La prise en compte effective du traitement des données personnelles dans les nouveaux CCAG

Dans les CCAG de 2009, la problématique des données personnelles était abordée de manière lapidaire. L'émergence du RGPD nécessitait de modifier les CCAG sur ce point. La nouvelle rédaction des CCAG approfondit tant la responsabilité des différents intervenants que les critères et fondements des opérations de traitement des données personnelles.

La réforme issue du Règlement européen 2016/679 sur la protection des données personnelles (aussi appelé RGPD), a fortement accru la responsabilité des organismes tant privés que publics. Au regard de la multitude des données personnelles susceptibles d'être traitées par les organismes publics dans le cadre de leurs marchés publics, il était fort à parier que les exigences allaient considérablement s'accroître. Ces derniers sont désormais pleinement responsables de la protection des données qu'ils recueillent et traitent.

L'évolution récente du cadre réglementaire

En France, la protection des données personnelles est une problématique relativement « ancienne ». En effet, sur le territoire national, le traitement automatisé des données personnelles est encadrée par la loi n° 78/17 du 6 janvier 1978 dite « Informatique et Libertés ».

Mais nul n'ignore que c'est par la voie communautaire que la protection des données personnelles a acquis une nouvelle notoriété et par là même, un encadrement plus strict et contemporain. Le règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, entré en application le 25 mai 2018, relatif à la protection des données à caractère personnel et à la libre circulation de ces données, plus connu sous le désormais célèbre acronyme « RGPD » a profondément bouleversé les règles relatives à la donnée personnelle.

L'émergence du RGPD n'a toutefois pas enterré la loi Informatique et Liberté, bien au contraire.

Depuis le 1er juin 2019, cette dernière est en vigueur dans une nouvelle rédaction issue de la loi n° 2018-493 du 20 juin 2018, intégrant notamment la plupart des notions issues du RGPD.

Auteurs

François Jouanneau
Avocat, Directeur du Département Droit public
Benjamin Brami
Avocat, collaborateur du Département Droit public
Lexing Alain Bensoussan Avocats

Toutefois, cette dernière n'a pas pour objet de reprendre stricto-sensu le RGPD même si elle y renvoie expressément. Partant, une bonne lecture de la réglementation sur le traitement des données personnelles, et toutes ses problématiques connexes, suppose la bonne compréhension de ces deux textes combinés.

C'est dans ce cadre que la problématique du traitement des données personnelles lors de la passation et l'exécution des contrats de la commande publique doit être appréhendée et notamment au travers des termes des ci-après CCAG déclinés pour chaque type de marché.

Mais pour comprendre comment les CCAG abordent la problématique des données personnelles, il convient de s'attarder sur la définition d'une donnée personnelle.

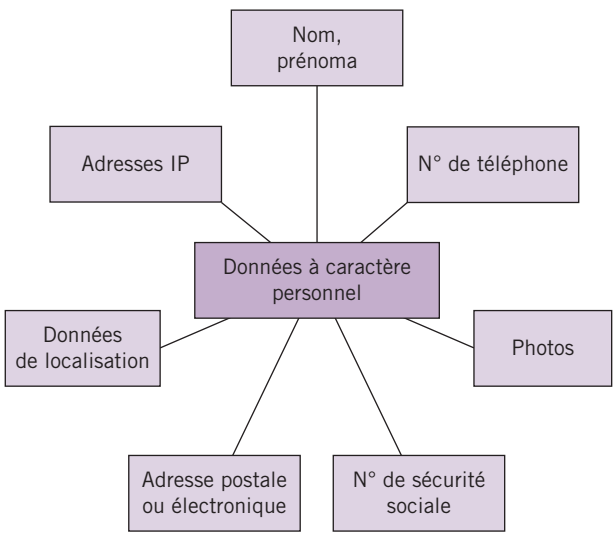
Une identification concrète des données personnelles

Il conviendra, à chaque acheteur de se référer à la définition de données personnelles pour apprécier de manière concrète les exigences tant des lois et règlements que des prescriptions des nouveaux CCAG.

L'article 4.1 du RGPD donne une définition théorique d'une donnée à caractère personnelle :

« Toute information se rapportant à une personne physique identifiée ou identifiable ».

De manière concrète, les données à caractère personnel, visent toutes informations relatives à une personne physique pouvant être identifiée directement ou indirectement. Ainsi à titre d'exemple, constituent des données à caractère personnel les éléments suivants :



Données à caractère personnel

Il faut toutefois savoir qu'au sein même de la grande famille des données personnelles, certaines se distinguent par leur degré d'intimité, les données personnelles particulières. Il s'agit précisément des données faisant apparaître de façon directe ou indirecte :
– les origines raciales ou ethniques ;
– les opinions politiques, philosophiques ou religieuses ;
– l'appartenance syndicale des personnes ;
– les données génétiques ou biométriques ;
– les données relatives à la santé ;
– les données concernant la vie sexuelles ou l'orientation sexuelle.

Si la définition des données personnelles est assez naturelle, tel n'est pas le cas du terme « traitement ».

A cet effet, l'article 4.2 du RGPD définit le traitement comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

De manière plus factuelle, dès lors qu'un opérateur est amené à appréhender des données personnelles, il réalise un traitement.

L'insuffisance du traitement des données personnelles dans les CCAG actuels

Dans la mise en œuvre du RGPD, on assiste à un réel positionnement des pouvoirs publics sur ses liens avec la commande publique.

Cette logique de responsabilisation vise à impliquer tous les acteurs de la commande publique et ce, depuis la phase de passation du marché jusqu'à son exécution.

Pourtant, alors qu'ils sont centraux dans le cadre de la passation des contrats administratifs, les CCAG n'étaient que peu imprégnés de cette problématique.

Dans les « anciens » CCAG (2009), la problématique des données personnelles est appréhendée au travers d'un seul article, l'article 5.2 « Confidentialité et mesures de sécurité ». À noter que l'article 5.2.3 relatif à la déclaration et aux autorisations administratives était devenu obsolète puisque cette obligation de déclaration n'est plus obligatoire depuis le 25 mai 2018 (date d'entrée en application du RGPD).

Pour combler cette carence, la Direction des affaires Juridiques avait publié le 25 octobre 2018, une fiche destinée à accompagner les acheteurs dans le cadre de l'impact du RGPD sur le droit de la commande publique.

À cet effet, la fiche DAJ du 25 octobre 2018 présente les essentiels du RGPD appliqué à l'exécution des marchés publics.

La fiche DAJ propose une traduction des terminologies du RGPD en vocable des marchés publics.

Dans ce contexte :
– le responsable du traitement issu de l'article 4.7 du RGPD correspondant à l'acheteur au sens de l'ordon-

nance n° 2015-899 du 23 juillet 2015 relative au droit des marchés publics[1] ;
– le « sous-traitant » issu de l'article 4.8 du RGPD correspondant au titulaire du marché public ;
– le « sous-traitant du sous-traitant » issu de l'article 28.2 du RGPD correspond au sous-traitant au sens du droit de la commande publique ;
– « L'autorité de contrôle » issue de l'article 4.21 du RGPD correspond à la Commission nationale de l'informatique et des libertés (CNIL).

Toutefois, malgré les apports de la fiche de la DAJ, notamment sur la prise en compte temporelle du RGPD dans les marchés, aucun cadre réglementaire précis ne concernait les exigences en matière de données personnelles de sorte qu'à défaut d'impératif, les acheteurs pouvaient ne pas modifier ni leurs marchés en cours, ni leurs futurs marchés.

Cette position présentait des avantages et des inconvénients. Tout d'abord cela permettait aux acheteurs de ne pas modifier des cadres contractuels bien établis et par là même éviter des considérations superflues dans des marchés non concernés par le traitement de données personnelles. Pour autant, cette démarche comportait un risque, celui de la difficulté de recherche de responsabilité en cas de faille dans le traitement des données personnelles.

La contractualisation du RGPD impliquait dès lors des difficultés tant pour les marchés à venir que pour les marchés en cours.

Concernant les marchés à venir, il était préconisé, même en l'absence de précision dans les CCAG, de prévoir des clauses spécifiques au traitement des données personnelles, fondées notamment sur les exigences appliquées dans les contrats privés. Ces clauses reprenaient globalement les attentes et les obligations qui pesaient sur les acheteurs et les titulaires des marchés publics.

S'agissant des marchés déjà passés, la fiche de la DAJ préconisait la conclusion d'un avenant actualisant la rédaction des contrats pour y inclure les exigences en matière de traitement des données personnelles issues du cadre réglementaire présenté ci-avant.

Face à de telles difficultés, il était fondamental que la nouvelle rédaction des CCAG tienne compte des exigences en matière de données personnelles et fixe un cadre tant en matière d'attentes et de niveau d'exigence, que du régime de responsabilité applicable à l'acheteur et au titulaire (voire même ses sous-traitants).

Les principes du RGPD adaptés dans les nouveaux CCAG et consacrés à l'article 5.2

La nouvelle rédaction des CCAG s'imprègne beaucoup plus de la problématique des données personnelles en en précisant largement les contours et les caractéristiques. À cet effet, la réécriture de l'article 5 des différents CCAG approfondit tant la responsabilité des différents intervenants que les critères et fondements des opérations de traitement des données personnelles.

Partant, l'article 5.2.1 concerne la problématique du transfert des données personnelles, notamment des transferts en dehors de l'Union Européenne. En plus de consacrer textuellement le respect des règles européennes et nationale (en l'occurrence le RGPD et la loi de 1978), cet article prohibe formellement le transfert de données en dehors de l'Union Européenne dont le niveau de protection ne serait pas à minima égale au niveau de protection européen.

En tout état de cause, c'est l'article 5.2.3 (qui remplace l'ancien article 5.2.3 devenu obsolète) qui développe de manière plus fonctionnelle et concrète le traitement des données personnelles.

À cet effet, il reprend les principes directeurs du RGPD et du traitement des données personnelles.

Le premier principe directeur consacré par cette nouvelle rédaction est le principe de finalité.

Le principe de finalité coïncide avec la raison pour laquelle la donnée est traitée, autrement dit le but poursuivi par le traitement. Les données personnelles doivent ainsi être traitées pour des finalités déterminées et explicites, et ne doivent pas être utilisées de manière incompatible avec ces finalités.

La finalité doit être déterminée, explicite, légitime et licite[2]. De plus, elle doit être portée à la connaissance des personnes concernées et inscrite au registre des traitements[3].

Plus précisément le caractère déterminé de la finalité renvoie à son expression formalisée par le responsable de traitement (dans les marchés publics, par l'acheteur).

Le caractère explicite renvoie au niveau de précision des fins poursuivies par le traitement afin d'éviter les finalités générale ou floues (amélioration d'expérience des clients…).

Le caractère légitime relève quant à lui d'un jugement sur les fins associées au traitement de la donnée.

Enfin, la licéité de la finalité implique de vérifier que l'objectif poursuivi n'est pas contraire à la loi.

(1) CCP, art. L. 1210-1 et s.

(2) Loi n° 78-17 du 6 janvier 1978, art. 4-1.
(3) RGPD, art. 30 (1) b).

En sus du principe de finalité et de ses différents composants, s'ajoutent également d'autres principes fondamentaux.

Parmi ceux-ci, on retrouve le principe de minimisation issu de l'article 5 paragraphe 1(c) du RGPD et de l'article 6 de la loi informatique et libertés. Il en résulte que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement. Les données doivent être minimisées dans l'ampleur de leur collecte mais également dans leur nature même afin d'une part de ne collecter et traiter uniquement ce qui est essentiel et d'autre part limiter les risques.

Ce principe est un corollaire du principe de proportionnalité résultant de l'article 4 de la loi Informatique et Libertés qui implique que les données traitées soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Cet article 5.2.3 qui, comme il aura été compris, est le pilier de la nouvelle rédaction des CCAG en termes de données personnelles, relève également la notion de description et de durée du traitement dont la réalisation est confiée au titulaire dans le strict respect des instructions documentées par le maître d'ouvrage (donc l'acheteur).

Par ceci, il faut comprendre que le titulaire, le sous-traitant au sens du RGPD, ne peut traiter les données que dans le cadre extrêmement circonscrit des indications données par la maître d'ouvrage que ce soit en terme de description des données personnelles qu'en ce qui concerne la durée du traitement. La responsabilité des traitements portant sur l'acheteur en tant que responsable de traitement, il paraît en effet absolument nécessaire de ne laisser aucune marge de manœuvre au titulaire dans le cadre du traitement des données collectées.

La résultante de l'ensemble de ces principes est également la prise en compte, par l'acheteur et le titulaire des droits des personnes concernés. Les personnes concernées sont naturellement les personnes dont les données personnelles sont collectées.

En application du principe de transparence, les personnes concernées ont le droit de connaître, au moment où leurs données à caractère personnel sont obtenues, la durée de conservation des données – qui comme il sera explicité ultérieurement est fondamental – ou a minima les critères utilisés pour déterminer cette durée[4].

En résumé, les personnes dont les données font l'objet d'un traitement bénéficient des droits suivants :

– le droit à l'information ;
– le droit d'accès ;
– le droit de rectification ;
– le droit à l'effacement ou droit à l'oubli ;
– le droit à la portabilité ;
– les droits d'opposition ;
– le droit à la limitation du traitement ;
– le droit d'interrogation ;
– le droit de définir des directives relatives à la conservation, l'effacement et la communication de ses données à caractère personnel après sa mort.

La nouvelle rédaction de l'article des CCAG relatif au traitement des données personnelles impose donc à l'acheteur public de prévoir la possibilité d'une demande de droit d'accès aux données archivées et, d'autre part, d'être en mesure d'y répondre favorablement.

Parallèlement à l'assurance de ces droits, l'acheteur devra prévoir les mesures de confidentialité et de sécurité permettant aux personnes concernées, d'obtenir toutes les informations utiles sur la protection de leurs données. De manière générale, les mesures de sécurité mises en œuvre par l'acheteur devront garantir un niveau de sécurité suffisant pour empêcher tout risque quant à la violation des données collectées.

À cet effet, l'article 32 du RGPD met à la charge du responsable de traitement une obligation générale de sécurité : « Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

la pseudonymisation et le chiffrement des données à caractère personnel ;

des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »

Il résulte de cette nouvelle rédaction que l'acheteur devra, dans le cadre de la passation et de l'exécution du marché public, prévoir un système de sécurité suffisamment coercitif pour répondre tant aux exigences du RGPD que celles issues de l'article 4 de la loi Informatique et Libertés.

Enfin, se pose la question déterminante de la durée, de la conservation et du sort des données collectées.

Dans le cadre de la collecte des données personnelles par le responsable de traitement, ce dernier doit prévoir des durées de conservation des données qui respectent des principes correspondant à la nature de la donnée collectée.

À titre d'illustration, concernant la durée de conservation des données courantes (données actives dans les systèmes informatiques) la CNIL recommande, dans sa

(4) RGPD, art. 13.2a).

délibération de 2005, de fixer une durée de conservation spécifique et proportionnée à la finalité du traitement.

Concernant les données intermédiaires (données qui présentent encore pour les services concernés un intérêt administratif, comme par exemple en cas de contentieux), la CNIL recommande que la durée de leur conservation soit proportionnelle aux durées des recours auxquels le responsable de traitement pourrait faire face.

En tout état de cause, la CNIL rappelle que la durée de conservation des données doit être proportionnelle et en adéquation avec la finalité pour laquelle ces dernières sont conservées.

Des sanctions à la hauteur des enjeux

Au regard d'un tel niveau d'exigences tant sur l'acheteur que le titulaire, il convient d'identifier les sanctions en cas du non-respect des exigences en matière de traitement des données personnelles.

À cet effet, il convient de différencier les sanctions qui pèsent sur le titulaire de celles qui pèsent sur l'acheteur.

Partant, l'article 5.2.3 identifie les nouveaux leviers coercitifs à l'initiative de l'acheteur en cas de manquement par le titulaire de ses obligations. Ainsi, les documents contractuels (notamment le CCAP) devront mentionner les sanctions en cas de manquement.

Ils devront dès lors prévoir précisément des pénalités spécifiques applicables par l'acheteur en cas de manquement par le titulaire à ses obligations en matière de données personnelles. Parallèlement, la nouvelle rédaction de l'article 50.3.1 du CCAG Travaux par exemple, prévoit que le manquement des exigences en matière de traitement des données personnelles peut justifier la résiliation du marché pour faute du titulaire, ou son sous-traitant.

En qualité de responsable de traitement l'acheteur est naturellement exposé à des sanctions en cas de manquements aux exigences en termes de traitement des données personnelles.

Le montant des sanctions prononcées par la CNIL à l'encontre des violations de la réglementation des données personnelles a considérablement augmenté depuis ces trois dernières années. À titre d'illustration, si entre 2006 et début 2019 le montant moyen des sanctions pécuniaires prononcées par la CNIL avoisinait les 35 000 euros[5], la moyenne des sanctions prononcées en application du RGPD est à ce jour de 275 000 euros (en dehors de la très récente décision Google LLC), soit une augmentation de 686 %.

Le RGPD organise en majeure partie, les pouvoirs permettant aux autorités de contrôle de sanctionner les violations des règles qu'il édicte, laissant aux États membres le soin de déterminer les autres sanctions pouvant s'avérer nécessaires. L'article 58 alinéa 2 du RGPD dresse une liste détaillée des pouvoirs dont les autorités de contrôle nationales disposent (en France, la CNIL). Il faut savoir que la loi Informatique et Libertés, si elle reprend en majeure partie les sanctions prévues par le RGPD, est moins coercitive que ce dernier.

Il convient à ce titre de distinguer les mesures correctrices pouvant être adoptées par les autorités de contrôle, des sanctions administratives d'ordre pécuniaires.

L'article 58 alinéa 2 RGPD du RGPD dresse la liste de ces mesures correctrices :
– Avertissement ;
– Rappel à l'ordre en cas de violation ;
– Ordonner au responsable du traitement/sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;
– Ordonner de mettre les opérations de traitement en conformité avec le règlement, le cas échéant, de manière spécifique ou dans un délai déterminé ;
– Ordonner la communication d'une violation à la personne concernée ;
– Imposer une limitation temporaire ou définitive, ou une interdiction du traitement ;
– Ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement et la notification de ces mesures aux destinataires auxquels les données ont été divulguées ;
– Retirer, ordonner de retirer ou ordonner de ne pas délivrer une certification ;
– Ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

Ces mesures sont prises en fonction de différents critères notamment la nature de la violation, le comportement de l'auteur avant, pendant et après la violation et toutes autres circonstances aggravantes ou atténuantes[6].

Ces mesures correctrices n'empêchent toutefois pas l'application de sanctions administratives d'ordre pécuniaire. À cet effet, les articles 20 de la loi Informatique et Libertés[7] et 83 du RGPD fixent le montant maximum de l'amende pouvant être adoptée en fonction notamment du manquement et de son auteur.

Le montant des amendes pouvant être prononcées sont fixées en fonction de la nature du manquement et peut monter jusqu'à 20 millions d'euros ou dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires mondial de l'exercice précédent[8].

(5) Moyenne des 68 sanctions pécuniaires prononcées par la CNIL entre 2006 et 2019.

(6) RGPD, art. 83.
(7) Loi n° 78-17 du 6 janvier 1978, art. 20 al. 7.
(8) RGPD, art. 83 al. 5.

Dans le cas de manquement « moins importants » ce montant est fixé à 10 millions d'euros et 2 % du chiffre d'affaires annuel mondial de l'exercice précédent[9].

Si le responsable du traitement ou le sous-traitant viole, délibérément ou par négligence, plusieurs dispositions du RGPD dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut excéder le montant fixé pour la violation la plus grave[10].

L'article 83 du RGPD est intitulé « conditions générales pour imposer des amendes administratives, formulation qui suggère que le régime devra être précisé, par la jurisprudence de la CJUE d'une part, et par les lois nationales d'autre part. Il faudra donc observer l'évolution de ces dernières dans les années suivant l'entrée en vigueur du règlement.

L'activité récente a attesté que la CNIL n'hésitait pas ou plus à sanctionner très fortement les structures ayant violé la règlementation en matière de données personnelles. Pour illustration, le 7 décembre 2020, la formation restreinte de la CNIL a sanctionné les sociétés Google LLC et Google IRELAND LIMITED d'un montant total de 100 millions d'euros, notamment pour avoir déposé des cookies publicitaires sur les ordinateurs d'utilisateurs du moteur de recherche google.fr sans consentement préalable ni information satisfaisante.

Toutefois, au regard de l'ambition du RGPD et des lois nationales chargées de réglementer le traitement des données personnelles (rappelons que cela concerne l'ensemble des structures publiques et privées), il conviendra de prêter fortement attention aux futures décisions de la CNIL surtout dans le cas de « zone de doute ».

À l'heure actuelle, si la sanction des collectivités publiques et de leurs établissements publics ne fait aucun doute, une interrogation plane concernant les établissements publics de l'État. En effet, l'article 20 alinéa 7 de la loi Informatique et Libertés exonère de sanctions pécuniaires, les traitements réalisés par l'État.

Se pose alors naturellement la question des traitements opérés par les établissements publics de l'État. À défaut d'avoir une définition précise de l'État, comment savoir si le régime de ses établissements publics conduit également à exonérer ces derniers de sanctions.

Un établissement qui agirait pour l'État, sous tutelle d'un ministère, doit-il être compris comme l'État à défaut d'avoir un régime expressément défini ?

La problématique de l'assimilation d'un établissement public administratif au traitement de l'État ressort de deux lectures différentes du mot « État » figurant dans l'article 20 de la Loi informatique et Liberté :

« 7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ».

Par analogie avec le Code de la commande publique, une lecture large du texte de l'article 20 de la Loi Informatique et Liberté permettrait de relier le terme « Etat » à l'ensemble de ses établissements publics. En effet, dans le Code de la commande publique, le traitement des établissements publics de l'État est assimilé au traitement appliqué pour l'État. Partant, une lecture large de l'article 20 supposerait que l'exclusion appliquée à l'État dans le traitement de données est applicable pour ses établissements publics.

A contrario, il pourrait être soutenu qu'une lecture stricte du texte de la loi est à favoriser et que, s'agissant de l'exclusion appliquée pour l'État, celle-ci n'est pas transposable à ses établissements publics puisque ceux-ci ne sont, à la différence du Code de la commande publique, pas spécifiquement mentionnés.

À défaut de jurisprudences pour traiter cette incertitude, il est à espérer une prochaine prise de position de la CNIL.

(9) RGPD, art. 83 al. 4.
(10) RGPD, art. 83, al. 3.