WEKA .media .jobs .fr

LES FOCUS WEKA

L'IMPACT DU RGPD SUR LES MARCHÉS PUBLICS

JANVIER - 2020

WEKA.fr

WEKA met à votre disposition les meilleurs spécialistes et toutes les ressources documentaires, réglementaires et méthodologiques.

l'expertise juridique du service public

- Toutes les ressources nécessaires pour **sécuriser** vos actions juridiques et opérationnelles.
- Informations et conseils en ligne **actualisés** des dernières évolutions réglementaires.
- Des outils et modèles de documents **prêts à l'emploi**.

WEKA.jobs

weka.jobs est un réseau entièrement dédié aux carrières publiques, aux offres d'emploi sur tout le territoire français et à l'actualité de l'emploi public.

le réseau de l'emploi public

- Bénéficiez d'une **visibilité optimale** sur tous les médias WEKA auprès de 120 000 professionnels de la fonction publique.
- Adressez-vous à une **audience qualifiée** sur tous les métiers du secteur et trouvez vos futurs talents.
- Valorisez l'attractivité de votre collectivité en communiquant sur votre **marque employeur.**

WEKA.media

Web-conférences, livres blancs, magazine, newsletters... WEKA propose une lecture interactive et actualisée des enjeux propres au secteur public.

l'audience web du secteur public

- Des web-conférences animées par des **experts de qualité** pour décrypter ensemble les sujets d'actualité.
- Des livres blancs gratuits pour vous apporter des **solutions** à des problématiques liées à votre activité.
- Des articles, publi-reportages, veille juridique pour vous informer de toute l'**actualité du secteur public.**

SOMMAIRE

ÉDITO

Le règlement européen n° 2016/679 du 27 avril 2016, dit « règlement général sur la protection des données personnelles » (RGPD), applicable depuis le 25 mai 2018 et complémentaire à la loi Informatique et Libertés, est venu renforcer les droits des personnes et les responsabilités des responsables de traitements et des sous-traitants. Nous sommes passés d'une logique de contrôle *a priori* à une logique de responsabilisation de tous les acteurs, privés ou publics. L'objectif poursuivi est de responsabiliser les organisations, privées comme publiques, qui gèrent des données personnelles.

Concernant les marchés publics, quels sont les impacts liés à cette réglementation ? Comment l'intégrer ? Quels sont les risques associés en cas de non-conformité ?

Le RGPD impacte la commande publique dès lors que le titulaire d'un contrat est amené à manipuler des informations sensibles issues des agents du pouvoir adjudicateur, des usagers du service public ou des citoyens. Au sens du texte européen, les acheteurs sont considérés comme des responsables du traitement. Ils doivent donc veiller à la protection des données personnelles par le prestataire, dénommé « sous-traitant » dans le RGPD.

Réaliser une cartographie précise des données et des acteurs, mettre en place des clauses relatives au RGPD dans les cahiers des clauses particulières ou, le cas échéant, réaliser un avenant pour les marchés en cours, veiller à la destruction des données sensibles au terme du contrat… De manière concrète, le RGPD se retrouve dans toutes les phases des procédures de la commande publique, de la préparation du marché à son exécution.

Le RGPD, comme l'indiquait récemment la DAJ de Bercy, « doit devenir une thématique comme une autre, parmi toutes les réglementations dont a à connaître un acheteur public au quotidien ».

Julien Prévotaux
Responsable éditorial Publishing & Media

LE RGPD : RAPPELS LÉGISLATIFS

L'élaboration du RGPD a nécessité plusieurs années de négociations entre les États membres de l'Union Européenne. Le RGPD aborde des principes clés qui ont été mis en avant lors des négociations par les représentants européens. Ce nouveau règlement européen impose inévitablement de respecter de nouvelles obligations et de suivre différentes étapes pour les organismes gestionnaires de traitements de données.

LES GRANDS PRINCIPES DU RGPD

Le RGPD met en avant quatre grands principes qui sont le consentement, la transparence, le droit des personnes et la responsabilité *(accountability)*.

Le consentement

Selon l'article 7 du RGPD « le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale ». Le consentement ne se présume pas, il doit pouvoir se prouver. Le consentement peut être retiré à tout moment par les personnes le demandant. Pour les entreprises, la collecte du consentement n'est pas obligatoire si la finalité de la collecte est bien respectée (les cases pré-cochées restent autorisées).

La transparence

L'article 12 du RGPD nous indique que les organisations doivent fournir aux individus des informations claires et sans ambiguïté sur la façon dont sont traitées leurs données. Celles-ci doivent être accessibles par tous, *via* des documents contractuels, des formulaires de collecte ou les pages dédiées des sites web.

Le droit des personnes

De nouveaux droits sont apparus dans le règlement, comme le droit à l'oubli pour tous les utilisateurs. Les organisations n'auront plus qu'un mois (au lieu de deux) pour supprimer les données suite à une demande. Le droit à la portabilité des données est aussi une nouveauté. Il permet à un individu de récupérer les informations qu'il a fournies sous une forme réutilisable pour, le cas échéant, les transférer à un tiers.

Le principe de responsabilité *(accountability)*

Ce principe regroupe toutes les mesures qui visent à responsabiliser davantage les entreprises dans le traitement des données à caractère personnel. Les organismes gestionnaires de traitements doivent par exemple mettre en place des mesures adéquates pour garantir la sécurité des données. Ils doivent également appliquer le « *privacy by design* » (art. 25 du RGPD), un concept qui impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. Elles doivent aussi choisir des sous-traitants qui soient conformes au RGPD (art. 28 du RGPD) ou encore désigner un *Data Protection Officer* (DPO) (art. 37 du RGPD), chargé de contrôler la conformité de l'organisme avec le RGPD *via*, entre autres, la tenue d'un registre des traitements (art. 30 du RGPD) et la mise en place d'analyses d'impact relatives à la protection des données (art. 35 du RGPD).

LES SANCTIONS PRÉVUES PAR LE RGPD

La Commission Nationale de l'Informatique et des Libertés (CNIL) continue de procéder à des vérifications dans les locaux des organisations ou en ligne. Étant donné que les principes fondamentaux de la protection des données, issus de la loi française Informatique et Libertés du 6 janvier 1978 ainsi que de la Directive européenne du 24 octobre 1995, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel restent globalement inchangés (sécurité des données, loyauté du traitement, durée de conservation...), ils continuent donc à faire l'objet de vérifications rigoureuses de la part de la CNIL. En revanche, les nouvelles obligations et les nouveaux droits mis en avant par le RGPD (droit à la portabilité, analyses d'impact...) sont susceptibles de faire l'objet de contrôles. Ces contrôles ont dans un premier temps été non punitifs. L'objectif étant avant tout d'aider les organismes à bien comprendre les enjeux et la mise en œuvre opérationnelle des nouvelles dispositions, si l'entité est de bonne foi et qu'elle est engagée dans une démarche de conformité, la CNIL n'a appliqué aucune sanction durant les premiers mois qui ont suivi l'entrée en vigueur du règlement. Les contrôles effectués sur les acteurs internationaux sont réalisés par plusieurs organismes afin de rendre une décision à portée européenne. Les sanctions sont de trois ordres : elles peuvent être financières, opérationnelles et/ou porter sur la réputation d'un organisme. Jusque-là, sauf manquement délibéré et grave, le rôle de la CNIL n'était que consultatif et elle se contentait de proposer des recommandations sans disposer d'un réel pouvoir de sanction. Le RGPD devient une législation contraignante *via* la possibilité d'émettre des amendes administratives financières. Les sanctions financières sont possibles à l'encontre des entités publiques ayant une personnalité morale distincte (EPA, EPIC, collectivités, etc.) et des revenus hors dotation mais *a priori* pas pour l'administration centrale qui en est exonérée. Pour le secteur privé, des pénalités sont prévues allant jusqu'à 20 millions d'euros ou 4 % du CA mondial annuel de l'entreprise (la loi vise clairement les multinationales sur ce point).

Les sanctions peuvent aussi être opérationnelles *via* une interdiction temporaire ou permanente de traiter des données personnelles.

Cette sanction se présente sous les formes suivantes selon la gravité des faits reprochés :

- Injonction de cesser le traitement ;
- Signalement au ministère de Tutelle voire au Premier ministre ;
- Mise en demeure (publique ou non) de se mettre en conformité avec le RGPD ;
- Un simple avertissement (logique d'accompagnement plutôt que de sanction).

Une sanction rendue publique peut entraîner des conséquences sur la réputation de l'organisme ou de l'entreprise. Il y a par exemple à craindre une dégradation de l'image de l'administration auprès du grand public, des usagers, des échelons supérieurs, etc. Dans un environnement commercial, il a pu être observé une perte de clientèle jusqu'à 4 % suite aux révélations au public du défaut de conformité à la législation sur la sécurité informatique de l'entreprise visée. Pour les géants du web comme Facebook ou Google, la note pourrait atteindre des dizaines ou des centaines de millions d'euros. Cependant, les multinationales ne sont pas forcément les entreprises les plus exposées. Le risque est en revanche plus élevé pour les petites entités comme les TPE, les PME, les associations, ou même les petites collectivités souvent peu renseignées sur le sujet, et qui disposent de beaucoup moins de ressources leur permettant de se mettre aux normes.

LE NOUVEAU RGPD ET SES INCIDENCES SUR LES MARCHÉS ET LES ACHETEURS PUBLICS

Le Règlement Général sur la Protection des Données (RGPD – n° 2016/679), ou « RGPD », est entré en application le 25 mai 2018 dans l'ensemble de l'Union Européenne.

En France, la loi CNIL 3 visant à adapter la loi Informatique et libertés du 6 janvier 1978 au RGPD, a été promulguée le 20 juin 2018, après avoir été validée par le Conseil constitutionnel le 12 juin 2018. Cette nouvelle réglementation vise à inciter chaque organisme, public ou privé, à veiller à une meilleure protection des données personnelles des citoyens.

OBLIGATIONS

En leur qualité de responsables de traitement, il découle pour les acheteurs publics de nouvelles obligations qu'il leur appartient de respecter, et ce afin d'éviter les lourdes sanctions auxquelles ils peuvent s'exposer.

Rappelons à ce titre que l'article 45 de la loi Cnil 3 permet désormais à la Commission nationale de l'Informatique et des Libertés (CNIL) de prononcer des amendes administratives pouvant aller de 10 à 20 millions d'euros, et que seul l'État est exempté de ces sanctions.

Les obligations des acheteurs publics en leur qualité de responsable de traitement ne sont pas différentes de celles incombant aux acteurs privés, sauf en ce qui concerne la désignation d'un délégué à la protection des données personnelles qui, aux termes de l'article 37.1.a du RGPD, est obligatoire pour toute autorité publique ou organisme public traitant des données personnelles.

Outre la désignation d'un délégué à la protection des données (qui peut se faire par le biais d'un marché public de services), les acheteurs publics doivent ainsi assurer :

- La tenue d'un registre de traitement (article 30 du RGPD) ;
- La mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (article 32 du RGPD) ;
- La conduite d'études d'impact si nécessaire (article 35 du RGPD) ;
- La mise en place de mesures techniques et organisationnelles destinées à garantir l'effectivité des droits garantis par le RGPD aux articles 12 à 22 (droit d'accès, rectification, modification, opposition…) ;
- La notification à la CNIL dans les 72 heures des cas de violation des données à caractère personnel (article 33 du RGPD) et la communication de cette violation aux personnes concernées dans les meilleurs délais en cas de risque élevé pour les personnes concernées (article 34 du RGPD).

MARCHÉ PUBLIC ET RGPD

Étant responsable vis-à-vis des personnes dont les données sont collectées, les organismes publics doivent faire preuve d'une vigilance particulière dans le choix du sous-traitant qui est amené à traiter les données personnelles des administrés pour leur compte.

SOUS-TRAITANT

À titre liminaire, la notion de sous-traitant au sens du RGPD ne doit pas être confondue avec celle de sous-traitant au sens de la loi n° 75-1334 du 31 décembre 1975 relative à la sous-traitance. La loi de 1975 définit la sous-traitance comme étant une opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant

l'exécution de tout ou partie du contrat d'entreprise, ou d'une partie du marché public conclu avec le maître d'ouvrage (article 1er).

Pour le RGPD, le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (article 4 du RGPD).

Dès lors, les titulaires de marchés publics peuvent, alors qu'ils sont considérés comme entrepreneurs vis-à-vis des acheteurs publics au regard de la loi de 1975, être considérés comme des sous-traitants vis-à-vis de l'acheteur public au regard du RGPD dans le cadre de l'exécution du marché public. C'est le cas par exemple dans le cadre de marchés publics passés avec des titulaires traitant des données personnelles pour des finalités et selon des moyens déterminés par l'acheteur public.

PASSATION DU MARCHÉ PUBLIC

De manière générale, l'intervention d'un sous-traitant suppose la passation d'un contrat ou d'un autre acte juridique entre le responsable du traitement et le sous-traitant.

Dans le cadre d'un marché public dont l'exécution suppose que le titulaire traite des données à caractère personnel pour le compte de l'acheteur public en tant que sous-traitant de ce dernier, le marché public qui lie l'acheteur public au titulaire devra donc également faire office de contrat entre le responsable de traitement et le sous-traitant au regard du RGPD.

Le cas échéant, l'acheteur public peut instaurer des critères et exigences au stade de la sélection des candidatures afin de s'assurer de la capacité technique du futur titulaire du marché pour traiter les données personnelles (ex : les candidats ont, dans certains cas, l'obligation de désigner un délégué à la protection des données ainsi que l'obligation de tenir un registre).

CONTENU DU MARCHÉ PUBLIC

La question est dès lors de savoir ce que l'acheteur public doit inclure dans les clauses contractuelles qu'il est amené à rédiger.

Le marché public (et plus particulièrement le cahier des clauses administratives particulières ou le cahier des clauses techniques particulières) doit contenir des principes permettant de veiller à ce que le sous-traitant mette en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes concernées.

L'acheteur public doit ainsi insérer des clauses visant à :

- Informer le sous-traitant de la nature de la finalité du traitement, du type de données à caractère personnel et des catégories de personnes concernées par les données à caractère personnel concernées par le marché ;
- Déterminer les mesures techniques et organisationnelles de sécurité et de confidentialité mises en œuvre ;
- Prévoir une obligation de notification sans délai de tout incident sur des données à caractère personnel ;
- Prévoir une obligation de faire agréer par l'acheteur public tout sous-traitant de second rang (au regard du RGPD) ;
- Prévoir une obligation de conseil et d'assistance (techniques et/ou opérationnels) du sous-traitant ;
- Prévoir une obligation de fournir les éléments de preuves de conformité au règlement européen (notamment par le biais de code de conduite ou de mécanisme de certification adopté par le sous-traitant) ;
- Prévoir une obligation de ne traiter les données que sur instruction de l'acheteur public ;
- Prévoir une obligation de détruire ou renvoyer sans copie toutes les données personnelles soumises au traitement ;
- Prévoir les sanctions en cas de non-respect des dispositions liées à la protection des données personnelles.

En outre, l'acheteur public doit veiller à ce qu'en sa qualité de sous-traitant, le titulaire respecte ses propres obligations au regard du RGPD.

SANCTION

En cas de non-respect du RGPD, l'acheteur public et le sous-traitant encourent chacun au titre de leur manquement respectif une amende administrative, étant précisé qu'ils sont solidairement responsables du dommage causé par le traitement vis-à-vis de la personne concernée.

Dès lors, le marché public doit contenir des sanctions contractuelles spécifiquement liées au non-respect par le titulaire de ses obligations RGPD, telles que des pénalités et/ou la possibilité de résilier unilatéralement le marché pour faute du titulaire.

Élise Dufour
Of counsel chez Bignon Lebray

Spécialiste en droit des nouvelles technologies, Élise Dufour accompagne une clientèle française et internationale dans leurs projets numériques (droit de l'informatique, droit des données personnelles, droit du commerce électronique).

Sébastien Pinot
Avocat associé chez
Bignon Lebray

Avocat spécialisé en droit public des affaires depuis plus de 15 ans, Sébastien Pinot a passé plusieurs années au sein du département Droit public/ Financement de projets de Linklaters, et a intégré le bureau parisien de Bignon Lebray en février 2010 pour renforcer le Département Droit public et de l'environnement.

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPD)

Pour être efficace, une réglementation portant sur la bonne gestion des données personnelles doit disposer de relais au plus proche des structures traitant ces informations. C'est dans ce but que le CIL (Conseiller Informatique et Libertés) avait été créé et son rôle était donc d'être un référent entre la Commission Nationale de l'Informatique et des Libertés (CNIL) et les administrations ou les entreprises, pour toutes les questions liées à la collecte et à la gestion des données personnelles par ces dernières. Les missions du CIL ont largement évolué avec la mise en action du RGPD le 25 mai 2018, les termes de son action ont été profondément modifiés ainsi que sa dénomination : le CIL est remplacé par le DPD (Délégué à la Protection des Données).

Le statut de CIL s'est éteint au 25 mai 2018 mais n'a pas entraîné de transformation automatique du CIL en DPD. Cela signifie que le nouveau DPD doit être à nouveau nommé pour chaque structure. La désignation d'un Délégué à la Protection des Données (DPD) est obligatoire si :

- Vous êtes un organisme public au sens large : EPIC ou EPA. Les EPA et EPIC sont les deux régimes juridiques possibles d'un établissement public. Ils se distinguent par leur activité : service public administratif, pour les EPA, ou service public industriel et commercial, pour les EPIC.
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle (un fichier client relève de cette terminologie incluant la quasi-totalité des entreprises, même les TPE et/ou PME).
- Vous traitez à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

On constate donc que le DPD devient obligatoire pour quasiment toutes les structures traitant des données. Comme pour le CIL, il est possible d'externaliser les missions du DPD ou de les mutualiser, c'est-à-dire qu'un DPD peut être désigné pour plusieurs organismes sous certaines conditions (être facilement joignable par exemple). La procédure de nomination du DPD est très simple, il suffit de remplir le formulaire suivant disponible sur le site de la CNIL : https://www.cnil.fr/fr/designation-dpo. L'article 37 paragraphe 5 du RGPD nous indique que « le DPD est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 ». À noter également qu'aucune forme de rémunération n'est prévue par les textes pour les missions du DPD. Dans la plupart des cas, et notamment dans les établissements publics, il s'agit d'un surplus de missions à titre gracieux en plus des missions habituelles du salarié, sauf convention contraire auprès de votre employeur.

LES MISSIONS DU DPD

Le Délégué à la Protection des Données Personnelles (DPD) ou Data Protection Officer (DPO) en anglais est chargé d'assurer la mise en conformité RGPD de l'organisme auquel il est rattaché (le plus souvent son employeur). Il doit faire en sorte que ses collaborateurs respectent les dispositions du RGPD quand ils utilisent des données à des fins commerciales ou à des fins internes (au sein des différents logiciels permettant de gérer les RH, la comptabilité ou encore les listes de clients/usagers par exemple). Il est donc amené à collaborer avec tous les services d'une entreprise/administration. Le Délégué à la Protection des Données est principalement chargé :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- De contrôler le respect du règlement et du droit national en matière de protection des données ;

- De conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Pour accomplir au mieux ces missions le délégué doit notamment :

- S'informer sur le contenu des nouvelles obligations (*via* le forum dédié de la CNIL, des formations, en consultant le texte du RGPD et les éventuelles jurisprudences qui en découlent…) ;
- Sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- Réaliser l'inventaire des traitements de données de ou des organisme(s) dont il dépend ;
- Concevoir des actions de sensibilisation (par des informations régulières auprès de ses collaborateurs) ;
- Piloter la conformité en continu (assurer un suivi sans interruption des différents traitements de l'organisme *via* le registre des traitements).

Le DPD doit pouvoir évoluer en toute indépendance : cela veut dire qu'il ne doit pas se retrouver en situation de conflit d'intérêts entre cette fonction et une autre mission, il ne doit pas recevoir d'instruction dans le cadre de son travail de délégué, ne pas subir de sanction pour l'exercice de cette tâche et pouvoir rendre compte de son action au plus haut niveau de la direction de l'organisme. Des outils de plus en plus nombreux sont élaborés par la CNIL pour assister le DPD dans ses missions, comme par exemple le logiciel open source PIA (Privacy Impact Assessment) qui, comme son nom l'indique, permet de mesurer l'impact des traitements sur les données personnelles en permettant de faciliter la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD. En termes plus clairs, ce logiciel permet d'aider le DPD à déterminer si ce dernier est compatible avec les règles du RGPD facilitant l'implication de tous les acteurs de la mise en place d'un traitement.

Anglicismes des acronymes :

- GPDR *(General Data Protection Regulation)* = RGPD (Règlement Européen sur la Protection des Données)
- DPO *(Data Protection Officer)* = DPD (Délégué à la Protection des Données)

Intégrer le RGPD et la loi informatique et libertés dans vos marchés publics

Référence Internet 11315

*Saisissez la Référence Internet **11315** dans le moteur de recherche du site www.weka.fr pour accéder à cette fiche*

La mise en place du règlement européen n° 2016/679 du 27 avril 2016, dit « règlement général sur la protection des données personnelles » (RGPD), applicable depuis le 25 mai 2018 et complémentaire à la loi informatique et libertés, doit conduire à sa bonne intégration dans vos marchés publics.

Quels sont les impacts liés à cette réglementation ? Comment l'intégrer ? Quels sont les risques associés ?

En pratique

Étape 1

Comprendre l'impact du RGPD

Le règlement européen n° 2016/679 du 27 avril 2016, dit « RGPD », est applicable depuis le 25 mai 2018. Dans ce cadre, la collecte et le traitement de données portant sur une personne physique identifiée ou identifiable, initialement encadrés par la loi informatique et libertés, doivent faire l'objet d'une attention renforcée.

Le non-respect de ce cadre réglementaire peut conduire, en cas de dommage subi par la personne physique concernée, à la mise en jeu de votre responsabilité, mais également à des sanctions administratives par la Commission nationale de l'informatique et des libertés (Cnil). Cette responsabilité peut être engagée à hauteur de 20 millions d'euros (4 % du chiffre d'affaires pour les entités privées – ceci étant peu applicable au secteur public).

Afin de se prémunir contre ce risque, une première action importante doit être **l'identification des traitements de données** mis en œuvre afin de mesurer ce qui doit être entrepris.

Étape 2

Identifier les traitements de données concernés par votre marché et les responsables des traitements

À titre liminaire, il convient de déterminer les acteurs, notamment le **responsable du traitement**. Celui-ci désigne « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* » (*source :* règlement européen du 27 avril 2016, art. 4).

En l'occurrence, il s'agit le plus souvent du pouvoir adjudicateur mais, dans certains cas, cela peut être une autre entité administrative. À cet égard, le **sous-traitant** désigne « *la personne physique ou morale […] qui traite des données à caractère personnel pour le compte du responsable du traitement* », à savoir, en principe, le titulaire.

Attention

Cette notion de sous-traitant, propre au RGPD, ne doit ainsi pas être confondue avec la notion de sous-traitant au sens du droit de la commande publique, ces deux notions ne

recouvrant pas nécessairement les mêmes périmètres.

Une fois les acteurs identifiés, il est essentiel de caractériser les traitements de données concernés. Il s'agit de discerner, pour chacun des traitements, la finalité de celui-ci *(ex. : traitement 1 : transmission des données personnelles de X à Y, la finalité étant la réalisation d'une enquête)*.

Une fois tous les traitements identifiés, et au-delà de la finalité, il convient de déterminer :

- la **catégorie des données** concernées *(ex. : données personnelles de type identification comme les nom, prénom, date de naissance ; coordonnées comme le mail ou le numéro de téléphone)* ;
- la **catégorie de la personne** concernée *(ex. : bénéficiaires de l'enquête dans notre exemple)* ;
- la **durée de conservation** des données *(ex. : notification du marché jusqu'à la fin de la réalisation des prestations [soit au plus tard le…]).*

Tous ces éléments doivent être clairement identifiés dans le cahier des clauses administratives particulières (CCAP) de votre marché au sein de l'article relatif à la protection des données personnelles.

Étape 3

Rappeler les obligations du titulaire, ses responsabilités et les conséquences de toute violation

La clause de votre CCAP doit comporter un certain nombre d'éléments :

- tous les **engagements généraux du titulaire** :
  - utiliser des données uniquement pour les finalités liées à l'exécution des prestations ;
  - prendre toutes les mesures utiles pour respecter les dispositions applicables en matière de protection des données à caractère personnel ;
  - désigner un délégué à la protection des données s'il y est tenu ;
  - disposer d'une politique interne de gestion des données à caractère personnel et la diffuser en interne ;
  - réaliser des programmes de sensibilisation de ses collaborateurs ;
  - collaborer avec le pouvoir adjudicateur pour le respect de la réglementation ;
  - informer de toute modification de mesure de sécurité ayant un impact en termes de conformité ou divulgation sans autorisation des informations ;
  - informer le pouvoir adjudicateur en cas de transfert de données à un pays tiers ou une organisation internationale ;
  - démontrer le respect des obligations en cas de demande d'une autorité de contrôle ;
  - informer le pouvoir adjudicateur si une violation de la réglementation est constituée par une instruction du pouvoir adjudicateur ;
- les **mesures de sécurité physique, logique et organisationnelle**, pour garantir la protection des données personnelles *(ex. : porte, digicode, code d'accès, charte informatique, etc.)* ;
- les **règles applicables en matière de gestion de la sous-traitance de second niveau** (sous-traitance du titulaire). Il s'agit en l'occurrence d'obtenir des précisions par rapport au dispositif classique prévu par la réglementation en matière de marchés publics (notamment afin de connaître les impacts en matière de traitement) ;
- les **spécificités liées au transfert de données en dehors de l'Union européenne**, notamment l'impossibilité de transférer les données à des pays non reconnus comme ayant des niveaux de protection adéquats ;
- le fait de tenir par écrit un **registre recensant les traitements effectués** avec l'ensemble des informations associées *(ex. : les catégories de traitements effectués pour le compte de chaque client)* ;

- la **notification au pouvoir adjudicateur de toute violation de données** à caractère personnel détectée, et le contenu de la notification *(ex. : date de la détection, nature de la violation, typologie des données concernées, etc.)* ;
- le fait de préciser **qui gère l'information et la gestion des droits des personnes concernées** (et si est applicable le droit d'accès, de rectification, d'opposition, d'effacement de limitation ou de portablité formulé par un individu) ;
- les **relations avec les autorités de contrôle** (collaboration avec le pouvoir adjudicateur en cas de contrôle d'une autorité) ;
- la **destruction des données** en fin de marché ;
- le fait de préciser la **nécessité de mise à disposition de la documentation** permettant de démontrer le respect des obligations applicables et la réalisation des audits.

En termes de responsabilité, la clause a notamment pour objet de rappeler :

- le périmètre de responsabilité en termes de paiement des amendes ainsi que les cas d'exonération de responsabilité (notamment en cas de preuve que le fait provoquant le dommage ne peut être imputé au titulaire) ;
- la possibilité de résiliation du pouvoir adjudicateur en cas de non-respect des clauses applicables en matière de protection des données personnelles.

Enfin, les noms du représentant du pouvoir adjudicateur et de son délégué à la protection des données doivent être précisés dans la clause, le titulaire devant faire de même dans l'acte d'engagement.

Notre conseil

En matière de droit de la protection des données personnelles, il est essentiel, dans le cadre de votre marché, de **réaliser une cartographie précise** :

- des traitements de données ;
- des finalités des traitements ;
- de la catégorie des données concernées ;
- de la catégorie de la ou des personne(s) concernée(s) ;
- de la durée de conservation des données.

Évitez les erreurs

En matière de droit de la protection des données personnelles, **il est important que les clauses soient adaptées au contexte spécifique de votre achat**. Par exemple, en matière de sécurité, vos clauses doivent être circonstanciées à votre achat, mais également au marché fournisseur (vos fournisseurs sont-ils capables d'y répondre ?). De même, les traitements, finalités, catégories de données/personnes concernées et la durée de conservation doivent être très clairement identifiés dans le marché. À défaut, il faudra les définir au plus tôt à travers une comitologie *ad hoc,* prévue dans le marché.

Foire aux questions

Peut-on obliger le titulaire à supprimer les données collectées à la fin du contrat ?

Oui. Cela doit d'ailleurs être prévu dans le CCAP du marché.

Existe-t-il des sanctions particulières en cas de non-respect des règles relatives au RGPD et, de manière générale, des règles relatives à la protection des données personnelles ?

Oui. En cas de dommage subi par la personne physique concernée, votre responsabilité peut être mise en jeu, et des sanctions administratives peuvent être prononcées à votre égard par la Cnil. Cette responsabilité peut être engagée à hauteur de 20 millions d'euros (4 % du chiffre d'affaires pour les entités privées – ceci étant peu applicable au secteur public).

Pour aller + loin

Références juridiques

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés »

Bibliographie

- Recommandations, avis et décisions des autorités de contrôle sur la protection des données et du Comité européen de la protection des données (CEPD) (*European Data Protection Board* [EDPB])
- Cnil, *Règlement européen sur la protection des données personnelles. Guide du sous-traitant*, éd. septembre 2017

Les plus Internet

*Saisissez la Référence Internet **11315** dans le moteur de recherche du site www.weka.fr pour accéder aux mises à jour de cette fiche ainsi que la Réf. Internet des rubriques suivantes :*

Références aux textes officiels rattachés à cette fiche

- Loi n° 78-17 du 6 janvier 1978
- Loi n° 2018-493 du 20 juin 2018
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Le forum des acteurs publics

Posez toutes vos questions et partagez votre expérience sur le forum. Nos experts et vos confrères vous répondent sur www.weka.fr/forum/.

Intégrer le RGPD dans les clauses du marché

Référence Internet
11313

1 outil associé

Saisissez la Référence Internet **11313** *dans le moteur de recherche du site www.weka.fr pour accéder à cette fiche*

Depuis l'entrée en vigueur, le 25 mai 2018, du règlement général sur la protection des données, dit « RGPD » (règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016), les acheteurs sont considérés comme des responsables du traitement au sens du texte européen.

Ce document européen, adopté dans le but de protéger les données à caractère personnel des personnes physiques, impacte la commande publique dès lors que le titulaire d'un contrat est amené à manipuler des informations sensibles issues des agents du pouvoir adjudicateur, des usagers du service public ou des citoyens. Sous peine d'être sanctionné, l'acheteur doit veiller à la protection de ces éléments par le prestataire, dénommé « sous-traitant » dans le RGPD.

Quelles sont les clauses à insérer dans les marchés et comment vérifier la mise en œuvre de ces nouvelles obligations ?

En pratique

Étape 1

Maîtriser l'impact du RGPD sur les marchés publics

Le règlement européen n° 2016/679 du 27 avril 2016, dit règlement général sur la protection des données (RGPD), a renforcé la protection des personnes concernées par un traitement de leurs données à caractère personnel.

Les dispositions du RGPD sont applicables depuis le 25 mai 2018. La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ainsi que son décret d'application n° 2018-687 du 1er août 2018 complètent ce règlement.

Il existe toute une série de données à caractère personnel issues des candidatures et des offres. En cas de sollicitation, le maître d'ouvrage doit désormais être en capacité de démontrer sa conformité au texte européen.

Ainsi, en vertu de l'article 12 du RGPD, le maître d'ouvrage a l'obligation de communiquer à la personne concernée, lorsqu'elle en fait la demande, toute explication sur le maniement de ces données.

Les entreprises postulant à un marché public peuvent dorénavant, conformément à cette disposition, solliciter les services de la commande publique pour connaître le sort des éléments sensibles (en dehors des informations en lien avec le secret commercial et industriel) issus de leurs plis.

Étape 2
Identifier les acteurs du RGPD

La responsabilité première quant à la légalité et la licéité des traitements de données à caractère personnel incombe au responsable du traitement.

Selon le RGPD, le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement.

Ainsi, en ce qui concerne les collectivités territoriales et leurs établissements publics, le responsable du traitement est identifié par les organes qui disposent du pouvoir de décider. En pratique, il s'agit de l'organe délibérant par principe et du chef de l'exécutif dans certains cas.

Étant responsables vis-à-vis des personnes dont les données sont collectées, les organismes publics devront donc faire preuve d'une vigilance particulière dans le choix du sous-traitant qui sera amené à traiter les données personnelles des administrés pour leur compte.

A noter

La notion de sous-traitant au sens du RGPD ne doit pas être confondue avec celle de sous-traitant au sens des dispositions relatives à la sous-traitance du Code de la commande publique. Le CCP définit la sous-traitance comme étant une « *opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maître de l'ouvrage* » (CCP, art. L. 2193-2).

Pour le RGPD, le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (RGPD, art. 4).

Le sous-traitant ne peut donc intervenir qu'à l'initiative et sur instruction du responsable du traitement.

L'intervention d'un sous-traitant suppose la passation d'un contrat ou d'un autre acte juridique entre le responsable du traitement et le sous-traitant.

A noter

Aux termes du RGPD, un sous-traitant se limite normalement à traiter des données qui lui sont préalablement fournies par le responsable du traitement. Mais il peut devenir à son tour un responsable de traitement au regard des mêmes données à caractère personnel.

Par exemple, un délégataire de service public chargé de l'exploitation et de la distribution d'eau potable par un EPCI sera qualifié de **sous-traitant** en ce qui concerne le traitement des données fournies par le délégant responsable du traitement (la base de données des abonnés au service d'eau potable) et sera qualifié de **responsable du traitement** s'il utilise la base de données des abonnés à d'autres fins que celles assignées dans le contrat de délégation de service public.

Étape 3

Mettre en place des clauses relatives au RGPD dans les cahiers des charges

Les contrats conclus avec des sous-traitants au sens du RGPD (donc les titulaires des marchés publics) portant sur le traitement total ou partiel de données à caractère personnel doivent contenir des clauses obligatoires prévues par le RGPD. Celles-ci précisent les obligations et la responsabilité du sous-traitant à l'égard du responsable de traitement, qu'il convient d'adapter dans la commande publique.

Le maître d'ouvrage doit adapter le dispositif en fonction de la prestation attendue et des éléments concernés. Pour des prestations ne nécessitant pas la divulgation d'informations sensibles, par exemple un marché de fourniture de papier, une déclaration sur l'honneur peut être suffisante.

Le candidat s'engage à respecter et mettre en œuvre toutes les mesures liées au RGPD.

Pour des marchés où l'entreprise va traiter des données à caractère personnel, deux choix sont possibles :

- l'intégration de clauses spécifiques ;
- l'utilisation des clauses types proposées par la Commission nationale de l'informatique et des libertés (Cnil).

@ Clauses types relatives à la protection des données [Réf. Internet : dtou8121] à consulter sur votre fiche en ligne.

Le marché public (et plus particulièrement le cahier des clauses administratives particulières ou le cahier des clauses techniques particulières) devra contenir des principes permettant de veiller à ce que le sous-traitant mette en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes concernées.

Dans ses futurs contrats, ou par le biais d'avenants pour les contrats existants, l'acheteur public devra instaurer des clauses relatives :

- à la description du traitement des données que le fournisseur aura à traiter dans le cadre du marché (objet et durée du traitement, nature et finalité, types de données) ;
- aux obligations du fournisseur dans l'usage des données :
  - ne traiter les données que sur instruction de l'acheteur public ;
  - faire intervenir des personnes soumises à une obligation légale et appropriée de confidentialité et ayant reçu une formation adaptée ;
  - prendre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ;
  - détruire ou renvoyer sans copie toutes les données personnelles soumises au traitement ;
  - conseiller et assister (techniques et/ou opérationnels) le fournisseur dans le cadre d'une demande d'exercice des droits des personnes concernées (droit d'information, droit d'accès, de rectification, d'effacement, d'opposition, etc.) ;
- à la notification des violations de données à caractère personnel auprès de l'acheteur public et/ou de la Cnil ;
- à l'établissement des éléments de preuves de conformité au règlement européen (notamment par le biais d'un code de conduite ou d'un mécanisme de certification adopté par le fournisseur) ;

- à l'encadrement de la sous-traitance des activités de traitement par le fournisseur titulaire du marché ;
- aux sanctions en cas de non-respect des dispositions liées à la protection des données personnelles.

En outre, l'acheteur public devra veiller à ce qu'en sa qualité de sous-traitant, le titulaire respecte ses propres obligations au regard du RGPD.

A noter

Par la suite, ces clauses pourront être remplacées par les clauses types, comme le prévoit l'article 28 du règlement européen, et devraient faire l'objet d'une modification des CCAG. En outre, la Cnil a publié un guide élaborant les principales clauses à prévoir dans un contrat présentant des données à caractère personnel (*cf.* Clauses types relatives à la protection des données [Réf. Internet : dtou8121]).

Pour accompagner les collectivités territoriales dans leur mise en conformité au RGPD, la Cnil a élaboré un *Guide de sensibilisation au RGPD*. Ce guide insiste sur la responsabilisation de **tous les acteurs** impliqués dans un traitement de données personnelles, en y incluant les **sous-traitants**. En effet, les marchés publics conclus avec des sous-traitants doivent comprendre les clauses obligatoires prévues par le RGPD (art. 28).

Pour les marchés en cours avant le 25 mai 2018, des avenants doivent procéder à l'ajout de ces clauses. Il est recommandé aux acheteurs publics d'insérer dans leurs contrats publics les clauses adéquates en se référant au clausier type élaboré par la Cnil dans le guide *Règlement européen sur la protection des données personnelles : guide du sous-traitant*.

Étape 4

Connaître les risques en cas de non-conformité

La non-conformité, totale ou partielle, au règlement européen le 25 mai 2018 peut faire l'objet d'un engagement de la responsabilité administrative du maître d'ouvrage, mais également de sanctions administratives par la Cnil.

En cas de non-respect du RGPD, l'acheteur public et le sous-traitant risquent chacun au titre de leur manquement respectif une amende administrative, étant précisé qu'ils seront solidairement responsables du dommage causé par le traitement vis-à-vis de la personne concernée.

A noter

Le marché public doit contenir des sanctions contractuelles spécifiquement liées au non-respect par le titulaire de ses obligations RGPD, telles que des pénalités et/ou la possibilité de résilier unilatéralement le marché pour faute du titulaire.

Le responsable de traitement peut faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement. Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement ;

- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

Les amendes administratives peuvent s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, à 2 % et jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Notre conseil

Maître d'ouvrage

Pensez à prévoir des avenants si votre marché n'est pas en adéquation. Le maître d'ouvrage doit mettre en place des garanties dès le lancement du marché. Concernant les contrats antérieurs au 25 mai 2018, la conclusion d'un avenant est obligatoire si la convention n'est pas en adéquation avec le texte.

En effet, l'article 5.2.2 de tous les CCAG prévoit qu'en cas d'évolution de la législation sur la protection des données à caractère personnel, en cours d'exécution du marché, les modifications éventuelles demandées par le pouvoir adjudicateur, afin de se conformer aux règles nouvelles, donnent lieu à la passation d'un avenant par les parties au marché.

Réalisez une cartographie des données sensibles. Afin de pouvoir déterminer les marchés concernés par le RGPD, il est conseillé de cartographier, avant le lancement de la passation, les données susceptibles d'être détenues par le titulaire. En effet, il est essentiel que le maître d'ouvrage adapte le dispositif en fonction de la prestation attendue et des éléments concernés.

Maître d'œuvre

Veillez au respect des obligations liées à la protection des données. Les entreprises titulaires de contrats de la commande publique sont elles-mêmes détentrices de données personnelles soit de leurs clients et interlocuteurs habituels (personnes physiques), soit au titre du périmètre des prestations objet du contrat impliquant le traitement d'un certain nombre de données personnelles.

Vous devez également veiller, comme les acheteurs, à faire respecter les obligations liées à la protection des données de la part de vos personnels, de vos sous-traitants et ainsi de suite, pour tous les détenteurs de ces données.

Élaborez un registre des traitements. En tant que « sous-traitant » (au sens du RGPD), vous devez tenir un registre des catégories d'activités de traitement que vous effectuez pour le compte de vos clients.

Ce registre doit être tenu par écrit et contenir :

- le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données ;
- le nom et les coordonnées de chaque sous-traitant ultérieur, le cas échéant ;
- le nom et les coordonnées du délégué à la protection des données, le cas échéant ;
- les catégories de traitements effectués pour le compte de chaque client ;
- les transferts de données hors Union européenne que vous effectuez pour le compte de vos clients, le cas échéant ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place.

Intégrer le RGPD dans les clauses du marché

Évitez les erreurs

Maître d'ouvrage

N'oubliez pas de vous assurer de la capacité de chaque acteur de la construction. Ainsi, vous devez vous assurer auprès des différents acteurs de la construction que les objets interconnectés, utilisés dans la gestion technique du bâtiment (chauffage, éclairage, climatisation, utilisation de l'énergie…), sont en capacité technique de respecter la protection des données personnelles et de recevoir le consentement de l'usager (RGPD, consid. 32).

N'oubliez pas d'intégrer le RGPD dans vos clauses d'exécution. Le non-respect des dispositions relatives au RGPD peut être sanctionné. Pensez à prévoir une clause d'exécution type, par exemple : « *tout manquement aux mesures relatives au règlement général sur la protection des données sera susceptible d'entraîner des sanctions, voire la résiliation du marché* », ainsi que des pénalités.

Foire aux questions

Quel impact le RGPD a-t-il sur la sous-traitance (au sens de la commande publique) ?

La Direction des affaires juridiques de Bercy a mis en ligne un DC4 et une notice explicative prenant en compte le RGPD entré en application le 25 mai 2018 (ces documents sont par ailleurs régulièrement mis à jour par la DAJ).

Ce DC4 comporte une nouvelle rubrique relative au traitement de données à caractère personnel : cette rubrique doit être remplie lorsque le sous-traitant se voit confier le traitement de données à caractère personnel.

En application du 2 de l'article 28 du RGPD, l'acheteur doit donner au titulaire son autorisation écrite préalable, spécifique ou générale, au recrutement d'un sous-traitant (au sens de la commande publique) lorsque ce dernier est chargé de traitements de données à caractère personnel. En cas d'autorisation générale, le titulaire doit informer l'acheteur de tout ajout ou remplacement de sous-traitants afin que celui-ci ait la possibilité d'émettre des objections à l'encontre des sous-traitants présentés.

Que l'autorisation donnée soit générale ou spécifique, le titulaire et son sous-traitant renseignent dans cette rubrique les activités de traitement de données à caractère personnel sous-traitées et notamment l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées.

Le soumissionnaire ou titulaire coche les deux cases déclaratives (de manière cumulative) qui ont pour but de lui rappeler qu'il lui appartient de s'assurer, d'une part, que son sous-traitant présente des garanties suffisantes pour la mise en œuvre de mesures techniques et organisationnelles propres à assurer la protection des données personnelles et, d'autre part, que le sous-traité intègre les clauses obligatoires prévues par l'article 28 du RGPD. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant l'acheteur de l'exécution par le sous-traitant de ses obligations.

Quel est le rôle du délégué à la protection des données ?

Depuis le 25 mai 2018, les collectivités territoriales doivent désigner un délégué à la protection des données qui a pour missions :

- d'informer et de conseiller le responsable de traitement de la collectivité ;

- de diffuser une culture « informatique et libertés » au sein de la collectivité ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller la collectivité sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec la Cnil et d'être le point de contact de celle-ci.

Pour aller + loin

Références juridiques

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit « règlement général sur la protection des données » (RGPD), articles 4 et 28
- Code de la commande publique, article L. 2193-2
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Délibération n° 2005-003 du 13 janvier 2005 décidant la dispense de déclaration des traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics (décision de dispense de déclaration n° 3)

Site Internet

www.cnil.fr : site de la Cnil, rubriques Médiathèque > Guide, où consulter notamment :

- *Guide de sensibilisation au RGPD pour les collectivités territoriales*, septembre 2019
- *Règlement européen sur la protection des données personnelles : guide du sous-traitant*, septembre 2017

@ Les plus Internet

Saisissez la Référence Internet **11313** *dans le moteur de recherche du site www.weka.fr pour accéder aux mises à jour de cette fiche ainsi que la Réf. Internet des rubriques suivantes :*

Outil téléchargeable

- **dtou8121 –** Clauses types relatives à la protection des données

Fiches associées

- **9344** – Imposer l'option A du CCAG prestations intellectuelles
- **9345** – Imposer l'option B du CCAG prestations intellectuelles

NOTES

WEKA .media .jobs .fr

Pour en savoir plus sur l'actualité de WEKA, nos expertises, les dernières innovations et toutes nos activités, visitez :

weka-service-public.fr

Contactez-nous relation.clientele@weka.fr | 01 53 35 17 17 À votre écoute du lundi au vendredi, de 9h à 18h

WEKA

Éditions WEKA
Immeuble Pleyad 1,
39 Boulevard Ornano,
93200 Saint-Denis

@EditionsWeka
@Weka_france
@editions-weka

WEKA .media .jobs .fr

WWW.WEKA.FR

Éditeur : Julien Prévotaux

Éditions WEKA - Pleyad 1 - 39, boulevard Ornano 93288 Saint-Denis Cedex
Tél. : 01 53 35 17 17 - Fax : 01 53 35 17 01 - Site internet : www.weka.fr