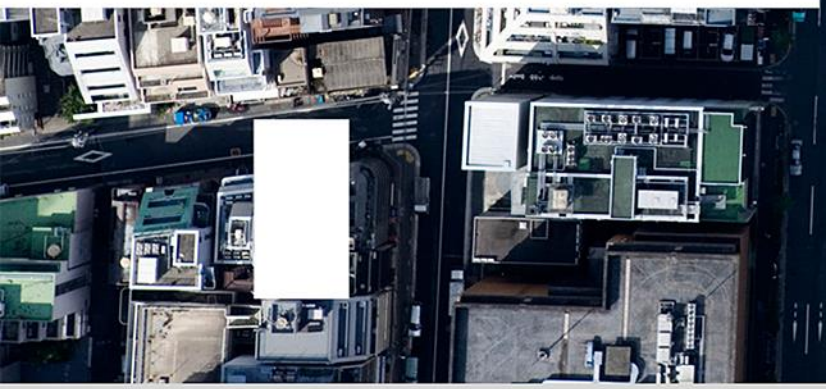
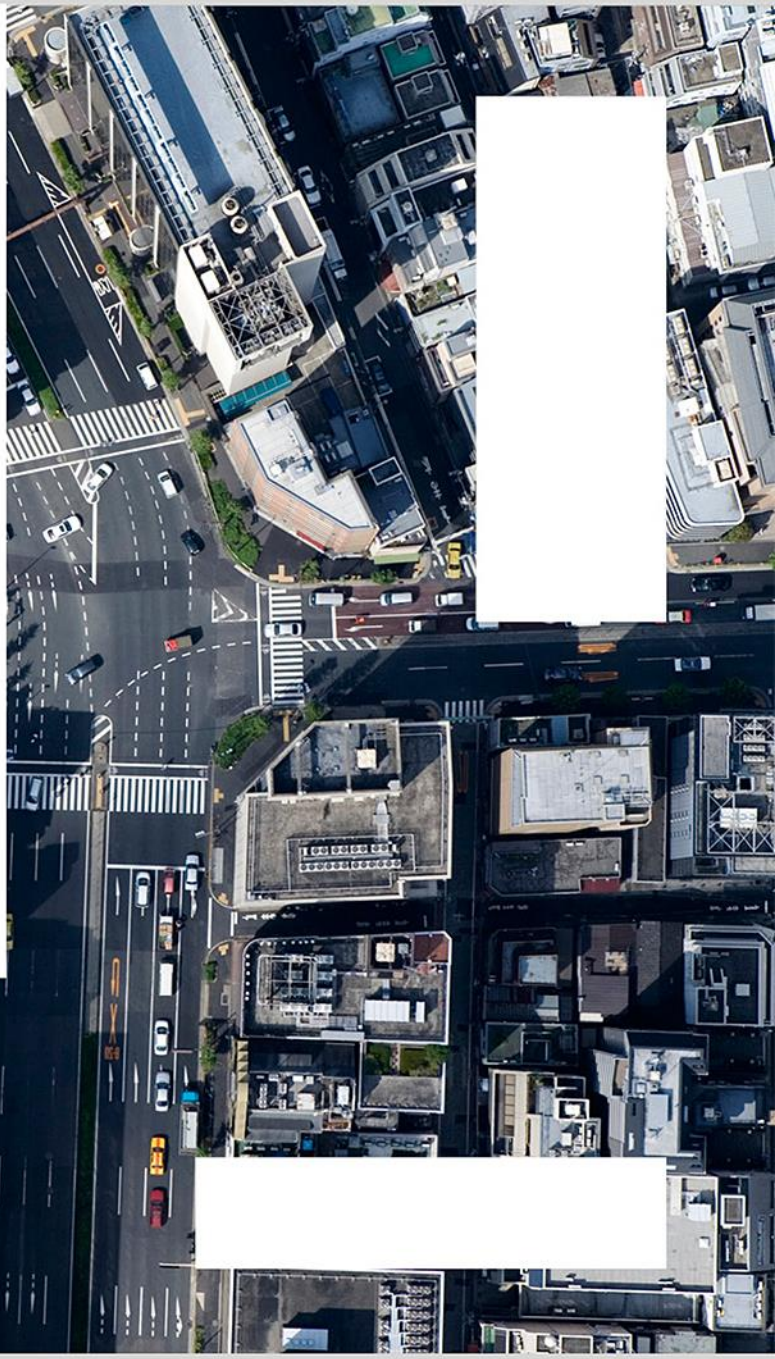
GRAS SAVOYE
Willis Towers Watson

Questionnaire de souscription

Cyber Risques





Ce questionnaire est destiné à permettre à Gras Savoye d'approcher les assureurs afin de vous faire parvenir des propositions d'assurance adaptées au profil de votre société.

Les informations communiquées dans ce questionnaire sont confidentielles.

1. INFORMATIONS GENERALES

- Raison sociale ou nom de la Société :

(*Ci-après désignée « le Souscripteur*)

- Adresse du Siège social :

- Date de création :
- Le souscripteur a-t-il une ou plusieurs filiales : OUI ☐ NON ☐

Si oui, joindre un organigramme (avec liens capitalistiques de détention)

- Forme juridique de la Société

☐ Société cotée
☐ Société non cotée
☐ Filiale d'une société cotée / non cotée
☐ Autres (organisme public, association à but non lucratif)

- Nombre d'employés :
- Dernier chiffre d'affaires (CA) annuel consolidé du souscripteur et de ses filiales :
- Part du CA réalisé aux USA/CANADA :
- Part du CA que représentent les ventes/activités en ligne :
- Part de transactions annuelles réglées par carte de paiement :
- Valeur moyenne par transaction
- Nom du site internet institutionnel du souscripteur :
- Nom du ou des sites internet de commerce en ligne :
- Activités :

2. LES DONNEES (TRAITEMENT, COLLECTE ET STOCKAGE) & SECURITE DE L'INFORMATION

2.1. Quel type de données à caractère personnel le souscripteur collecte, traite et/ou stocke-t-il ?

- Données relatives à des comptes bancaires ou de numéro de carte de crédit ☐
- Données commerciales et/ou stratégiques de vos clients ☐
- Données fiscales ☐
- Données médicales ☐
- Données relatives à la Propriété Intellectuelle/ secrets de fabrique ☐

2.2. Nombre de postes mobiles

☐ <100
☐ 101 – 1000
☐ >1000

2.3. Nombre de serveurs

☐ <100
☐ 101 – 1000
☐ >1000

2.4. Le souscripteur recense-t-il et/ou traite-t-il les données d'utilisateurs provenant de sources libres telles que des réseaux sociaux ou des sites de collecte de données marketing (ex : les sites permettant d'obtenir des réductions commerciales) ?

☐ Oui ☐ Non

2.5. Le souscripteur est-il en conformité avec les standards de sécurisation des données publiées par les institutions financières avec lesquelles il entretient des relations d'affaires (ex PCI-DSS) ?

☐ Oui ☐ Non

Si oui, lesquelles ?

2.6. Le souscripteur transmet il de manière transfrontalière des données à caractère personnel ?

☐ Oui ☐ Non

Si oui, dans quels pays ?

2.7. Les données sensibles et importantes sont-elles :

- Cryptées par le souscripteur ? ☐ Oui ☐ Non
- Sauvegardées quotidiennement par le souscripteur ? ☐ Oui ☐ Non
- Hébergées chez un tiers ? ☐ Oui ☐ Non

2.8. Le souscripteur a-t-il mis en place :

- Des procédures écrites sur la collecte, l'utilisation ou la diffusion des données à caractère personnel ?
  ☐ Oui ☐ Non
- Une politique de restriction d'accès aux informations personnelles et confidentielles aux seuls employés ou sous-traitants qui en ont exclusivement besoin dans le cadre de leurs fonctions ?
  ☐ Oui ☐ Non

2.9. Vous avez notifié à la CNIL du traitement des données personnelles réalisé dans le cadre de votre activité et vous avez obtenu son autorisation

☐ Oui ☐ Non

2.10. Volumétrie des données personnelles stockées (en nombre d'enregistrements)?

Nature des données / Volumétrie	< 100	< 1000	< 10 000	< 100 000	> 100 000
Comptes clients / Identité simple					
CRM : identité + données commerciales					
Moyens de paiement ou Transactions financières					
Données médicales					
Autres					

2.11. Processus utilisant les données personnelles *(Cochez les cases qui correspondent à votre situation)*

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

2.12. Les données personnelles sont-elles cryptées ?

- En transit : ☐ Oui ☐ Non
- En stockage : ☐ Oui ☐ Non

2.13. Mettez-vous en œuvre des mesures de sécurité plus strictes pour les données personnelles sensibles (Données bancaires PCI, données médicales PHI) ? ☐ Oui ☐ Non

2.14 Le personnel est-il sensibilisé à la sécurité informatique au moins une fois par année ? Cela inclut-il des exercices d'hameçonnage (phishing) ?

- Formation annuelle : ☐Oui ☐ Non
- Phishing Exercises : ☐Oui ☐ Non

2.15. Volumétrie des transactions par carte bancaire (le cas échéant) ?

2.16. Stockez-vous des informations de carte de paiement ? ☐ Oui ☐ Non

- Si la réponse est oui, vous conformez-vous à PCI-DSS ? ☐ Oui ☐ Non
- Si la réponse est non, votre fournisseur est-il agréé PCI--DSS ? ☐ Oui ☐ Non

2.17. Si vous utilisez des tiers pour héberger vos données, leur imposez-vous des règles de sécurité de l'information ou des règles de gestion de l'information ? ☐ Oui ☐ Non

2.18. En cas d'hébergement de données ou services externalisés, ces prestations sont elles hébergées dans au moins deux data centers séparés d'au moins 350 km ?
☐ Oui ☐ Non

2.19. Est-ce que vos sauvegardes sont conservées séparément de votre réseau (offline), ou dans un service cloud conçu à cet effet ? ☐ Oui ☐ Non

2.20. Utilisez-vous un service de synchronisation cloud (p. ex. Dropbox, OneDrive, SharePoint, Google Drive) pour les sauvegardes ? ☐ Oui ☐ Non

2.21. Avez-vous testé la restauration et la récupération réussies des configurations de serveurs clés et des données provenant de sauvegardes au cours des 6 derniers mois ? ☐ Oui ☐ Non

2.22. Êtes-vous en mesure de tester l'intégrité des sauvegardes avant la restauration pour être sûr qu'ils sont exempts de logiciels malveillants ? ☐ Oui ☐ Non

3. FORMATION ET CONNAISSANCE

3.1. Le souscripteur affiche-t-il et distribue-t-il les politiques et procédures informatiques à ses employés et sous-traitants ?

☐ Oui ☐ Non

3.2. Le souscripteur met-il en place des formations pour chaque salarié ou utilisateur des systèmes d'informations dédiés aux procédures de sécurité ou à la protection des systèmes ?

☐ Oui ☐ Non

3.3. Le règlement intérieur et/ou les contrats de travail imposent-t-ils une clause de respect de la confidentialité ?

☐ Oui ☐ Non

4. ENGAGEMENTS CONTRACTUELS

4.1. Le souscripteur

- Formalise-t-il toujours ses relations d'affaires par un contrat écrit ? ☐ Oui ☐ Non
- Insère-t-il dans ses contrats les clauses suivantes
  - Clauses limitatives de responsabilité ☐ Oui ☐ Non
  - Clauses d'exonération de la responsabilité ☐ Oui ☐ Non
  - Clauses de réserves de propriété ☐ Oui ☐ Non
  - Clause d'arbitrage ☐ Oui ☐ Non

4.2. Le souscripteur requiert-il toujours les services d'un avocat et/ou d'un service juridique pour vérifier et approuver tous les contrats, accords et autres documents marketing ?

☐ Oui ☐ Non

Veuillez détailler votre réponse :

4.3. Le souscripteur fait-il appel à des intérimaires ou à de sous-traitants ?

☐ Oui ☐ Non

Si oui, veuillez indiquer le pourcentage que cela représente par rapport aux salariés (par catégorie) :

4.4. Veuillez indiquer pour quelles missions le souscripteur fait appel à des sous-traitants *:*

- Traitement des paiements ☐ Oui ☐ Non
- Sécurité Informatique/ Protection des données ☐ Oui ☐ Non
- Infrastructure Informatique / Cloud Computing / Hébergement de données ☐ Oui ☐ Non
- Centre d'appel / Plate-forme de services ☐ Oui ☐ Non
- Processus opérationnels ☐ Oui ☐ Non
- Autres : préciser :

Si des processus relatifs à la sécurité informatique sont externalisés, veuillez lister ces entreprises ainsi que le type de service fournis :

4.5. Le Souscripteur et ses filiales vérifient-ils 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 :

4.6. Le souscripteur

- Accepte-t-il des clauses de renonciation à recours au bénéfice de ses sous-traitants ? ☐ Oui ☐ Non
- Exige-t-il de ses sous-traitants une attestation d'assurance en Responsabilité Civile ? ☐ Oui ☐ Non

5. RANSOMWARE PROTECTION

5.1. Filtrez-vous/scannez-vous les e-mails entrants pour les pièces jointes malveillantes et/ou les liens ?
☐ Oui ☐ Non

5.2. Votre programme de sensibilisation à la cybersécurité comprend-il une formation et des tests d'hameçonnage (phishing) ?
☐ Oui ☐ Non

5.3. Utilisez-vous Office 365 dans votre organisation ?
☐ Oui ☐ Non

Si Oui appliquez-vous l'authentification multifacteur pour tous les utilisateurs ?

☐ Oui ☐ Non

5.4. Utilisez-vous l'authentification multifacteur :

- Pour les comptes d'utilisateurs à haut privilège ? ☐ Oui ☐ Non
- Pour un accès à distance au réseau de votre organisation ? ☐ Oui ☐ Non

5.5. Avez-vous établi des processus d'application rapide de correctifs de sécurité critiques ?
☐ Oui ☐ Non

Sur les serveurs, les ordinateurs portables, les ordinateurs de bureau et les appareils mobiles gérés ?

☐ Oui ☐ Non

5.6. Acheminez-vous toutes les demandes Web entrantes via un proxy Web qui surveille et bloque le contenu potentiellement malveillant ?
☐ Oui ☐ Non

Si Oui quel service de proxy Web utilisez-vous :

5.7. Utilisez-vous un filtrage DNS (p. ex. Quad9, OpenDNS ou le secteur public PDNS)?
☐ Oui ☐ Non

5.8. Faites-vous des sauvegardes régulières (au moins mensuelles) des configurations et des données des serveurs clés ?
☐ Oui ☐ Non

5.9. Vos sauvegardes sont-elles stockées déconnectées et inaccessibles via le réseau de l'organisation ?
☐ Oui ☐ Non

5.10. Testez-vous la restauration et la récupération réussies des configurations et des données des serveurs clés à partir de sauvegardes ?
☐ Oui ☐ Non

5.11 Utilisez-vous un produit de protection de point de terminaison (PPE) dans l'ensemble de votre entreprise?
☐ Oui ☐ Non

6. BUSINESS INTERRUPTION

6.1. Faites-vous des copies de sauvegarde de toutes les données nécessaires à vos activités critiques ?
☐ Oui (Offsite) ☐ Oui (Onsite) ☐ Non

6.2. Avez-vous des solutions de secours pour toutes les missions critiques ?
☐ Oui (Alternate) ☐ Oui (Manual) ☐ Non

6.3. Si vous dépendez de Tiers (hébergeurs / Cloud services) pour des activités critiques, avez-vous des solutions alternatives en cas de défaillance ?
☐ Oui ☐ Non

6.4. Disposez-vous d'une architecture tolérante aux pannes pour les équipements critiques ?
☐ Oui ☐ Non

6.5. Avez-vous mis en place des process pour le remplacement des équipements ou réseaux obsolètes ?
☐ Oui ☐ Non

6.6. Un plan de réponse à une fuite de données personnelles est défini et communiqué au personnel concerné ?

☐ Oui ☐ Non

6.7. Le système informatique est composé de plusieurs réseaux informatiques indépendants permettant le maintien de tout ou partie de l'activité en cas de cyber attaques

☐ Oui ☐ Non

7. SECURITE RESEAU

7.1. Avez-vous une personne nommée responsable de la sécurité de l'information (p. ex. RSSI / CISO) ?
☐ Oui (interne) ☐Oui (externe) ☐ Non

7.2. Avez-vous un plan d'intervention en cas d'incident ou un autre processus pour traiter les incidents de cybersécurité ?

- Avoir un plan : ☐Oui ☐ Non
- Testé l'an dernier : ☐Oui ☐ Non

7.3. Utilisez-vous des Firewall ou autres outils en défense de périmètre Réseau ?
☐ Oui ☐ Non

7.4. Est-ce que tous les équipements sont équipés d'Antivirus ou autres outils de protection (EDR) ?
☐ Oui (EDR) ☐ Oui (AV uniquement) ☐ Non

7.5. À quelle fréquence les correctifs logiciels (patchs) sont-ils appliqués (y compris sur les systèmes critiques) ?

7.6. Avez-vous des systèmes essentiels à votre activité qui sont en fin de vie (EOL) ?
☐ Oui ☐ Non
Détails:

7.7. Votre réseau est-il segmenté / partitionné ? ☐ Oui ☐ Non

7.8. Avez-vous activé un MFA (Multi Factor Authentication) ? ☐ Oui ☐ Non

7.9. Quel pourcentage du budget informatique consacrez-vous à la sécurité ?

Détails:

8. GESTION DES RISQUES INFORMATIQUES

8.1. Une politique de Securité des SI est formalisée et approuvée par la direction et/ou des règles de sécurité SI sont définies et communiquées à l'ensemble du personnel et leurs représentants
□ Oui
□ Non

8.2. L'inventaire et la classification des systèmes d'information selon leur niveau de criticité ou de sensibilité, sont réalisés et des exigences de sécurité sont définies en conséquence
□ Oui
□ Non

8.3. Veuillez cocher les moyens de protections utilisés au sein du souscripteur :

- Contrôle accès réseau ☐
- Antivirus ☐
- Pare-feu ☐
- Détection d'intrusion ☐

8.4. En complément du pare-feu, le système informatique est équipé d'une Système de Détection d'Intrusion (IDS) qui analyse en temps réel le trafic sur le réseau ?

□ Oui □ Non

8.5. En complément des antivirus, les postes de travail sont tous équipés d'un outil de détection comportementale des fichiers téléchargés et de blocage des actions malveillantes (prévention des cryptolockers notamment)
□ Oui □ Non

8.6. Les équipements privés (ordinateurs, tablettes, smartphones appartenant aux collaborateurs) sont autorisés à être connectés au système informatique de l'entreprise
□ Oui □ Non

8.7. Le souscripteur dispose-t-il :

- D'un responsable de la sécurité informatique ou équivalent ? ☐ Oui ☐ Non
- D'une charte de sécurité informatique ? ☐ Oui ☐ Non
- D'un plan de réponse à un incident ? ☐ Oui ☐ Non
- D'un processus d'escalade en cas d'atteinte aux systèmes ? ☐ Oui ☐ Non
- D'un processus de traitement des plaintes des clients ? ☐ Oui ☐ Non

8. 8. Le souscripteur se met-il constamment à jour des règles et normes relatives à la protection de la vie privée qui gouvernent son domaine d'activité ?

☐ Oui ☐ Non

8.9. Le souscripteur a-t-il procédé à un audit de sécurité dans les 24 derniers mois ?

☐ Oui ☐ Non

Si oui, veuillez fournir les résultats de cet audit (résumé) :

8.10. Le souscripteur utilise-t-il les normes standards du marché pour gérer les contrôles de sécurité comme ISO 27000, CoBIT, etc?

☐ Oui ☐ Non

Si non, indiquez les normes utilisées et les raisons de ce choix :

8.11. Le souscripteur a-t-il des accords de niveau de service (SLA) avec les fournisseurs qui facilitent le contrôle et la résolution d'incident ainsi que la remontée d'information ?

☐ Oui ☐ Non

8.12. Le responsable de la conformité reporte-t-il directement à la direction de la société ?
☐ Oui ☐ Non

8.13. Le souscripteur permet-il des accès externes aux systèmes d'information aux membres du département informatique et à son personnel ?
☐ Oui ☐ Non
Si oui, veuillez détailler votre réponse sur les moyens utilisés pour sécuriser ces connexions :

8.14. Tous les réseaux sans fil du souscripteur sont-ils sécurisés ? ☐ Oui ☐ Non

8.15. Le souscripteur impose-t-il une politique de mot de passe renforcée au sein de l'entreprise ? (changement régulier, usage obligatoire de caractère alphanumérique et alphabétique, interdiction d'utiliser un mot de passe déjà utilisé, interdiction de divulguer son mot de passe pendant ses congés…) ?
☐ Oui ☐ Non

8.16. Existe-t-il une vérification régulière de la cohérence entre les droits d'accès et les besoins des utilisateurs dans le cadre de leurs fonctions ? ☐ Oui ☐ Non

8.17. Le souscripteur a-t-il :

- Mis en place des contrôles d'accès pour prévenir toute utilisation non autorisée des systèmes et/ou matériels portables ou amovibles ? ☐ Oui ☐ Non
- Une politique de classification de données ? ☐ Oui ☐ Non
- Mis en place une procédure de sauvegarde des données dans un lieu sécurisé différent des locaux principaux de l'activité de la société ? ☐ Oui ☐ Non

Veuillez préciser la périodicité des sauvegardes :

9. DEPENDANCE AUX SYSTEMES ET PLAN DE REPRISE D'ACTIVITE/ RESILIENCE

9.1. Le souscripteur dispose-t-il :

- D'un plan de reprise d'activité (PRA) ? ☐ Oui ☐ Non
- D'un plan de continuité d'activité (PCA) ? ☐ Oui ☐ Non

9.2. Les PRA et/ou PCA sont-ils testés annuellement ?
☐ Oui ☐ Non

9.3. Des mesures ont-elles été mises en place ? (type Site froid, Site chaud, Site de réplication continue…)?
☐ Oui ☐ Non

9.4. En cas de panne du système informatique, à combien estimez-vous la perte de revenue quotidienne ?

9.5. Veuillez estimer au bout de combien de temps la perte d'accès :

- Par les **employés** aux systèmes informatiques aurait un impact significatif sur l'activité de la société ?

Immédiatement ☐ Moins d'un jour ☐ Plus d'une journée ☐ Jamais ☐

- Par les **clients** aux systèmes informatiques aurait un impact significatif sur l'activité de la société ?

Immédiatement ☐ Moins d'un jour ☐ Plus d'une journée ☐ Jamais ☐

10. BILAN / POINT D'ETAPE RGPD

10.1. Avez-vous un Correspondant Informatique et Liberté et/ou un responsable de la protection des données (DPO)?

☐ Oui ☐ Non

10.2. Après l'entrée en vigueur du RGPD, où en êtes-vous par rapport à :

- L'inventaire des données personnelles et des traitements
- La gestion des réclamations
- La sous-traitance
- PIA, Security by design
- Gestion de crise

11. QUESTIONS RELATIVES A LA CRISE SANITAIRE LIEE AU COVID-19

11.1. Le client a-t-il mis en place des mesures particulières sur la période de la crise sanitaire (sensibilisation, accès à distance, patching à distance …) ? ☐ Oui ☐ Non

11.2. Des mesures de contrôle spécifiques ont-elles été mises en place pour le retour au bureau suite au dé confinement (contrôle hygiène du poste avant reconnexion au réseau …) ? ☐ Oui ☐ Non

11.3. Quel a été et quel est encore l'impact de l'épidémie de Covid-19 sur l'activité de l'assuré ? Est-ce qu'il est en mesure d'accomplir ces missions à un niveau d'exigence identique à celui antérieur à la crise ?

11.4. La procédure de contrôle préalable des clients de l'entreprise a-t-elle été sensiblement modifiée à la suite de l'épidémie de Covid-19 ? ☐ Oui ☐ Non

11.5. Quels changements le client a-t-il apportés à son plan de continuité des activités ? Et s'il n'en avait pas, a-t-il décidé d'en mettre un en place ?

11.6. Patch management : est-ce que les mises à jours concernant les vulnérabilités suivantes : Wannacry, Petya, Windows NTLM zero day, RDP, Citrix and Pulse Secure VPN ont-elles été réalisées ? ☐ Oui ☐ Non

11.7. Sensibilisation des salariés : est-ce qu'une communication appelant les salariés à être vigilants aux tentatives d'attaque par hameçonnage (phishing) a-t-elle été faite ? ☐ Oui ☐ Non

11.8. Télétravail : Les équipes de sécurité informatique peuvent-elles travailler à distance et sont-elles toujours mobilisées en cas de réponse à incidents ? ☐ Oui ☐ Non

11.9. Télétravail : Les salariés en télétravail utilisent-ils bien le réseau privé virtuel (VPN) fourni par l'assuré afin de sécuriser la communication entre le terminal et le système d'information de l'assuré ? ☐ Oui ☐ Non

12. SOLARWINDS ORION

12.1. Utilisez-vous actuellement une version de Solarwinds ORION vulnérable aux portes dérobées SUNBURST ou SUPERNOVA

□ Oui □ Non

12.2. Avez-vous déjà utilisé dans le passé une version de Solarwinds ORION vulnérable aux portes dérobées SUNBRUST ou SUPERNOVA

□ Oui □ Non

12.3. Quelles mesures avez-vous prises pour surveiller une potentielle activité malveillante sur votre système ?

□ L'arrêt et isolement des logiciels vulnérables ?

□ L'activité du système et les balayages de la mémoire pour déterminer les communications avec des IP non autorisés et les flux d'informations ?

12.4. Pouvez-vous confirmer qu'il n'y a aucune trace/ preuve d'activité malveillante résultant de cette vulnérabilité sur votre système ?

□ Oui □ Non

13. MICROSOFT EXCHANGE

13.1. La société proposante/ses filiales utilise-t-elle Microsoft Exchange Server sur site ou par l'intermédiaire d'une solution hybride ?

□ Oui □ Non

13.2. Si oui, la société proposante a-t-elle identifié les vulnérabilités ci-dessous sur les serveurs Exchange ?

□ CVE-2021-26855

□ CVE-2021-26857

□ CVE-2021-26858

□ CVE-2021-27065

13.3. Si OUI, la société proposante/ses filiales a-t-elle suivi les instructions de Microsoft pour mettre à jour/corriger cette vulnérabilité ?

□ Oui □ Non

13.4. La société proposante/ses filiales a-t-elle effectué une évaluation de compromission associée à cette vulnérabilité ?

□ Oui □ Non

13.5. La société proposante/ses filiales utilise-t-elle uniquement la solution Microsoft Exchange Online ?

□ Oui □ Non

12. SINISTRALITE

12.1. Le souscripteur a-t-il connaissance à ce jour de sinistres/réclamations/ faits ou circonstances relatifs à :

- La diffamation ☐ Oui ☐ Non
- L'atteinte au droit à la vie privée ☐ Oui ☐ Non
- La perte de données à caractère personnel ☐ Oui ☐ Non
- Un défaut de sécurité informatique ☐ Oui ☐ Non
- La violation de brevets, licences, droits d'auteurs de logiciels, commis par le souscripteur ou par une personne dont elle est responsable ☐ Oui ☐ Non

12.2. Le souscripteur a-t-il déjà fait l'objet d'enquêtes (CNIL ou autorités gouvernementales ou administratives indépendantes) ? ☐ Oui ☐ Non

Si oui, veuillez détailler votre réponse

13. INCIDENTS AU COURS DES TROIS DERNIERES ANNEES

13.1. Le souscripteur a-t-il été victime :

- D'intrusion réseau ? ☐ Oui ☐ Non
- D'attaque par déni de service ? ☐ Oui ☐ Non

Si oui, quelles en ont été les conséquences ?

13.2. Le souscripteur a-t-il été averti par un tiers que des données à caractère personnel ont été compromises à partir des systèmes du souscripteur ? ☐ Oui ☐ Non

13.3. Le souscripteur a-t-il déjà informé ses clients (procédure de notification) suite à la violation de la confidentialité des données à caractère personnel ? ☐ Oui ☐ Non

Le Souscripteur déclare :

- **Que les renseignements communiqués dans ce questionnaire sont exacts et qu'il n'a omis ou supprimé aucun fait.**
- **Avoir été informé que toute réticence ou fausse déclaration intentionnelles peut entraîner la nullité du contrat, si cette réticence ou fausse déclaration change l'objet du risque ou diminue l'opinion pour l'assureur (article 113-8 du code des assurances).**
- **S'engager à déclarer toutes circonstances nouvelles modifiant les déclarations faites dans le présent questionnaire et qui pourraient survenir entre ce jour et la date de prise d'effet de son contrat d'assurance**

Fait à

Le

Signature du représentant légal du souscripteur + cachet du souscripteur

Nom :

Fonction :

Signature :

GRAS SAVOYE
Willis Towers Watson

A propos du Groupe Willis Towers Watson

Willis Towers Watson (NASDAQ : WLTW) est une entreprise internationale de conseil, de courtage et de solutions logiciellesqui accompagne ses clients à travers le monde afin de transformerle risque en opportunité de croissance.
Willis Towers Watson compte 39 000 salariés dans plus de 120 pays.
Nous concevons et fournissons des solutions qui gèrent le risque, accompagnent les talents et optimisent les profits afin de protéger et de renforcer les organisations et les personnes. Notre vision, unique sur le marché, nous permet d'identifier les enjeux clés au croisement entre talents, actifs et idées: la formule qui stimule la performance de l'entreprise. Ensemble, nous libérons les potentiels.
Pour en savoir plus : www.willistowerswatson.com

GRAS SAVOYE, Société de courtage d'assurance et de réassurance
Siège Social : Immeuble Quai 33, 33/34 quai de Dion-Bouton, CS 70001, 92814 Puteaux Cedex.
Tél: 01414350 00. Télécopie: 01 414355 55. http://www.grassavoye.com.
Société par actions simplifiée au capital de 1 432 600 euros. 311 248 637 RCS Nanterre.
N° FR 61 311 248 637. Intermédiaire immatriculé à l'ORIAS sous le n° 07 001 707 (http://www.orias.fr).
Gras Savoye est soumis au contrôle de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution)
61 rue Taitbout 75436 Paris Cedex 9. © Gras Savoye Willis Towers Watson. Tous droits réservés.