Commande publique :
quel est l'acteur responsable au regard du RGPD ?

17 mai 2024

Animé par :

Jean-Philippe SOUYRIS
Avocat à la Cour
Chef du pôle Data

jpsouyris@haas-avocats.com
01 85 73 15 49
www.haas-avocats.com

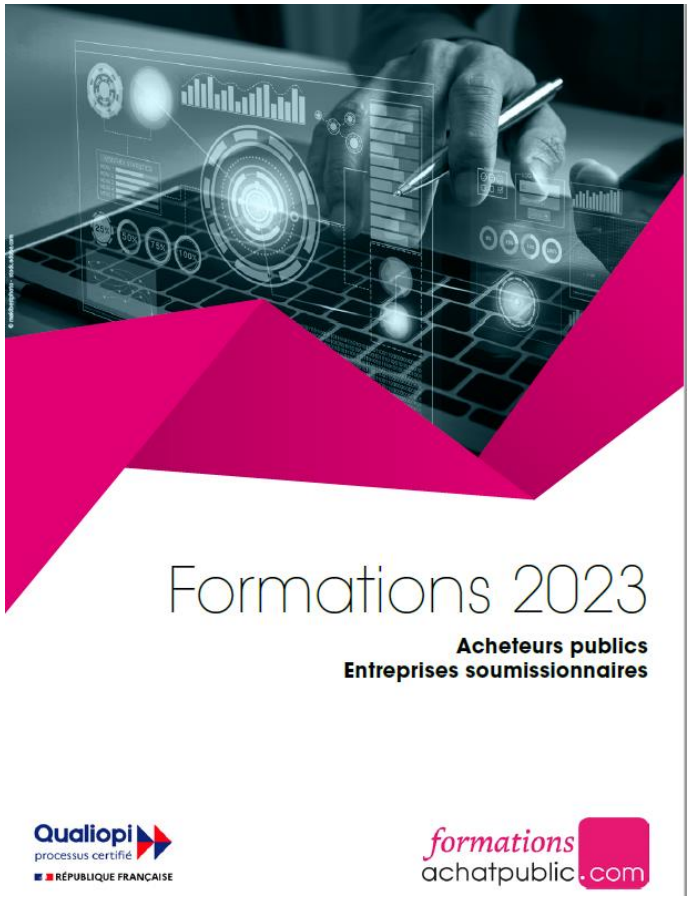
Un webinaire organisé par :

formations achatpublic.com

Les formations achatpublic.com

formations.achatpublic.com

Les formations aux marchés publics achatpublic.com délivre des formations pour les acheteurs publics et les entreprises soumissionnaires.
Ce sont plus de 50 programmes et 600 sessions programmées à Paris et en province en 2023.
Notre organisme est certifié Qualiopi.



La formation associée au thème d'aujourd'hui

FORMATIONS INTER

APPLIQUER LE RGPD DANS VOS PROCESSUS D'ACHATS PUBLICS | MMP92

Respecter la réglementation dans ses procédures de marchés publics

https://evenements.infopro-digital.com/achatpublic-public/

LE CABINET HAAS AVOCATS

Notre expertise :

- Droit de l'internet, de la data et cybersécurité
- Droit des nouvelles technologies, de l'informatique et de la communication
- Droit de la propriété intellectuelle
- Droit des affaires numériques

Nos dernières publications :

- Ouvrages juridiques (« Le RGPD expliqué à mon boss », « Le Guide juridique du RGPD », « Sécuriser les données personnelles »)
- Livres blancs (« RGPD & Marketplaces », « RGPD et DPO », « RGPD et secteur privé »)
- Site internet dédié (https://www.haas-avocats.com)

Le **Cabinet Haas Avocats** est membre du Réseau International d'Avocats indépendants GESICA, qui compte plus de 2 200 avocats et plus 250 cabinets.

LE CABINET HAAS AVOCATS

haas AVOCATS
Le droit l'humain la technologie

DROIT DES NOUVELLES TECHNOLOGIES / IT

- RGPD
- DPO
- Contrats Informatiques
- Chartes Informatiques
- Cybersécurité
- Sobriété numérique
- Green Tech
- E-santé
- Formations juridiques
- Legal Design

DROIT DU E-COMMERCE ET DES PLATEFORMES

- Audit juridique
- CGV/U, Mentions légales
- E-commerce
- Dropshipping
- Marketplace
- Due diligence IT
- Plateformes
- Logistique
- Economie circulaire
- Formations juridiques
- Legal Design

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE

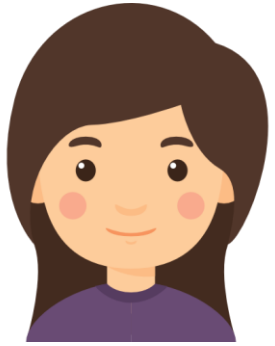
- Marque
- Dessins & modèles
- Droit d'auteur / logiciel
- IA / Bases de données
- Droit à l'image
- Savoir-faire
- Audit juridique
- Due diligence IP
- Franchise
- Formations Juridiques
- Legal Design

DROIT DES AFFAIRES ET DU NUMERIQUE

- Contentieux
- Concurrence
- E-réputation /droit de la presse
- Droit des affaires
- Fintech / Blockchain /NFT
- RSE Compliance
- Formations juridiques
- Legal Design

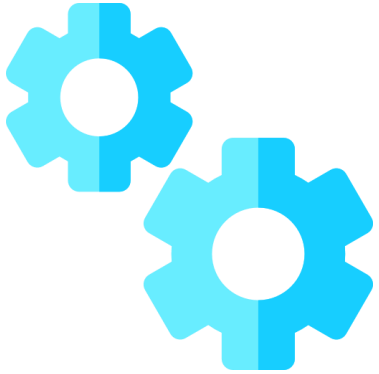
Sommaire

DONNEE PERSONNELLE & TRAITEMENT



Donnée personnelle

Toute information relative à une personne physique identifiée ou qui peut être identifiée, **directement** ou **indirectement**



Traitement de données

Toute opération ou tout ensemble d'opérations, automatisés ou non, portant sur de telles données, quel que soit le procédé utilisé

LE RESPONSABLE DE TRAITEMENT

Responsable de traitement

Le **responsable du traitement** est 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.

Le pouvoir adjudicateur (acheteur ou concédant) définit la « nature et l'étendue de ses besoins », il sera le plus souvent amené à déterminer les finalités et moyens du traitement.

LES **CO-RESPONSABLES DE TRAITEMENT**

Co-responsables de traitement

Lorsque plusieurs entités de traitement participent conjointement à la détermination des finalités et des moyens d'une opération de traitement, elles sont considérées comme « responsables conjoints du traitement »

En pratique, les acheteurs publics peuvent être co-responsables de traitement en cas d'achats mutualisés impliquant une détermination commune des finalités et moyens d'un traitement.

LE SOUS-TRAITANT

Sous-traitant

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 de traitement

En pratique, le sous-traitant est le plus souvent le titulaire du marché : dès lors qu'il exécute, dans le cadre de son contrat, un traitement de données personnelles préalablement déterminé par l'autorité contractante.

Attention : Ne pas confondre le « sous-traitant » au sens du RGPD avec le « sous-traitant » au sens de la commande publique.

LE SOUS-TRAITANT ULTERIEUR

Sous-traitant ultérieur

Le sous-traitant peut lui-même avoir recours à un **sous-traitant ultérieur** pour mener des activités de traitement spécifiques pour le compte du responsable du traitement.

Si un sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le **sous-traitant initial demeure pleinement responsable** devant le responsable du traitement de l'exécution par le sous-traitant ultérieur de ses obligations.

Attention : Le recours du titulaire du contrat de la commande publique à un sous-traitant ne signifie pas que ce dernier sera « sous-traitant ultérieur » au sens du RGPD.

Sommaire

INTEGRER LE RGPD A CHAQUE ETAPE DE LA COMMANDE PUBLIQUE

QUI EST RESPONSABILITE DE L'ENCADREMENT CONTRACTUEL?

edpb
European Data Protection Board

Tant le responsable du traitement que le sous-traitant sont chargés de veiller à ce qu'un contrat ou un autre acte juridique régisse le traitement

Les contrats entre les responsables du traitement et les sous-traitants peuvent parfois être rédigés unilatéralement par l'une des parties

CNIL.

La CNIL a récemment sanctionné un éditeur de logiciels de laboratoire considéré comme sous traitant au sens de la protection des données. Parmi les manquements sanctionnés: le manquement à l'obligation d'encadrer par un acte juridique formalisé les traitements effectués pour le compte du responsable de traitement (article 28 du RGPD)

QUID DES CCAG ?

Les **CCAG** entrés en vigueur le 1er avril 2021 intègrent un article dédié à la protection des données à caractère personnel.

Cette « clause RGPD », commune à tous les CCAG, offre un cadre général rappelant les obligations essentielles des parties en termes de protection des données personnelles.

Attention : il s'agit d'un **simple cadre de référence**, qui ne doit pas dispenser les acheteurs d'une réflexion spécifique à chaque marché sur le traitement de données.

QUALIFICATION DES ACTEURS

Définir les qualifications de l'acheteur et du prestataire : responsable du traitement, co-responsable du traitement, sous-traitant ?

Les qualifications reposent sur des considérations factuelles et non contractuelles.

Approche du faisceau d'indices par l'analyse du rôle de chacun

Se référer aux définitions du RGPD et aux lignes directrices par le Comité Européen de la Protection des Données (CEPD) et la Commission Nationale Informatique et Libertés (CNIL).

INTEGRER LE RGPD A CHAQUE ETAPE DE LA COMMANDE PUBLIQUE

PENDANT LA PHASE DE RÉDACTION DU MARCHÉ PUBLIC

L'objectif du contrat doit être de définir le rôle et les responsabilités de chacun des co-contractants.

Le contrat devra impérativement inclure les mentions obligatoires listées aux **articles 26 ou 28.3 du RGPD**, en les déclinant pour la situation particulière du marché.

Selon l'article 5.2 des CCAG, les documents particuliers du marché devront les modalités de respect par le titulaire de différentes obligations en matière de protection des données

Sommaire

RISQUES EN MATIERE DE RESPONSABILITE

- **Responsabilités**

- Une source de nouvelles fautes contractuelles pour le titulaire en cas de manquements à ses obligations relatives à la protection des données : **pénalités** prévues par les documents particuliers du marché et/ou **résiliation du marché pour faute** (**art. 5.2.3 CCAG**)

- Des obligations de contrôle de l'autorité contractante sur son cocontractant, dès l'attribution du marché et durant toute l'exécution du contrat (**art. 28§1 RGPD**)

- Une obligation de réparation des manquements subis par toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD (**art. 82 RGPD**)

- Une action de groupe en matière de protection des données personnelles (**Loi Informatique et libertés, art. 37**)

- **Responsabilité pénale**

- Risque de poursuites pénales en cas d'atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques. (**C. pén., art. 226-16 à 226-24**)

CONTRÔLE DE LA CNIL

En cas de méconnaissance du droit des données personnelles, le responsable de traitement et son sous-traitant sont **collectivement responsables devant la CNIL**.

La CNIL est dotée d'importants pouvoirs de sanction :

Ces sanctions peuvent être rendues publiques.

Sanction de la CNIL le 27 janvier 2021 d'un responsable de traitement et de son sous-traitant à la suite de violations de données liées à des attaques par bourrages d'identifiants (*credential stuffing*) en raison de l'insuffisance des mesures de sécurité mises en place.

Sommaire

REGULARISER LES CONTRATS EN COURS

Tous les contrats de la commande publique doivent nécessairement être **mis en conformité avec le droit des données personnelles** :

- conclusion d'avenants pour les marchés conclus avant le 25 mai 2018 (date d'entrée en vigueur du RGPD)

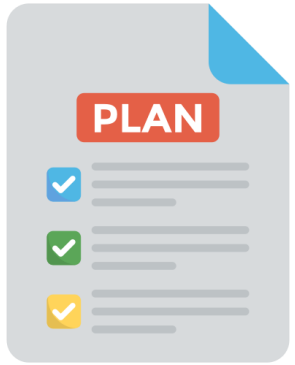
- en cas d'évolution de la réglementation sur la protection des données en cours d'exécution du marché, l'acheteur peut modifier unilatéralement le marché pour se conformer à la réglementation en vigueur en l'absence d'accord des parties (**art. 5.2.2 CCAG**)

ADAPTER LES CLAUSES CONTRACTUELLES

- Ne pas se reposer sur un « clausier RGPD » type : **adapter les clauses au contexte spécifique de chaque marché**, en tenant compte de l'objet du marché, des caractéristiques du traitement de données et des compétences du titulaire

AUDIT DES SOUS TRAITANTS - ANTICIPER PLAN D'AUDIT

Le responsable de traitement doit assurer le contrôle de ses sous-traitants en mettant en œuvre un plan d'audit :



- Périodicité et typologie des audits
- Plan d'audit
- Courrier de préavis
- Grille d'audit
- Suivi du rapport d'audit

BONNES PRATIQUES

PREPARER LA DOCUMENTATION

Responsable de traitement

- Mesures techniques et organisationnelles
- garanties des sous-traitants
- règles de sécurité proportionnées et documentées
- questionnaires préalables à l'audit

Sous-traitant

- *Accountability* du responsable de traitement
- Plan Assurance Sécurité
- Analyses d'impact
- Instructions formalisées du responsable de traitement

L'ENJEU DES CLAUSES D'AUDIT

Enjeu des clauses d'audit

Responsable de traitement

- Audit des procédures et de la documentation
- Coûts de l'audit
- Délai de remédiation et conséquences
- Coopération du sous-traitant avec l'auditeur

Sous-traitant

- Nombre d'audits et préavis raisonnable
- Auditeur diligenté
- Engagement de confidentialité
- Encadrer techniquement l'audit

LE CABINET HAAS AVOCATS ET LA PROTECTION DES DONNEES

Démarche de mise en conformité

- Diagnostic de l'existant
- Registre des traitements
- Notes de conformité juridique
- Analyses d'impact

Externalisation DPO

- Actualisation du registre
- Gestion droits des personnes
- Relations avec la CNIL
- Gestion des violations de données

Définition de politique contractuelle

- Contrats clients / contrats sous traitants
- Politique de Confidentialité
- Charte Cookies
- Référentiel sécurité

Merci de votre attention

Besoin d'aller plus loin ?

formations achatpublic.com

https://evenements.infopro-digital.com/achatpublic-public/

Jean-Philippe SOUYRIS
Avocat à la Cour
Chef du pôle Data

jpsouyris@haas-avocats.com
01 85 73 15 49
www.haas-avocats.com