CHARTE CYBERSECURITE EN NORMANDIE

DES PRESTATAIRES DE SERVICES INFORMATIQUES ET NUMERIQUES

Septembre 2019

Préambule

La présente charte est destinée aux prestataires de services informatiques et numériques, dont le siège ou au moins un établissement est situé en Normandie.

La transformation numérique de la société et, particulièrement, des entreprises engendre de légitimes préoccupations mais également de formidables opportunités de croissance. La captation illégale d'informations portant sur les savoirs, les savoir-faire, les procédés ou les innovations est une réalité qui concerne tous les secteurs d'activité, toutes les entités et toutes les fonctions d'une organisation. L'utilisation malveillante de l'espace numérique amplifie ces risques pour la plupart méconnus ou sous-estimés.

Cette charte s'inscrit dans une démarche destinée à réduire les risques numériques tant au niveau des prestataires que de leurs clients. Elle pourra faire l'objet d'évolutions validées par le comité de pilotage opérationnel et sera consultable dans sa dernière version sur le site internet mis en place par le comité de pilotage stratégique, constitué de la Région Normandie et de la Chambre de Commerce et d'Industrie de Normandie, avec le soutien de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

En effet, adopter un comportement vigilant et de bonnes pratiques en s'appuyant sur la puissance des systèmes d'information et des outils numériques est un levier essentiel qui peut contribuer au développement économique de la Normandie.

Article 1 – Fondement

La présente charte ne comporte aucune mesure coercitive, elle invite les prestataires qui souhaitent rejoindre cette initiative à se conformer aux principes qu'elle édicte, et ne se substitue pas aux dispositions légales et réglementaires existantes.

La charte est issue d'une démarche collaborative et volontaire de prestataires impliqués dans l'amélioration des pratiques et de la communication autour des risques numériques, avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de la Région Normandie, de la Chambre de Commerce et d'Industrie de Normandie (CCI Normandie), de Cap'Tronic, de Normandigital, de Normandy Web Xpert (NWX) et du Pôle TES.

Article 2. DEFINITIONS

Bonnes pratiques : ensemble de méthodes et de comportements qui font consensus et qui sont considérés comme indispensables, relevant d'une évidence non formalisée, de normes et de méthodes techniques, de textes réglementaires et figurant notamment dans des guides cités en référence.

Charte : document établissant l'ensemble des principes fondamentaux qui doivent être respectés par les signataires.

Client : entité bénéficiant des services proposés par les prestataires et mis en œuvre par les intervenants, dans le cadre d'une relation suivie et récurrente avec ces derniers.

Comité de pilotage opérationnel : groupe formé de membres choisis par les signataires de la Charte et renouvelé régulièrement. Il est chargé de veiller au bon fonctionnement et à l'évolution de cette dernière, d'apprécier les conditions de conformité de l'activité du prestataire avec les principes de la Charte et d'instruire les signalements de clients.

Cybersécurité : état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent

accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Intervenant : employé ou sous-traitant d'un prestataire réalisant une mission pour celui-ci.

Médiateur : personne désignée par le comité de pilotage opérationnel. Elle est chargée de vérifier la capacité d'engagements d'un demandeur ou de trouver une solution amiable en réponse à un signalement auprès du comité de pilotage et non résolu.

Prestataire : organisme proposant une offre de service.

Article 3. OBJET

Les prestataires signataires s'engagent à intégrer fondamentalement la sécurité du numérique et le renforcement de la protection des systèmes d'information dans leurs organisations, leurs processus et leurs relations avec leurs clients, afin de réduire les risques de cybermalveillances.

Les clients sont incités à adopter les bonnes pratiques et les recommandations formulées par les prestataires signataires à la Charte.

Article 4. PERIMETRE

Les principes promus par cette Charte ont vocation à l'être auprès de toutes les parties prenantes: clients, prestataires, sous-traitants et autres partenaires.

Cette Charte est mise en œuvre par les prestataires signataires qui s'engagent à en respecter les principes.

Article 5. CONDITIONS D'ENGAGEMENT

Chaque prestataire qui souhaite se prévaloir de la Charte devra adresser au comité de pilotage opérationnel motivée et appuyée des éléments nécessaires à l'appréciation du respect de la Charte.

Cette demande est ensuite instruite par le comité de pilotage opérationnel pour s'assurer de la conformité de l'activité du prestataire avec les principes de la Charte.

Le prestataire signifie par courrier avant le 31 janvier de chaque année son engagement à poursuivre le respect des principes de la Charte.

Article 6. ENGAGEMENTS DES MEMBRES

Les adhérents à la Charte s'engagent à :

- Respecter les bonnes pratiques professionnelles en termes de cybersécurité (techniques, juridiques, organisationnelles, communication, protection des données personnelles…) selon les recommandations de l'ANSSI et de la CNIL,
- Inciter les intervenants à respecter les engagements de la Charte,
- Informer et conseiller les clients et les inciter à adopter de bonnes pratiques numériques,
- Proposer aux clients de réaliser un état des lieux de leurs pratiques en matière de sécurité numérique,
- Permettre aux clients de formuler un avis sur la qualité de la prestation,
- Participer assidument aux échanges avec la communauté des adhérents de la présente Charte,
- Porter à la connaissance des autres adhérents toute information qu'il juge pertinente pour améliorer la connaissance et les moyens de lutte contre les risques numériques,
- Tenir informés ses clients des risques numériques et de leur prévention,
- Respecter les questions liées au secret et à la confidentialité,

- Intégrer dans toutes ses propositions techniques et commerciales un volet cybersécurité,
- Promouvoir la Charte, les guides et les recommandations de l'ANSSI et de la CNIL sur ses outils de communication.

Article 7. PREROGATIVES DES ADHERENTS

Tout signataire de la présente Charte est en droit de s'en prévaloir et de valoriser son engagement au regard de la cybersécurité.

Il bénéficie des échanges d'informations entre signataires, dont il peut faire profiter sa clientèle.

Article 8. CONTROLE ET SANCTIONS

Les clients ont la possibilité de faire part de leur niveau de satisfaction quant au respect des engagements du prestataire tels que définis à l'article 6.

Le prestataire est informé que tout signalement peut faire l'objet d'une instruction par le comité de pilotage opérationnel qui peut désigner un médiateur. Tout manquement à la présente Charte peut entrainer la radiation temporaire ou définitive de la liste des prestataires référencés.

Article 9. REFERENCES

- Guide d'élaboration en 8 points-clés d'une Charte d'utilisation des moyens informatiques et des outils numériques
- Guide des bonnes pratiques de l'informatique :
- Guide d'hygiène informatique
- Référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels
- CNIL–Guide LA SÉCURITÉ DES DONNÉES PERSONNELLES
- Flash INGERENCE n°33 publié par la DGSI – Mai 2017 - Lles risques cyber liés aux prestataires et aux sous-traitants
- La cybersécurité et l'Union Européenne

- Articles 323-1 à 323-7 du Code pénal, issus de la loi n°88-19 du 5 janvier 1988 et complétés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique «Des atteintes aux systèmes de traitement automatisé de données»
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n°2004-801 du 6 août 2004et par la LOI n°2016-1321 du 7 octobre 2016 et Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD)