CHARTE D’ENGAGEMENT DES PRESTATAIRES EN RELATION AVEC LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR V2.5

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:

- la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises, aux associations et aux administrations victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». Plus particulièrement, le groupement s'attachera d'une part, à permettre la mise en relation avec des acteurs de proximité capables de procéder à la sécurisation et à la reprise d'activité des victimes et d'autre part, à fournir l'aide aux démarches administratives requises pour le dépôt de plainte ;

- la sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière ;

- la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.

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 usagers de la plateforme qui le souhaitent des prestations d’installation, de maintenance et d’assistance.

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.

Cette mise en relation peut aboutir à la contractualisation d'un contrat de vente de prestations entre un prestataire inscrit sur la plateforme et l'usager souhaitant bénéficier d'une assistance. Il est précisé que cette contractualisation s'effectue 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 [« usager »] bénéficiaire 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 est gratuite et 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.

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

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 (futurs)bénéficiaires et traitement de leurs demandes d'assistance

- Accueil des (futurs) bénéficiaires

Le prestataire inscrit sur la plateforme Cybermalveillance.gouv.fr s'engage à réserver le meilleur accueil aux (futurs)bénéficiaires - particuliers, entreprises, associations et administrations - 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.

Il est attendu que chaque prestataire fournisse une réponse personnalisée au (futur) bénéficiaire en prenant en compte la nature de son incident, ainsi que sa position géographique.

- Obligation générale d'information

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.

- Transparence vis-à-vis des bénéficiaires

Le prestataire fournit au (futur) bénéficiaire en amont de la prestation de remédiation, un diagnostic complet, comportant le cas échéant 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, ainsi que la description de l’accompagnement proposé, les coordonnées électroniques et/ou téléphoniques de la personne à contacter ainsi que les horaires d’ouverture.

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.

- Transparence vis-à-vis des autres prestataires

Ainsi qu’il a été dit précédemment, lorsqu’un prestataire a accepté une demande d’intervention, il doit obligatoirement se mettre d’accord avec le bénéficiaire sur la nature de l’intervention et son éventuelle tarification.

Suite à cet accord, le prestataire doit programmer l’intervention dans son espace privé sur Cybermalveillance.gouv.fr afin de notifier ses homologues que l’incident est en cours de traitement.

Le cas échéant, il est possible de passer l’intervention au statut résolu directement sans passer par le statut programmation.

- Engagements éthiques et déontologiques

D’une manière générale, le prestataire s’engage à réaliser les prestations d’assistance aux bénéficiaires 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. S’il n’existe pas à ce jour de Code de déontologie s’appliquant aux prestataires informatiques, il est attendu des prestataires présents sur la plateforme Cybermalveillance.gouv.fr de faire preuve d’éthique professionnelle dans l’exercice de leurs activités liées à la plateforme.

Le prestataire présent sur la plateforme Cybermalveillance.gouv.fr ne saurait accomplir d’autres prestations et activités que celles prévues par la présente charte : tout dévoiement du système d’information, ayant porté atteinte ou non au bon fonctionnement de la plateforme, constituera un motif de suspension et/ou de désinscription.

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.

c) Respect de la confidentialité du bénéficiaire de la prestation 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 (RGPD[2]) 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 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.

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

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.

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 au bénéficiaire, qui 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 sur l’adresse courriel de contact et/ou au numéro de portable enregistrés 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. Ces coordonnées ne seront pas communiquée à des tiers sans leur accord et seront supprimées de la base de données un an maximum après que leur inscription sur la plateforme soit révoquée;

- de faire l’objet d’une évaluation par les (futurs) bénéficiaires; cette évaluation est à la fois quantitative (étoiles de notation) et qualitative (avis).

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

Par principe, l'engagement des prestataires inscrits sur la plateforme Cybermalveillance.gouv.fr a une durée indéterminée. Ce principe admet néanmoins trois exceptions :

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 dpo@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 à l'initiative du GIP ACYMA

Le GIP ACYMA se réserve le droit de procéder à la suspension temporaire du compte 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 bénéficiaires ayant recouru aux services dudit prestataire ;
- d'irrégularités constatées.

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. La mesure de suspension provisoire sera prise après avoir recueilli les observations du prestataire, sauf en cas d'un manquement d'une gravité particulière nécessitant une mesure de suspension immédiate.

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.

c) Désinscription à l'initiative du GIP ACYMA

Le GIP ACYMA se réserve le droit de désinscrire un prestataire en cas de manquement à ses obligations et 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.

La mesure 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 désinscription immédiate.

7 – Dispositions relatives au Label Expert Cyber

Le label ExpertCyber est destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Il couvre les domaines suivants : systèmes d'informations professionnels (serveurs, messageries, logiciels bureautiques…), téléphonie (serveurs téléphoniques

professionnels) et sites Internet (administration et protection). La plateforme de labellisation est accessible sur : https//expertcyber.afnor.org.

Ces professionnels labellisés Expert Cyber ont la possibilité de se faire référencer sur la plateforme Cybermalveillance.gouv.fr, dans les conditions suivantes:

a) Engagements des prestataires labellisés et référencés

Il est attendu des professionnels labellisés Expert Cyber qui seront référencés sur la plateforme Cybermalveillance.gouv.fr de respecter les mêmes engagements que ceux auxquels sont soumis les professionnels déjà référencés et exposés dans la présente charte.

b) Annuaire inversé

Ces professionnels apparaissent dans l'annuaire inversé et en sont informés par courrier électronique. S'ils ne souhaitent plus apparaître dans l'annuaire inversé, ils peuvent adresser une demande à dpo@cybermalveillance.gouv.fr et l'ensemble de leur compte sera désactivé.

Lors de leur connexion sur leur espace privé, ils sont invités à mettre à jour leurs compétences afin de pouvoir être mis en relation avec des entreprises, associations et administrations souhaitant être accompagnées dans l'installation et la sécurisation de leur système d'information. Les professionnels concernés ne pourront être mis en relation qu'après avoir renseigné ces nouvelles compétences. S'ils ne souhaitent plus recevoir les demandes de mise en relation pour accompagner les entreprises, associations et administrations hors incident de sécurité, ils peuvent adresser une demande à dpo@cybermalveillance.gouv.fr et l'ensemble de leur compte sera désactivé.

8 – 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.

A chaque modification ou mise à jour de la charte d'engagement, les nouveaux termes seront communiqués et transmis pour acceptation aux prestataires présents sur la plateforme Cybermalveillance.gouv.fr. L'acceptation de ces modifications ou mises à jour constitue une condition à la poursuite, par les prestataires, de leur activité sur la plateforme.

9 – Responsabilité

Il est expressément rappelé que Cybermalveillance.gouv.fr est opéré dans le cadre d'une mission de service public administratif visant notamment à assurer la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises, aux associations et aux administrations victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». L'accès aux fonctionnalités de la plateforme Cybermalveillance.gouv.fr est gratuite, tant pour les prestataires inscrits que pour les usagers.

Dans ce cadre, s'agissant des prestataires inscrits, la plateforme Cybermalveillance.gouv.fr se borne à présenter aux usagers bénéficiaires des prestataires référencés de proximité et le cas échéant titulaires du label Expertcyber.

Il en résulte qu'en signant la présente charte, les prestataires sont informés et reconnaissent expressément :

- que leur inscription ne leur garantit pas la contractualisation d'une prestation avec un bénéficiaire via la plateforme Cybermalveillance.gouv.fr.

- que le GIP ACYMA n'exerce aucun contrôle, de quelque nature que ce soit, de manière directe ou indirecte, sur la nature ou le contenu des engagements contractuels susceptibles d'être conclus entre un prestataire et un bénéficiaire, de sorte que leurs relations contractuelles demeurent inopposables au GIP ACYMA ;

- que le GIP ACYMA n'est pas garant de la bonne exécution des obligations contractuelles souscrites par les parties. A ce titre, les prestataires sont seuls responsables de la vente et de l'exécution des services qu'ils sont susceptibles de fournir aux bénéficiaires et des réclamations ou tout autre problème survenant ou lié au contrat de prestation entre eux et les bénéficiaires. Ils engagent seuls leur responsabilité à ce titre, eu égard à l'ensemble des dispositions de nature législative ou réglementaire en vigueur susceptibles de s'appliquer en fonction de la nature des bénéficiaires, qu'ils soient particuliers, entreprises, associations ou administrations.

Le GIP ACYMA se réserve la possibilité d'effectuer des interventions techniques, de maintenance ou d'actualisation sur la plateforme Cybermalveillance.gouv.fr, occasionnant éventuellement une interruption temporaire d'accès. Les dysfonctionnements et/ou indisponibilités de services qui en résulteraient ne peuvent donner lieu à un quelconque dédommagement, ni pour les prestataires inscrits, ni pour les (futurs)bénéficiaires.

Par ailleurs, il est rappelé que le GIP ACYMA ne garantit ni aux prestataires, ni aux (futurs)bénéficiaires, la fiabilité, la performance et l'exhaustivité des contenus et services proposés sur la plateforme Cybermalveillance.gouv.fr. Les intéressés acceptent d'utiliser les contenus et de recourir aux services sous leur responsabilité exclusive. Le GIP ACYMA ne peut être tenu pour responsable des dommages directs ou indirects dont se prévaudraient les prestataires inscrits et les futurs(bénéficiaires) en recourant aux contenus et services offerts par la plateforme.

10 – Droit applicable

La présente charte d’engagement est soumise au droit français : tout litige relèvera de la compétence exclusive des tribunaux français compétents.