CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

CHARTE D'ENGAGEMENT DES PRESTATAIRES INSCRITS SUR LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR V.2

1 – Description de la plateforme Cybermalveillance.gouv.fr et de la mise en relation entre les victimes d'actes de cybermalveillance et les prestataires inscrits.

La plateforme Cybermalveillance.gouv.fr est mise à disposition et opérée par le Groupement d'Intérêt Public « Actions contre la Cybermalveillance » (GIP ACYMA) afin de remplir les missions d'intérêt général du GIP :
- sensibiliser au risque numérique et aux bonnes pratiques de sécurité ;
- porter assistance aux victimes d'actes de cybermalveillance ;
- observer la menace numérique afin de mieux l'anticiper.

C'est dans ce cadre que la plateforme Cybermalveillance.gouv.fr inscrit des prestataires de service informatique basés sur le territoire français afin de proposer aux victimes une assistance technique de proximité.
Lorsqu'une victime vient chercher de l'assistance sur Cybermalveillance.gouv.fr, elle va tout d'abord se faire guider pour décrire le problème qu'elle a rencontré. L'aide au diagnostic apportée par le dispositif va permettre de lui proposer soit des conseils et informations de nature à lui permettre de résoudre son problème, soit une mise en relation avec des prestataires professionnels de proximité en mesure de l'assister.
Le prestataire qui assiste la victime le fait par le biais d'une prestation commerciale en dehors du dispositif qui facilite leur mise en relation. Leurs relations contractuelles sont inopposables au GIP ACYMA, ce dernier ne disposant d'aucun droit de regard sur le contenu des obligations souscrites par les parties.
L'inscription des prestataires ne leur garantit pas la contractualisation d'une prestation avec un client victime via la plateforme Cybermalveillance.gouv.fr.
En demandant à être inscrit sur la plateforme Cybermalveillance.gouv.fr, le prestataire accepte de respecter les règles énoncées dans la présente charte, et de s'inscrire ainsi dans la démarche globale de sensibilisation, d'assistance et d'observation du dispositif Cybermalveillance.gouv.fr.

2 – Processus d'inscription sur la plateforme Cybermalveillance.gouv.fr

L'inscription d'un prestataire sur la plateforme Cybermalveillance.gouv.fr se fait sur candidature du prestataire, examen de son dossier par le GIP ACYMA et acceptation de la Charte d'engagement par le prestataire, qui vaut acceptation de l'ensemble du processus et des règles de fonctionnement de la plateforme.

Le GIP ACYMA opérant la plateforme Cybermalveillance.gouv.fr a mis en place un processus et des règles d'inscription, de refus d'inscription ou de désinscription de la plateforme.

Seuls les prestataires répondant aux conditions fixées par la présente Charte et l'ayant acceptée peuvent être inscrits sur la plateforme.

Les prestataires qui demandent à être inscrits sur la plateforme Cybermalveillance.gouv.fr doivent proposer, parmi leurs prestations, une assistance technique sur a minima un domaine d'activité parmi la liste suivante :
- Applications Web
- Système d'exploitation
- Sauvegarde
- Objet connecté
- Équipement industriel
- Téléphonie fixe
- Équipement réseau ou de sécurité.

Cette liste peut être élargie en fonction des nécessités d'assistance évaluées par Cybermalveillance.gouv.fr.

L'inscription nécessite de fournir sous forme numérisée, dans l'espace de candidature du prestataire, les pièces et éléments d'informations suivants :

Informations administratives	- dénomination sociale et nom commercial du prestataire - adresse postale, numéro de téléphone, courriel de contact générique, valide et non filtré, adresse du site web (si existant) - forme juridique du prestataire, numéro de SIRET, code APE/NAF - carte nationale d'identité en cours de validité du responsable légal - extrait kbis de moins de 3 mois - justificatif d'assurance responsabilité civile professionnelle
Informations sur l'entreprise	- texte court de présentation de l'entreprise - logo de l'entreprise (si existant) - appartenance éventuelle à un groupement, une fédération ou un syndicat - typologies d'intervention du prestataire - rayon géographique d'intervention - types de clientèle traitée (particuliers, entreprises ou associations, collectivités territoriales)
Questionnaire de candidature	Réponse aux questions posées dans le formulaire de candidature, permettant de juger si le prestataire candidat a une bonne compréhension des compétences et pratiques requises pour répondre aux objectifs de la plateforme Cybermalveillance.gouv.fr
Signature	En validant son dossier d'inscription le prestataire confirme qu'il accepte l'ensemble des règles et processus décrits dans la Charte.

Le prestataire candidat à l'inscription reçoit un accusé de réception validant l'envoi de sa candidature. Le délai de traitement de cette candidature est au maximum de deux mois après la date de réception et court à partir de l'envoi de l'accusé de réception .

Si la demande d'inscription est jugée incomplète, le prestataire recevra en retour la liste des pièces et informations manquantes nécessaires au traitement de sa candidature. Il dispose alors d'un délai de quinze jours pour renvoyer les pièces, ce qui suspend le délai de traitement de la candidature .

En cas d'acceptation, le prestataire en sera informé par un courriel qui lui sera adressé dans un délai maximum de deux mois après réception de sa candidature (le cas échéant après demande de pièces et informations complémentaires). Il sera alors inscrit sur la plateforme Cybermalveillance.gouv.fr.

Le prestataire sera informé par voie postale ou électronique du refus de son inscription. L'absence de réponse

de la part du GIP ACYMA dans un délai de deux mois à compter de la date de l'accusé de réception de la demande d'inscription (le cas échéant ayant fait l'objet d'une suspension par l'effet d'une demande de pièces et informations complémentaires) équivaut à un refus d'inscription.

3 – Engagements du prestataire inscrit sur la plateforme Cybermalveillance.gouv.fr

a) Accueil des clients victimes d'actes de cybermalveillance et traitement de leurs demandes d'assistance

Le prestataire inscrit sur la plateforme Cybermalveillance.gouv.fr s'engage à réserver le meilleur accueil aux victimes (particuliers, entreprises ou collectivités locales) qui s'adressent à lui pour remédier à un incident de sécurité lié à une cybermalveillance. La qualité de cet accueil repose sur la courtoisie, le respect de la confidentialité, l'écoute des attentes de la victime, la clarté des réponses apportées, la pertinence et l'adéquation de l'offre commerciale, et le respect des délais annoncés.

Le prestataire s'engage à communiquer de façon précise et en des termes simples sur la nature des services proposés pour la réparation, le dépannage ou la réponse aux incidents.

Le prestataire s'engage à informer de façon claire et compréhensible sur ses compétences propres, détenues par lui ou ses employés, et sur les compétences extérieures qu'il peut solliciter en cas de besoin.
Le prestataire fournit à la victime, en amont de la prestation de remédiation, un diagnostic complet comportant une description du problème technique identifié et des opérations nécessaires à sa remédiation. Il complète ce diagnostic par un devis précisant les délais et tarifs nécessaires à la remise en état.

Dans le cas où le prestataire estime qu'un premier examen technique est nécessaire pour établir le devis, il informe le client des modalités de réalisation.

Le prestataire informe dès que possible le client de tout changement dans la durée prévisible de l'intervention, sa nature ou son coût final. Il doit s'assurer de l'accord écrit du client avant de poursuivre ses travaux d'investigation ou de remédiation.

D'une manière générale, le prestataire s'engage à réaliser les prestations d'assistance aux victimes qui l'ont sollicité dans le cadre de la plateforme Cybermalveillance.gouv.fr en parfaite conformité avec les règles de l'art et la réglementation applicable aux prestations de service fournies à des consommateurs ou à des professionnels. Il s'abstient de toute pratique commerciale illicite au regard notamment des dispositions du Code de la consommation, du Code de commerce et plus généralement de tout comportement ou pratique susceptible de violer une disposition légale de nature législative ou réglementaire, ou de contrevenir à une règle de bonne pratique professionnelle.

b) Conservation des traces utiles à la préservation de la preuve numérique en vue d'un dépôt de plainte

Le prestataire s'engage à prendre toutes les mesures adaptées afin de préserver les traces utiles pour les services de l'État chargés d'investigations numériques (services enquêteurs saisis d'un dépôt de plainte ou éléments communiqués à titre d'information judiciaire). Il conseille et oriente la victime pour qu'elle puisse déposer plainte lorsque cela est opportun.

Le prestataire s'informe des coordonnées des services de police ou de gendarmerie situés dans son périmètre d'intervention[1].

Conformément aux dispositions du code pénal (article 434-1) et dans les limites fixées par ledit article s'agissant des personnes astreintes au secret, lorsqu'il en a connaissance, le prestataire informe les autorités administratives ou judiciaires de tout crime dont il est encore possible de prévenir ou de limiter les effets ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés.

[1] Contacter une brigade de gendarmerie ou un commissariat de police ; porter plainte auprès du Procureur de la République.

c) Respect de la confidentialité de la victime et des données personnelles

Le prestataire s'engage à respecter la confidentialité de l'ensemble des données et renseignements donnés par son client, qu'il s'agisse de la sécurité des moyens de paiement ou des données à caractère personnel et confidentiel.

Il prend toutes les mesures raisonnables et nécessaires pour en assurer la protection.

Il veille au respect du Règlement Européen sur la Protection des Données (RGPD2) et s'assure en particulier du consentement de ses clients avant tout traitement de ses données.

Il met en place les mesures de sécurité nécessaires à la protection des données de ses clients. . Il ne transmet aucune information à des tiers non autorisés.

Le prestataire s'engage à ne pas utiliser les données personnelles et de contact des victimes d'actes de cybermalveillance en dehors de la prestation d'assistance découlant de la mise en relation effectuée sur la plateforme Cybermalveillance.gouv.fr, sauf à obtenir ensuite un consentement dans le cadre du RGPD en dehors de toute responsabilité de la plateforme Cybermalveillance.gouv.fr.

Tout manquement pourra entraîner une suspension ou un retrait du référencement sur Cybermalveillance.gouv.fr

d) Obligation de mise à jour régulière des informations administratives et juridiques relatives au prestataire inscrit

Le prestataire s'engage à communiquer au GIP ACYMA tout changement de responsable légal, de numéro de SIRET, d'adresse postale ou de messagerie, de type de prestation, de rayon d'intervention géographique ou toute autre information susceptible de faire évoluer les conditions dans lesquelles il est inscrit sur la plateforme Cybermalveillance.gouv.fr. Lorsqu'il reçoit une demande de mise à jour d'informations envoyée par la plateforme, il se met en conformité dans le délai demandé, faute de quoi il pourra être suspendu voire désinscrit de la plateforme.

4 – Remontées d'informations vers Cybermalveillance.gouv.fr et veille technologique

Le prestataire informe son client des missions du dispositif national Cybermalveillance.gouv.fr et de la possibilité qui lui est ouverte de transmettre des données opérationnelles anonymisées relatives aux cybermalveillances (par exemple un échantillon de virus informatique, une description des modes opératoires utilisés etc.). Cette communication se fait à travers l'outil de rapport d'intervention mis à disposition du prestataire depuis son espace privé sur la plateforme Cybermalveillance.gouv.fr.

Les éléments envoyés au dispositif permettent à l'ensemble des prestataires ainsi qu'aux services de l'État en charge de la prévention et de la répression des actes de cybermalveillance d'être le plus rapidement possible informés des nouvelles pratiques et techniques utilisées par les cyberdélinquants. Elle revêt une grande importance pour la collectivité nationale.

Les informations remontées par le prestataire demeurent confidentielles.

En tout état de cause, le prestataire veille à ne pas transmettre de données personnelles relatives à la victime. La victime peut s'opposer à cette transmission d'information.

5 – Envoi d'informations liées au statut de prestataire inscrit sur Cybermalveillance.gouv.fr

Les prestataires acceptent, en étant inscrits sur la plateforme Cybermalveillance, de recevoir périodiquement

[2]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, et abrogeant la directive 95/46/CE – Règlement Général sur la Protection des Données.

sur l'adresse courriel de contact enregistrée au moment de leur candidature, des contenus de formation et de sensibilisation nécessaires et pertinents pour leur activité d'assistance et de remédiation, et toute communication liée à leur statut de prestataire inscrit sur la plateforme.

Leur adresse courriel de contact ne sera pas communiquée à des tiers sans leur accord et sera supprimée de la base de données un an maximum après que leur inscription sur la plateforme soit révoquée.

6 – Règles applicables à la désinscription de la plateforme Cybermalveillance.gouv.fr

a) Désinscription à l'initiative du prestataire

La désinscription peut être réalisée sur demande du prestataire lui-même. Il peut demander au GIP ACYMA sa désinscription par courriel à l'adresse contact@cybermalveillance.gouv.fr ou par voie postale à l'adresse 6 rue Bouchardon 75010 Paris. Le GIP ACYMA désinscrit le prestataire de la plateforme dans un délai maximal d'un mois à compter de la réception de sa demande.

b) Suspension temporaire – désinscription définitive sur initiative du GIP ACYMA

Le GIP ACYMA se réserve le droit de procéder à la suspension temporaire du compte du prestataire voire à la désinscription définitive du prestataire en cas de manquement à ses obligations au titre de la présente charte, et notamment en cas d'absence de réponse à une demande de mise à jour des informations relatives à sa situation administrative ou de réclamations répétées de la part de victimes ayant recouru aux services dudit prestataire. Le GIP ACYMA se réserve le droit de désinscrire un prestataire toutes les fois que la situation administrative et professionnelle du prestataire a évolué de sorte qu'il ne répond plus aux conditions initialement fixées pour son inscription sur la plateforme de remédiation.

Lorsque le GIP ACYMA constate un manquement à la présente charte, il peut demander au prestataire de remédier sans tarder à ce manquement, et le suspendre provisoirement de son inscription sur la plateforme.
Si le manquement n'est pas résolu dans le délai demandé par le GIP ACYMA, alors le prestataire pourra faire l'objet d'une désinscription. La mesure de suspension provisoire et/ou de désinscription sera prise après avoir recueilli les observations du prestataire, sauf en cas d'un manquement d'une gravité particulière nécessitant une mesure de suspension ou de désinscription immédiate.Demander à Me Clot : que peut-on faire si on constate qu'un prestataire a des pratiques commerciales bordeline ? Signalement DGCCRF etc.

7 – Modalités d'acceptation de la charte

Le candidat ne peut valider le dépôt de son dossier de candidature sans acceptation des termes de la présente charte.

Le prestataire est invité à prendre connaissance des termes de la présente charte au moment du dépôt de sa demande d'inscription sur la plateforme, un onglet spécifique à cette fin étant proposé en fin de processus d'enregistrement de la candidature.

La confirmation de sa demande d'inscription vaut acceptation sans réserve des termes de la présente charte.