QUESTIONNAIRE CYBER-RISQUES

SOUSCRIPTEUR

Dénomination sociale de la société proposante : .....

Adresse du siège social : .....

Code Postal :|__|__|__|__|__| Ville : .....

Numéro SIRET : ..... Code NAF : .....

E-mail : .....

Site Internet : .....

Date de création de l'entreprise : ..... Nombre d'employés : .....

Dénomination sociale et siège social de chaque filiale/succursale pour laquelle la couverture est requise : .....
.....
.....
.....

VOS ACTIVITES

Description des activités de la société proposante et de chacune de ses filiales/succursales : .....
.....
.....
.....
.....

INFORMATIONS FINANCIERES

Année	Effectifs	Chiffre d'affaires (€) (Honoraires & Commissions)	Ventilation du chiffre d'affaires		
			France	Monde entier hors USA / Canada	USA / Canada
N					
N - 1					
N - 2					

Part du chiffre d'affaires annuel représentant les ventes de produits et/ou services via un site Internet : ..... %

Part de transactions annuelles réglées par carte de paiement : ..... %

Valeur moyenne par transaction : .....

Budget annuel consacré pour la protection de ses systèmes informatiques et des données : .....

DONNEES PERSONNELLES

Nature des données personnelles utilisées / volume des données personnelles utilisées (en nombre d'enregistrements)

Nature des données / volumétrie	< 100	< 1 000	< 10 000	< 100 000	> 100 000
Comptes clients / Identité simple					
CRM : identité + données commerciales					
Moyens de paiement ou transactions financières					
Données médicales					
Autres					

Processus utilisant les données personnelles (cochez les cases qui correspondent à votre situation) :

☐ Prospection / mailing
☐ Gestion commerciale
☐ Conception
☐ Production
☐ Facturation
☐ Logistique
☐ Gestion financière
☐ Autres (à décrire) : .....

SECURITE RESEAU ET DONNEES

La société proposante et ses filiales disposent-elles d'un correspondant informatique et liberté et/ou d'un responsable de la protection des données ?
☐ **Oui** ☐ **Non**

La société proposante et/ou ses filiales stockent-elles, traitent-elles ou transmettent-elles sur leur système informatique les données suivantes ? (cochez les cases qui correspondent à votre situation)

☐ Informations carte de paiement
☐ Données personnelles clients
☐ Informations santé
☐ Informations financières
☐ Secrets commerciaux
☐ Actifs de la propriété intellectuelle

La société proposante et/ou ses filiales traitent-elles des paiements pour le compte de tiers, y compris transactions d'e-commerce ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales disposent-elles de procédures rigoureuses de révocation pour les comptes utilisateur et d'une procédure de récupération des données utilisées, mises en œuvre au moment de la cessation du contrat de travail ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales disposent-elles de logiciels antivirus mis à jour conformément aux recommandations des fournisseurs de ces logiciels sur l'ensemble des dispositifs informatiques, serveurs et réseaux ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales ont-elles mis en place des pare-feux et une détection de surveillance des intrusions pour prévenir et surveiller les accès non autorisés ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales ont-elles mis en place des procédures de contrôle d'accès et un cryptage des disques durs afin d'empêcher la divulgation non autorisée de données sur l'ensemble des ordinateurs portables, PDA, smartphones (ex. Blackberry) et PC utilisés à domicile ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales ont-elles configuré leur réseau afin de limiter l'accès aux données sensibles aux seules demandes autorisées ?
☐ **Oui** ☐ **Non**

Toutes les informations sensibles et confidentielles stockées dans les bases de données et serveurs de la société proposante et de ses filiales sont-elles cryptées ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales ont-elles mis en place une politique de conservation et de destruction des données ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales imposent-elles à leurs salariés des formations de sensibilisation à la protection des données personnelles et aux procédures de sécurité informatique ?
☐ **Oui** ☐ **Non**

Si « oui », veuillez décrire le format et la fréquence de ces formations : .....
.....
.....

SOUS-TRAITANCE

La société proposante et/ou ses filiales externalisent-elles une partie de leur réseau, de leur système informatique ou des fonctions de sécurité informatique suivantes : (cochez les cases qui correspondent à votre situation)

	Nom des fournisseurs de services
☐ Hébergement de données	
☐ Gestion de la sécurité	
☐ Traitement des données	
☐ Fourniture d'applications hébergées	
☐ Surveillance des systèmes d'alerte	
☐ Sauvegarde et stockage hors site	

La société proposante et ses filiales vérifient-elles que les systèmes informatiques des prestataires auprès desquels elles externalisent ces fonctions, ont des niveaux de sécurité et de performance suffisants ?
☐ **Oui** ☐ **Non**

Si « oui », veuillez indiquer la méthode de vérification : .....

INCIDENTS / GESTION DE CRISE

La société proposante et ses filiales ont-elles mis en place un plan de réponse aux incidents de sécurité en cas de violation de la sécurité ?
☐ **Oui** ☐ **Non**

Le plan de réponse de la société proposante et de ses filiales aux incidents de sécurité comporte-t-il des options de rechange destinées à prendre la relève de prestataires d'externalisation tiers dont elles dépendent ?
☐ **Oui** ☐ **Non**

La société proposante et ses filiales ont-elles identifié tous les cadres de réglementation et de conformité de leur industrie ?
☐ **Oui** ☐ **Non**

Veuillez fournir des informations détaillées sur les cadres de conformité suivants :

La société proposante et ses filiales sont-elles en conformité avec les règles de PCI (Payment Card Industry) ?
☐ **Oui** ☐ **Non**

Si « oui », un rapport de conformité a-t-il été rédigé par une société extérieure certifiée ?
☐ **Oui** ☐ **Non**

Si « oui » à quel niveau ?
☐ **1** ☐ **2** ☐ **3** ☐ **4**

La société proposante et ses filiales ont-elles élaboré un Plan de Continuité d'Activité (PCA) et un plan de reprise d'activité régulièrement testés ?
☐ **Oui** ☐ **Non**

Si « oui », décrivez brièvement ces plans : .....
.....
.....
.....

Délai estimé pour reprendre les activités après une attaque informatique ou autre perte / corruption de données :
☐ **12h au moins** ☐ **13-24h** ☐ **Plus de 24h**

Délai estimé après lequel l'incapacité du personnel à accéder aux systèmes informatiques aurait un impact significatif sur la société proposante ou sur ses filiales :
☐ **Immédiatement** ☐ **Après 6h** ☐ **Après 12h** ☐ **Après 24h** ☐ **Après 48h**

Délai estimé après lequel l'incapacité des clients à accéder au site web de la société proposante et/ou celui de ses filiales aurait un impact significatif sur leur activité :
☐ **Immédiatement** ☐ **Après 6h** ☐ **Après 12h** ☐ **Après 24h** ☐ **Après 48h**

ASSURANCE ANTERIEURES ET ANTECEDENTS

La société proposante et/ou l'une de ses filiales sont-t-elles ou ont-elles déjà été assurées pour les risques d'atteinte aux données[1] et/ou de cybercriminalité ?
☐ **Oui** ☐ **Non**

Si « oui », veuillez compléter le tableau suivant :

Période	Assureur	Montant de garantie	Franchise	Prime

Une demande d'assurance pour les risques d'atteintes aux données et/ou de cybercriminalité a-t-elle déjà été rejetée par une compagnie d'assurances ?
☐ **Oui** ☐ **Non**

La société proposante a-t-elle connaissance, après enquête, de faits ou d'événements et/ou de fautes susceptibles de mettre en jeu sa responsabilité civile et/ou celle de ses filiales et de déclencher une ou plusieurs garanties de la police d'assurance cyber-risques ?
☐ **Oui** ☐ **Non**

Si « oui », veuillez expliquer : .....
.....
.....

1 Atteinte aux données : toute divulgation ou transmission sans autorisation de données personnelles ou de données confidentielles collectées et conservées par ou pour le compte de la Société Proposante et/ou ses filiales (ci-après désignée « Atteinte aux données »)

La société proposante et/ou l'une de ses filiales et/ou leurs prestataires, partenaires passés et présents ont-ils fait l'objet d'une enquête de la CNIL ou de toute autre autorité équivalente à l'étranger fondée sur la réglementation relative aux données personnelles ?
☐ **Oui** ☐ **Non**

Au cours des cinq dernières années, la société proposante et/ou l'une de ses filiales ont-elles subi une panne, interruption ou suspension de leur système informatique pour tout motif (hors maintenance planifiée) d'une durée supérieure à 4 heures ?
☐ **Oui** ☐ **Non**

La société proposante et/ou l'une de ses filiales ont-elles déjà subi :

Une intrusion sur leur réseau	☐ **Oui**	☐ **Non**
Une falsification système significative ou importante	☐ **Oui**	☐ **Non**
Une violation intentionnelle de la sécurité informatique	☐ **Oui**	☐ **Non**
Des dégradations de réseau	☐ **Oui**	☐ **Non**
Une attaque virale ou par codes malveillants	☐ **Oui**	☐ **Non**
Une corruption de système	☐ **Oui**	☐ **Non**
Une perte ou vol de données	☐ **Oui**	☐ **Non**

Au cours des cinq dernières années, la société proposante a-t-elle eu connaissance, après enquête, de réclamations liées à une Atteinte aux données personnelles[2], amiables ou judiciaires faites à son encontre et/ou à l'encontre de l'une de ses filiales ?
☐ **Oui** ☐ **Non**

Au cours des cinq dernières années, la Société Proposante et/ou ses filiales ont-elles informé des personnes de l'existence d'une Atteinte aux données personnelles, réelle ou potentielle ?
☐ **Oui** ☐ **Non**

2 Atteinte aux données personnelles : toute divulgation ou transmission sans autorisation de données personnelles dont la Société Proposante et/ou ses filiales sont responsables en qualité de responsables de traitement

INFORMATIQUE ET LIBERTE

Je reconnais avoir été informé(e) conformément à l'article 27 de la Loi du 6 janvier 1978 du caractère obligatoire des réponses aux questions posées ci-dessus, ainsi que des conséquences qui pourraient résulter d'une omission ou d'une fausse déclaration prévues aux articles L 113-8 (nullité du contrat) et L 113-9 (réduction des indemnités) du Code des assurances.
J'autorise l'assureur à communiquer mes réponses à ses correspondants dans la mesure où cette transmission est nécessaire à la gestion et à l'exécution du contrat.
Je l'autorise également à utiliser mes réponses dans la mesure où elles sont nécessaires à la gestion et à l'exécution des autres contrats souscrits auprès de lui.
Je dispose d'un droit d'accès et de rectification auprès du correspondant du service clientèle pour toute information me concernant.

Toute omission, toute déclaration fausse ou inexacte pourrait entraîner la nullité du contrat ou vous exposer à supporter la charge de tout ou partie des indemnités dans les conditions prévues par les articles L. 112-3, L. 113-8 et L. 113-9 du Code des assurances.

SIGNATURE

Fait à : .....

Le : .....

Signature :

COMPLEMENT D'INFORMATION POUR L'ACTIVITE DE COMMERCE DE DETAIL

1. Décrivez la manière dont les données bancaires sont capturées et transférées au prestataire de solutions de paiement ?

.....
.....
.....

2. Les systèmes informatiques des points de vente sont-ils indépendants :

- Les uns des autres ? ☐ **Oui** ☐ **Non**
- Des autres systèmes informatiques du groupe ? ☐ **Oui** ☐ **Non**
- Des systèmes informatiques des autres entreprises du groupe ? ☐ **Oui** ☐ **Non**

3. Quelle technologie est utilisée pour le transfert de données bancaires des magasins vers les banques (réseau public, VPN, etc…)?

.....
.....
.....

4. Quels sont les moyens de protection des systèmes de paiements par carte ?

.....
.....
.....

5. La société proposante et/ou ses filiales disposent-elles de procédures de surveillance des systèmes informatiques des points de vente en ce qui concerne la détection de malware et la vérification de la « qualité logicielle » ?

☐ **Oui** ☐ **Non**

Si « oui », lesquels ?

.....
.....
.....

6. Les systèmes informatiques des points de vente disposent-ils de moyens de protection contre la malveillance informatique ? Oui Non ; si oui, lesquels ?

☐ **Oui** ☐ **Non**

Si « oui », lesquels ?

.....
.....
.....

7. Les logs des systèmes informatiques des points de vente sont-ils relevés et analysés régulièrement ?

☐ **Oui** ☐ **Non**

Si « oui », merci de préciser :

- La fréquence de ces analyses : .....
- La personne les effectuant : .....
- La personne en charge de la conservation des logs : .....

8. Lors de la modification d'un fichier sur les systèmes informatiques des points de vente, une alerte est-elle déclenchée en temps réel ?

☐ **Oui** ☐ **Non**

9. La société proposante et/ou ses filiales utilisent-elles des moyens de cryptage/chiffrement dans les systèmes informatiques des points de vente ?

☐ **Oui** ☐ **Non**

Si « oui », merci de préciser :
- Le type de cryptage ou chiffrement utilisé (chiffrement de bout en bout des données bancaires, etc…) : .....
.....
.....
.....

10. La société proposante et/ou ses filiales ont-elles recours à des inspections du trafic SSL ?

☐ **Oui** ☐ **Non**

11. Une autorisation formelle est-elle requise avant toute modification des systèmes informatiques des points de vente ?

☐ **Oui** ☐ **Non**

12. Lorsque les systèmes informatiques des points de vente sont fournis et administrés par un ou plusieurs prestataires extérieurs, quelles-sont les mesures de contrôle et d'audit de ces prestataires ?
.....
.....
.....

13. Quels sont les principaux prestataires SI utilisés par la société proposante et/ou ses filiales (notamment en ce qui concerne la gestion des terminaux de paiement) ?
.....
.....
.....

14. La société proposante et/ou ses filiales imposent-elles la souscription d'une police d'assurance Cyber à leurs prestataires SI ?

☐ **Oui** ☐ **Non**

Si « oui », quelle est la limite de garantie minimum imposée ?
.....
.....
.....

15. La société proposante renonce-t-elle à recours contre ses prestataires SI ?

☐ **Oui** ☐ **Non**