du RGPD.

Il importe, en particulier, de souligner que la validité du consentement suppose une dissociation claire et intelligible des différentes finalités du traitement, de sorte que la personne concernée soit en mesure d’exercer un choix libre et éclairé à chacune des étapes de la collecte.

Finalement, l’approche adoptée par l’APD quant à la durée de conservation, laquelle s’aligne sur celle découlant du référentiel relatif à la gestion des activités commerciales de l’autorité de protection des données française, peut être le témoignage d’une volonté d’harmonisation dans la mise en œuvre du RGPD.

Proposition de citation : Nathanaël PASCAL, Votre carte d’identité comme carte de fidélité RGPD, 19 mai 2025 *in* www.swissprivacy.law/353

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.