Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 28 – Novembre 2016

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°28 Novembre 2016

Risque d'ingérence dans le cadre du suivi de l'exécution des marchés publics étrangers

L'exécution des marchés publics en dehors du territoire national fait souvent l'objet d'un contrôle étroit de la part des pouvoirs adjudicateurs étrangers. En effet, les entreprises prestataires d'organismes publics se voient régulièrement imposer un grand nombre d'obligations pouvant conduire à la captation par les autorités étrangères d'informations sensibles de nature technique et commerciale.

Cas n°1 : Une surveillance étendue de l'exécution des marchés publics.

Les réglementations en matière de marché public peuvent ainsi imposer aux prestataires des personnes publiques de soumettre des rapports réguliers sur l'état d'avancement de leurs travaux. Plus intrusifs, certains contrats prévoient également la possibilité pour les autorités adjudicatrices de mener des inspections au sein des installations de leurs prestataires. Plusieurs entreprises françaises opérant dans des domaines sensibles ont ainsi fait l'objet d'inspections en présence d'individus liés à un gouvernement étranger.

Enfin, des audits financiers auprès des entreprises cocontractantes et de leurs sous-traitants, sont spécifiquement prévus dans certaines situations, notamment dans le cadre des contrats à coût variable pour lesquels le coût de la prestation n'est pas défini au moment de la conclusion du contrat1.

Lors du contrôle de l'exécution des marchés publics, les autorités adjudicatrices peuvent ainsi accéder à un grand nombre d'informations relatives aux entreprises prestataires et à leur activité.

Cas n°2 : Des obligations renforcées en matière de marchés publics sensibles

Les entreprises participant à des marchés publics sensibles se voient généralement imposer des obligations renforcées en matière de contrôle, notamment du fait des informations critiques qu'elles peuvent être amenées à détenir.

[1] L'objectif est officiellement d'éviter des abus dans la fixation du prix par le prestataire.

Plusieurs entreprises françaises se sont ainsi dernièrement vu imposer par des autorités adjudicatrices le respect d'une norme nationale étrangère de sécurité des systèmes d'information. Elles ne sont alors plus libres du choix des mesures de sécurité à adopter et doivent supporter le coût d'une telle mise en conformité. Des audits par les autorités adjudicatrices peuvent également être prévus pour vérifier la mise en conformité avec ce type de norme.

Les entreprises prestataires de ces autorités adjudicatrices peuvent également être obligées de signaler tout incident de sécurité visant des systèmes contenant des informations sensibles. Ce signalement doit généralement être accompagné d'éléments de preuves et d'un rapport technique détaillé. Les autorités adjudicatrices peuvent, en outre, se réserver la possibilité d'accéder à toutes les informations ou équipements détenus par leurs cocontractants qui seraient nécessaires à l'analyse de cet incident de sécurité.

Au travers de ces mesures de sécurité renforcées, les gouvernements étrangers bénéficient ainsi d'un accès élargi à des supports (ordinateurs, serveurs, etc.) contenant un grand nombre de données appartenant aux entreprises.

Commentaires

Au motif de vérifier la bonne exécution de leurs marchés publics, les autorités adjudicatrices sont en mesure de collecter de manière incidente des données sensibles appartenant aux entreprises françaises telles que :

- les données relatives aux technologies et savoir-faire de l'entreprise ;
- les données relatives aux marchés en cours (chiffrage des appels d'offres) et perspectives commerciales ;
- les données relatives aux clients, fournisseurs et distributeurs ;
- des données relatives aux vulnérabilités de l'entreprise (organisation, personne, etc.).

En pratique, ces données pourraient ensuite être transmises aux concurrents étrangers des entreprises françaises ou encore être instrumentalisées par les autorités régulatrices à des fins protectionnistes (rejet de demande d'autorisation, interdiction d'accès aux marchés, taxation, etc.).

Préconisations de la DGSI

Avant de se porter candidates à un marché public, les entreprises doivent intégrer les risques liés à ces réglementations ainsi que les surcoûts induits par leur mise en œuvre. L'impact économique de ces dernières (mise en conformité technique, risque d'amende sur le fondement d'une loi étrangère, risque de contentieux à l'étranger, fuite d'information vers des concurrents étrangers, annulation du contrat, interdiction de toute participation à un appel d'offres public, etc.) doit ainsi être comparé aux bénéfices escomptés sur le long terme par l'entreprise et, le cas échéant, provisionné.

Au regard de l'importance des risques identifiés, la DGSI recommande également aux entreprises d'adopter toutes mesures permettant de limiter le risque de fuite d'information dans le cadre du suivi de l'exécution des marchés publics, telles que :

- Prévenir leur point de contact au sein de la DGSI dès la connaissance d'un audit ;
- Strictement compartimenter les réseaux de l'entreprise afin d'empêcher les autorités de contrôle d'accéder à des données relatives à d'autres contrats ou projets ainsi qu'aux secrets de fabrication et autres savoir-faire ;
- Privilégier, dans le cadre des inspections et audits, la consultation en direct des systèmes d'informations, de préférence dans une pièce dédiée, sur un matériel fourni par l'audité ;
- Imposer la présence de l'officier sécurité de l'entreprise et d'un administrateur réseau lors de la réalisation des opérations de contrôle ;
- S'assurer que l'audit est réalisé dans le strict respect des clauses prévues par le contrat en associant étroitement l'équipe juridique de l'entité auditée ;
- Veiller à l'interdiction de l'installation de logiciels ou l'exécution de scripts présentés comme nécessaires à l'audit ;
- Assurer le traçage des opérations réalisées afin de prévenir tout abus.