HISCOX

Assurance Cyber
Questionnaire de souscription

Identification

Nom du proposant et forme juridique:

Adresse de la société :

Site(s) Web(s) :

Numéro BCE :

Vos activités :

Chiffre d'affaires

Montant du chiffre d'affaires réalisé :

Dernier exercice	Exercice en cours / prévisionnel	Exercice à venir
€	€	€

Taux de marge brute d'exploitation moyen sur les 3 dernières années : %

Part du chiffre d'affaires réalisée via des transactions en ligne ? %

Nombre d'employés :

Vos données

Nombre de personnes à propos desquelles vous êtes susceptibles de collecter et/ou détenir des données sensibles* :

* Données sensibles : 1. Numéro de sécurité sociale, permis de conduire ou passeport. 2. Données bancaire (carte de crédit, etc.) 3. Données relatives aux origines, à l'orientation sexuelle, à la santé, aux convictions religieuses ou philosophiques, aux opinions politiques, aux engagements syndicaux…

Nombre / Type			
< 20.000	☐	**500.001 - 1.000.000**	☐
20.000 - 100.000	☐	**1.000.001 - 6.000.000**	☐
100.001 - 250.000	☐	**> 6.000.000**	☐
250.001 - 500.000	☐		

Questions

Part de votre chiffre d'affaires annuel générée via export vers les USA/CANADA	%
Disposez-vous d'une filiale hors de l'Union européenne ? En cas de filiale(s) hors UE, précisez le(s) pays concerné(s) et leur part du chiffre d'affaires annuel total en pourcentage : …… …… ……	Oui ☐ Non ☐
La totalité des filiales du groupe utilise-t-elle le même système d'information ? Et ont-elles le même niveau de sécurité informatique que le souscripteur de la police ?	Oui ☐ Non ☐ Oui ☐ Non ☐

En cas de filiales, les réseaux de chacune sont-ils segmentés entre eux ? Si oui, comment ? …….. ……..	Oui ☐ Non ☐
Confirmez-vous ne pas utiliser de systèmes d'exploitation dont les mises à jour ne sont plus supportées par leur fabricant (par exemple Windows XP et Windows 7) ? **A défaut,** quel système d'exploitation utilisez-vous et expliquez comment il est segmenté du reste de votre réseau et d'Internet : …….	Oui ☐ Non ☐
Mettez-vous à jour les logiciels et les systèmes (y compris anti-virus et pare-feu) que vous utilisez dans les 30 jours suivants la mise à disposition de patchs par le fabricant ?	Oui ☐ Non ☐
Limitez-vous les privilèges administrateur aux seuls utilisateurs qui en ont besoin? **Et** Les administrateurs possèdent-ils tous deux comptes : un pour leurs missions d'administrateur et un pour les usages quotidiens ?	Oui ☐ Non ☐ Oui ☐ Non ☐
Restreignez-vous les accès de vos employés à votre système d'information et aux informations sur la base de ce dont ils ont besoin pour travailler ? Leurs accès sont-ils systématiquement coupés lorsque vos employés quittent votre entreprise ?	Oui ☐ Non ☐ Oui ☐ Non ☐
Avez-vous recours à la vérification en deux étapes* (A2F) pour gérer les accès à distance et/ou les accès à des applications web (par exemple, Gsuite ou Office 365) ? * Au-delà du nom d'utilisateur et du mot de passe, s'ajoute la réception d'un code de sécurité que seul l'utilisateur authentique pourra recevoir sur son téléphone, sa messagerie ou une application spécifique d'authentification.	Oui ☐ Non ☐
Les données que vous stockez sont-elles cryptées lorsqu'elles sont : - Sur votre réseau ? - Sur les périphériques de stockage mobiles ou terminaux mobiles ? - Sur les serveurs gérés par d'autres en votre nom ?	Oui ☐ Non ☐
Si vous avez déclaré plus de 100.000 à la question Vos données Les données sensibles* (cf. définition Page 1), sont-elles cryptées avec un cryptage d'au moins 256 bits lorsqu'elles sont sur votre réseau, y compris sur les périphériques de stockage, les appareils mobiles (y compris les ordinateurs portables et les téléphones intelligents), sur les serveurs et autres terminaux ?	Oui ☐ Non ☐
Si vous avez déclaré plus de 100.000 à la question Vos données Tous les employés ayant accès aux données sensibles que vous stockez ou traitez reçoivent-ils une formation et/ou un rappel au moins annuel sur la confidentialité des données et la cyber-sensibilisation ?	Oui ☐ Non ☐
Si vous acceptez les paiements par carte bancaire, êtes-vous conforme au standard PCI DSS 3.2 ou avez-vous recours à un fournisseur qui y est conforme ? Si vous ne savez pas, merci de préciser le nom de votre fournisseur : Iraiser / ingenico pas de coservation des données de CB ……. …….	Oui ☐ Non ☐
Avez-vous mis en place une politique de gestion des données personnelles et de sécurité informatique applicable à l'ensemble des services et filiales de l'entreprise ? Si vous avez obtenu une certification (par exemple, ISO 27001), merci de préciser laquelle/lesquelles :…….. ……..	Oui ☐ Non ☐

Si vous êtes dans l'obligation de le faire, avez-vous désigné un Délégué à la protection des données (Data Protection Officer DPO), en interne ou externe? ……	Oui ☐ Non ☐
Vos données et systèmes critiques* font-ils l'objet de sauvegardes hebdomadaires ? Cette sauvegarde prend-elle la forme: (a) ☐ d'au moins une sauvegarde physique maintenue déconnectée de vos systèmes à un moment donné et / ou (b) ☐ de l'une des solutions de sauvegarde basées sur le cloud suivantes: Microsoft OneDrive, Google Drive, iCloud ou Azure Recovery Services Vault. *Les données et systèmes critiques sont définis comme ceux dont l'indisponibilité ou le maintien hors ligne plus de 24 heures, engendreraient pour vous une perte de revenus. **A défaut :** Quelle est votre solution de sauvegarde ?..... Et à quelle fréquence la réalisez-vous ? ……..	Oui ☐ Non ☐
Avez-vous mis en place un plan régulièrement testé de reprise / de continuation d'activité en cas d'incident sur vos systèmes d'information ? Si, oui à quelle fréquence ce plan est-il testé ? Si oui , ce plan inclut-il les scénarios d'attaques par ransomware ?	Oui ☐ Non ☐ Oui ☐ Non ☐

Questions supplémentaires

Interruption de vos activités du fait d'un incident Informatique chez l'un de vos prestataires

En cas d'hébergement externalisé de vos données et systèmes critiques*, sont-ils hébergés par les prestataires suivants : AWS, Google, IBM, Alibaba, Salesforce, Microsoft, Oracle, ou OVH . **A défaut,** merci de préciser quels prestataires hébergent vos données et systèmes critiques :……	Oui ☐ Non ☐
En cas d'hébergement externalisé de données ou services, ces prestations sont-elles hébergées dans au moins deux data centers séparés d'au moins 350 km ?	Oui ☐ Non ☐
En dehors de l'hébergement, faites-vous appel à des prestataires informatiques externes ? Si oui qui et pour quelles prestations/missions ? ……..	Oui ☐ Non ☐
Faites-vous annuellement des audits de cyber-sécurité de vos prestataires informatiques ?	Oui ☐ Non ☐
Avez-vous externalisé certains de vos services auprès de prestataires tiers hors prestations informatiques ? Si oui, qui et pour quelles prestations/missions ? …….. Si oui, faites-vous annuellement des audits de cyber-sécurité chez ces prestataires ?……	Oui ☐ Non ☐ Oui ☐ Non ☐
Tous vos droits de recours sont-ils maintenus auprès de vos sous-traitants et prestataires ainsi que leurs assureurs ?	Oui ☐ Non ☐
Vos sous-traitants et prestataires sont-ils assurés contre les cyber-risques ?	Oui ☐ Non ☐

Questions spécifiques

Questions facultatives <u>sauf dans les cas suivants</u>:

- **chiffre d'affaires supérieur à 100 M€ et/ou ;**
- **activités dans le secteur des Technologies de l'informatique et/ou ;**
- **vous avez déclaré plus de 250 000 à la question Vos données.**

Qui est responsable de la politique des données personnelles et de leur sécurisation : ☐ a. Responsable IT ☐ b. Responsable de la sécurité ☐ c. CEO ou équivalent ☐ d. Autre (préciser) Quelle est l'expérience de ce dernier ?.....	
Pouvez-vous préciser votre stratégie de sauvegarde et plus précisément, comment : 1) vous protégez vos sauvegardes contre le chiffrement en cas d'attaque de ransomware? …… …… 2) vous protégez l'intégrité de vos sauvegardes considérant l'éventualité où les cyber-pirates infiltrent les SI durant 45 jours ? …… ……	
Quelle est la fréquence de vos tests des sauvegardes de vos systèmes ? …… Quand a été réalisé votre dernier test des sauvegardes de vos systèmes ? ……	
Précisez le type d'audits réalisés sur votre réseau : ☐ a. Test de vulnérabilité ☐ b. Test de pénétration ☐ c. Autre (préciser)	
Est-ce que ces audits sont réalisés par un prestataire externe ? Si oui, à quelle fréquence réalisez-vous ces audits : a. Annuellement b. A une fréquence plus élevée, précisez: c. Jamais	Oui ☐ Non ☐
Sous quels délais procédez-vous aux corrections s'avérant nécessaires suite à un audit de sécurité ? ……	
Avez-vous déployé des pare-feu pour réguler le trafic réseau ? ☐ a) Au périmètre du réseau ☐ b) Sur tous les systèmes informatiques et autres points d'extrémité ☐ c) WAF ☐ d) Aucun pare-feu n'est déployé	
Les données en transit sont-elles cryptées, y compris en cas d'utilisation d'un VPN pour les accès distants ?	Oui ☐ Non ☐
Avez-vous mis en place des mesures pour détecter toute attaque, tentative d'attaque ou incident ? Si oui, utilisez-vous l'un des systèmes d'analyse d'alerte suivants : ☐ a. SIEM ☐ b. In house SOC ☐ c. Managed SOC ☐ d. Autre (préciser)……	
Conservez-vous les fichiers logs et les informations liées à de potentielles attaques ? Si oui, pendant combien de temps sont-ils conservés ?	Oui ☐ Non ☐

Les correctifs et nouveaux codes sont-ils testés dans un environnement de test distinct avant déploiement dans l'environnement réel ?	

Cyber-Fraude

Existe-t-il une procédure de double signature pour les paiements supérieurs à 10.000 € ? Non ☐ une procédure de double signature est requise pour des paiements supérieurs à : …….. (précisez la somme) Non ☐ aucune procédure de double signature n'est jamais requise	Oui ☐ Non ☐
Confirmez-vous que les fonctions d'ordonnancement et de paiement sont séparées au sein de votre organisation ?	Oui ☐ Non ☐
Quels contrôles sont effectués sur les comptes de gestion pour vérifier que tous les paiements sont légitimes ? ……	
Confirmez-vous que lors d'un recrutement ou un changement de poste interne, impliquant l'exercice de fonctions de gestions de stocks, et/ou de comptabilité et/ou de gestion des approvisionnements, et/ou de gestion de trésorerie dont ordonnancement et paiement, vérifier les missions antérieures du candidat ou préposé, ainsi que ses références ? Et au terme du processus de recrutement externe ou interne pour ce type de fonctions, vérifiez-vous le casier judiciaire des préposés concernés ?	Oui ☐ Non ☐ Oui ☐ Non ☐

Combien de personnes au sein du groupe peuvent autoriser des transferts de fonds ?	
Quelles vérifications avez-vous mises en place pour ajouter, modifier ou supprimer un bénéficiaire de paiement ?	

Antécédents

Durant les 5 dernières années, avez-vous subi un sinistre d'un coût total supérieur à 1.500 euros (que celui-ci ait été indemnisé ou non) Si oui, précisez le montant, la date, les faits et mesures mises en place pour s'en prémunir à l'avenir …… ……	Oui ☐ Non ☐
Avez-vous fait l'objet d'une enquête de l' APD (ou son équivalent à l'étranger) ? Si oui, fournissez les détails :…….. ……	Oui ☐ Non ☐
Avez-vous connaissance d'événements ou circonstances pouvant donner lieu à la mise en jeu de la garantie ? Si oui, fournissez les détails :…….. ……	Oui ☐ Non ☐
Avez-vous déjà été assuré en cyber auprès d'Hiscox ou avez-vous demandé une proposition d'assurance au cours des trois derniers mois ?	Oui ☐ Non ☐

HISCOX

Assurance Cyber
Questionnaire de souscription

Assurance

Date de prise d'effet souhaitée : _____ Echéance souhaitée : _____

Déclaration

Je déclare que les explications et les informations figurant dans cette déclaration sont exactes et qu'aucun fait matériel n'est erroné.

J'accepte que cette déclaration et toute autre information communiquée servent de base au contrat d'assurance.

Je m'engage à informer les assureurs de toute modification matérielle des faits survenant avant l'échéance ou pendant la durée de validité du contrat d'assurance. Un fait matériel est un fait qui pourrait influencer l'acceptation ou l'évaluation du risque.

Je déclare également avoir pris connaissance des conditions générales applicables et en avoir compris la portée, les exclusions et les limitations.

Signature

Le soussigné déclare être habilité à représenter le preneur d'assurance, comme directeur, partenaire ou manager compétent.

_____

Fait à _____ le / /

Signature _____

Protection de la vie privée

Hiscox est une dénomination commerciale d'un certain nombre de sociétés Hiscox. La société spécifique qui agit en tant que responsable du traitement de vos données à caractère personnel est indiquée dans la documentation que nous vous remettons. En cas de doute, vous pouvez toujours nous contacter par téléphone au 0032 2 788 26 00 ou par e-mail à l'adresse dataprotectionofficer@hiscox.com. Nous collectons et traitons des informations vous concernant pour vous proposer des polices d'assurance et traiter des demandes d'indemnisation. Vos informations sont également utilisées à des fins professionnelles comme la prévention et la détection des fraudes, ainsi que la gestion financière. Il peut s'agir de partager vos informations avec / d'obtenir des informations vous concernant de la part des sociétés de notre Groupe et de tiers comme des courtiers, des gestionnaires de sinistres, des bureaux d'information de crédit, des prestataires de services, des conseillers professionnels, nos organes de contrôle ou les instances de prévention de la fraude. Il est possible que nous enregistrions des conversations téléphoniques pour nous permettre de surveiller les services que nous offrons et pour les améliorer. Pour plus d'informations concernant la manière dont vos informations sont utilisées et concernant vos droits liés à vos informations, veuillez consulter notre déclaration de protection de la vie privée sur le site Web www.hiscox.be.

□ J'autorise Hiscox à utiliser mes données comme décrit ci-dessus