Commande publique

16 octobre 2018
Veille juridique

Bienvenue au cahier des clauses simplifiées de cybersécurité

Dans le cadre du mois européen de la cybersécurité, le cahier des clauses simplifiées de cybersécurité a été approuvé par un arrêté en date du 18 septembre 2018. Ce nouvel instrument contractuel a pour vocation d'instaurer un cadre de sécurisation des systèmes d'information et données qui y sont associées. Il concerne aussi bien des marchés ayant pour objet principal les technologies de l'information et de la communication que des marchés de fournitures ou services, ou même encore le simple échange d'informations par messagerie électronique.

Cet arrêté permet aux administrations de bénéficier d'un clausier type en matière de cybersécurité et aux entreprises d'être au fait de leurs obligations y afférentes. Ces obligations s'imposent aux titulaires des marchés publics ainsi qu'à leurs sous-traitants. Toutefois, tous les contrôles et les éventuelles actions de remédiation en cas de défaut (y compris jusqu'au remplacement), même menés par les sous-traitants, sont à la charge des titulaires selon l'article 8 de ce cahier des clauses simplifiées.

Point sur les différentes obligations :

Tout d'abord, aux termes de l'article 2 de ce cahier des clauses simplifiées, les candidats et titulaires sont tenus de respecter les prescriptions des politiques de sécurité des systèmes d'information (PSSI) des pouvoirs adjudicateurs, dès lors que ces politiques ont été publiées avant la contractualisation des marchés, *a fortiori* si elles sont fournies au cours de l'appel d'offres.

En sus, durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants. De même, lors de l'appel d'offres ou en cours de marché, l'acheteur peut également demander aux candidats de présenter tous labels et certificats afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché.

Ensuite, l'article 4.3 affirme que dans tous les cas, un titulaire de marché est tenu de fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données des bénéficiaires et aux démonstrations du respect de leurs obligations par les bénéficiaires du marché. Et, si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre « Sécurité » du mode d'emploi.

Les articles 5 et 6 imposent quant à eux deux obligations, d'une part, de mise à jour des composants logiciel afin de maintenir le niveau de sécurité et, d'autre part, d'information des événements et changements impactant la sécurité (annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel) par la mise à disposition d'un système d'information (flux RSS ou liste de diffusion par courriel).

Enfin, si l'article 10 prévoit la mise en place d'un comité consultatif de règlement des litiges, l'article 11 vient obliger le titulaire du marché à s'aligner sur les standards et référentiels concernant les services qu'il propose, utilise ou met à disposition. Ainsi, pour les interfaces web, les services de courriels, les appareils connectés,

les sauvegardes de données et l'administration de systèmes d'information, les référentiels à retenir sont résumés ci-après et détaillés dans les textes techniques publiés sur le portail de l'Économie, des finances, de l'action et des comptes publics.

Puisque la sécurisation des systèmes informatiques dépend de l’évolution des technologies, il est par ailleurs prévu, qu’à première demande, le candidat ou titulaire devra fournir la preuve de la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures afin de permettre aux administrations d’être rassurées sur le niveau de cybersécurité dont elles bénéficient.