

Marchés publics et grands comptes : répondre aux exigences cyber

Questionnaires sécurité, clauses RGPD, plans d'assurance : les exigences numériques des donneurs d'ordres deviennent éliminatoires. S'y préparer une fois, gagner à chaque fois.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/exigences-cyber-marches

Le questionnaire de 60 questions sécurité au milieu de l'appel d'offres, la clause RGPD de 8 pages, l'attestation d'assurance cyber exigée : les donneurs d'ordres — publics comme privés — répercutent leurs propres obligations (NIS2, RGPD, secteurs régulés) sur leurs fournisseurs. Pour la PME, c'est une barrière... ou un avantage : la plupart des concurrents répondent mal. Préparer une fois le « dossier cyber commercial », c'est transformer la contrainte en arme de sélection.

1. Ce qui est demandé, en pratique

- Le questionnaire sécurité : MFA, sauvegardes, chiffrement, gestion des accès et des incidents, sensibilisation — nos fondamentaux, sous forme de cases à cocher
- Les preuves RGPD : registre, DPA signable, localisation des données, mentions — surtout si la prestation touche aux données du client
- Les assurances : RC pro et de plus en plus cyber, avec attestations
- Les certifications, selon l'ambition du marché : labels accessibles (ExpertCyber...) jusqu'à ISO 27001 pour les marchés exigeants
- Dans le public : le RGPD s'applique via les clauses (CCAG, annexes), l'hébergement des données sensibles peut exiger des qualifications (SecNumCloud pour certaines données publiques), et la dématérialisation impose ses propres outils (profils d'acheteurs, signature électronique)

2. Le « dossier cyber commercial » : préparer une fois

- Une politique de sécurité d'une à deux pages : vos mesures réelles, en langage clair — le document qui répond à 80 % des questionnaires
- Le kit de preuves : attestations d'assurance, DPA type, fiches de tests de sauvegarde, attestation de sensibilisation, résultats d'audit (la synthèse, pas le détail des failles !)
- La FAQ interne des questions récurrentes avec les réponses validées : chaque questionnaire rempli enrichit la base — le troisième se remplit en une heure
- Le régime des écarts : pour chaque « non » actuel, la réponse honnête « planifié pour T2 » avec le plan — les acheteurs préfèrent la trajectoire sincère au « oui » invérifiable
- Ce dossier vit avec la documentation et se met à jour aux mêmes rituels

ATTENTION

Ne jamais surcocher : le questionnaire commercial devient contractuel — le « oui » à « chiffrez-vous les données au repos ? » non tenu se transforme en faute contractuelle le jour de l'incident, avec l'assureur du client en face (même mécanique que le questionnaire d'assurance). La règle : on coche ce qu'on fait, on planifie ce qu'on fera, on négocie ce qu'on ne fera pas.

3. Répondre efficacement à un questionnaire

- Qualifier d'abord : le questionnaire de 200 questions pour un marché à 10 k€ mérite une discussion avec l'acheteur — souvent une version allégée existe pour les PME
- Répondre depuis la base, adapter à la marge : la cohérence entre vos réponses successives compte (les acheteurs comparent)
- Impliquer le prestataire IT pour les questions techniques pointues — prévoir ce support dans son contrat
- Transformer l'exercice : chaque question sans bonne réponse est un item priorisé de votre feuille de route — le client vous paie presque votre audit

4. En faire un avantage offensif

- Afficher la posture avant qu'on la demande : la page « sécurité & confidentialité » du site, la mention dans les propositions — le différenciant que vos concurrents n'ont pas
- Anticiper la marche suivante : les exigences ne font que monter (NIS2 ruisselle) — le fournisseur prêt AVANT la vague récupère les marchés de ceux qui la subissent
- Viser les labels au bon moment : quand deux ou trois marchés visés les mentignent, le calcul devient simple
- Se souvenir que tout est vrai : cette préparation n'est pas du théâtre commercial — c'est votre vraie sécurité, qui protège aussi vos propres données au passage

L'essentiel à retenir

- 01 Rédiger la politique de sécurité commerciale (1-2 pages)
- 02 Constituer le kit de preuves (assurances, DPA, tests, audits)
- 03 Tenir la FAQ des questionnaires et capitaliser chaque réponse
- 04 Ne cocher que le réel, planifier les écarts honnêtement
- 05 Prévoir le support du prestataire IT dans les réponses
- 06 Afficher la posture sécurité dans l'offre commerciale

Questions fréquentes

Un petit sous-traitant peut-il négocier les clauses cyber d'un grand compte ?

Plus qu'on ne croit — sur le raisonnable : les délais de notification irréalistes (2 h !), les audits illimités à vos frais, les exigences sans rapport avec la prestation se discutent, surtout avec un plan sérieux en face. Ce qui ne se négocie pas : les fondamentaux (MFA, notification d'incident, DPA) — les demander est légitime, et vous devriez les avoir de toute façon.

Le client exige un audit de NOS systèmes. Jusqu'où accepter ?

Le principe est légitime (vous feriez pareil — voir notre guide fournisseurs) ; le cadre se négocie : périmètre limité à ce qui touche SA prestation, préavis, confidentialité des résultats, fréquence raisonnable, et l'alternative de la certification ou de l'attestation tierce qui évite l'audit direct. L'audit sauvage de tout votre SI par chaque client ne passe pas à l'échelle — les alternatives existent pour ça.

Ces exigences valent-elles pour les marchés de quelques milliers d'euros ?

De plus en plus, par ruissellement automatique des clausiers types — d'où des absurdités occasionnelles (le questionnaire bancaire pour une prestation de tonte). Répondez proportionné : votre politique d'une page + les attestations couvrent l'essentiel ; pour le reste, le dialogue avec l'acheteur ramène souvent l'exigence au niveau du marché. Et un refus d'exigence disproportionnée, documenté, est une réponse recevable.

Pour aller plus loin

ANSSI — NIS2 et la chaîne d'approvisionnement — cyber.gouv.fr/la-directive-nis-2

France Num — répondre aux marchés publics dématérialisés — www.francenum.gouv.fr

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr