RÉPUBLIQUE FRANÇAISE

Ministère de l'Économie,
des Finances et de la souveraineté
industrielle et numérique

Projet d'arrêté

fixant les critères pour l'application de la loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public

Article 1er

Le présent arrêté s'applique aux services visés par le Projet de décret fixant les seuils pour l'application de la loi n° 2022-309 du 3 mars 2022 relatif à la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public

Article 2

En application de l'article L. 111-7-3 du code de la consommation, les critères et le système de notation applicables aux services visés par la Loi n° 2022-309 du 3 mars 2022 pour calculer le cyber score sont spécifiés en annexe 1

Article 3

La forme de présentation du cyberscore en application de l'article L. 111-7-3 du code de la consommation consiste en une signalétique déterminée conformément aux modalités fixées dans le cahier des charges figurant en annexe du présent arrêté (annexe 2)

Les services en ligne visés par les critères du décret fixant les seuils pour l'application de la loi n° 2022-309 du 3 mars 2022 devront afficher le cyberscore dans un délai de 3 mois à compter de leur désignation par le présent décret.

Article 4

Les audits réalisés dans le cadre de la loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public devront être réalisés par des prestataires d'audit de la sécurité des systèmes d'informations (PASSI) qualifiés par l'ANSSI.

Les prestataires d'audit de la sécurité des systèmes d'informations (PASSI) qualifiés par l'ANSSI pourront librement recourir aux services d'un auditeur qui ne serait pas

individuellement qualifié PASSI, sous réserve de s'assurer du respect des normes d'audit et des méthodes définis par l'ANSSI pour le cyberscore.

L'audit réalisé pour la définition du cyberscore est réalisé sur la base d'informations ouvertes, librement accessible et de manière non intrusive par le prestataire.

Article 5

Les audits réalisés dans le cadre de la loi n° 2022-309 du 3 mars 2022 permettant l'attribution d'un cyberscore auront une durée de validité de 12 mois et devront être renouvelé dans un délai de 3 mois suivant l'expiration du précédent audit, sous réserve que la plateforme demeure en situation de se conformer à l'obligation d'apposition d'un cyberscore.

Article 6

Le présent arrêté entre en vigueur le [1er janvier 2024].

Article 7

Le ministre de l'économie, des finances et de la souveraineté industrielle et numérique, le ministre des outre-mer, et le ministre délégué au numérique auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

ANNEXE 1

Proposition de critères d'audit en vue de la détermination d'un cyber score tel que défini par la Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public

SECTION D'AUDIT	CRITERES D'AUDIT	Notation Référence						
		F	E	D	C	B	A	A+
Organisation et Gouvernance	La société délivrant le service est assujettie au droit européen				✓	✓	✓	✓
Organisation et Gouvernance	Organisation de maîtrise des risques				✓	✓	✓	✓
Organisation et Gouvernance	Assurance permettant de couvrir les risques numériques pour le service numérique étudié					✓	✓	✓
Organisation et Gouvernance	Certifications de sécurité relevant d'un standard international (type norme ISO) ou national (reconnue par l'ANSSI)					✓	✓	✓
Protection des données	Les données techniques et/ou personnelles des usagers sont revendues et/ou partagées à des tiers							✓
Protection des données	Exposition des données du service numérique à des législations à portées extraterritoriales (fournisseurs du service et partenaires tiers)				✓	✓	✓	✓
Protection des données	Existence de mesures techniques, organisationnelles et juridiques assurant la conformité du service aux recommandations de l'EDPB en matière d'hébergement et de traitement des données.				✓	✓	✓	✓
Connaissance et maîtrise du service numérique	Existence d'une cartographie des informations traitées par le service numérique étudié et de leur sensibilité		✓	✓	✓	✓	✓	✓
Connaissance et maîtrise du service numérique	Existence d'une cartographique des partenaires et des sous-traitants contribuant au service numérique étudié		✓	✓	✓	✓	✓	✓
Connaissance et maîtrise du service numérique	Maintien en condition opérationnelle et de sécurité du service numérique			✓	✓	✓	✓	✓
Connaissance et maîtrise du service numérique	Existence d'un dossier d'architecture technique du service numérique			✓	✓	✓	✓	✓
Connaissance et maîtrise du service numérique	Existence de mécanismes de cloisonnement réseau visant à prémunir le service numérique d'une attaque par rebond sur les environnements mutualisés			✓	✓	✓	✓	✓
Niveau d'externalisation	Localisation des infrastructures d'hébergement du service numérique en UE				✓	✓	✓	✓
Niveau d'externalisation	Les sous-traitants en matière d'administration et de supervision du service numérique sont de nationalité UE					✓	✓	✓
Niveau d'externalisation	Externalisation de certains sous-systèmes et/ou interfaces sensibles (service de paiement, gestion des sauvegardes, etc.)				✓	✓	✓	✓
Niveau d'exposition sur Internet	Sécurité de la connexion utilisateur		✓	✓	✓	✓	✓	✓
Niveau d'exposition sur Internet	Utilisation d'un nom de domaine maîtrisé				✓	✓	✓	✓
Niveau d'exposition sur Internet	Utilisation de sous domaines pour des sous-systèmes spécifiques (paiement, administration, mail etc…)				✓	✓	✓	✓
Niveau d'exposition sur Internet	Réalisation de scans de sécurité réguliers sur l'exposition du service numérique sur Internet				✓	✓	✓	✓
Niveau d'exposition sur Internet	Mise en œuvre d'une solution visant à se prémunir des dénis de services (DDoS)				✓	✓	✓	✓

Niveau d'exposition sur Internet	Gestion de l'identification/authentification de l'utilisateur du service		✓	✓	✓	✓	✓	✓
Niveau d'exposition sur Internet	Gestion de l'identification/authentification des administrateurs techniques et fonctionnels du service		✓	✓	✓	✓	✓	✓
Niveau d'exposition sur Internet	Gestion de l'administration technique du service numérique étudié					✓	✓	✓
Niveau d'exposition sur Internet	Sécurisation de la messagerie - Utilisation d'un protocole de sécurité (DKIM/DMARC/SPF) dans la gestion de la messagerie				✓	✓	✓	✓
Dispositif de traitement des incidents de sécurité	Existence d'une stratégie de réponse à incidents			✓	✓	✓	✓	✓
Dispositif de traitement des incidents de sécurité	Existence d'une stratégie de gestion des crises / Plan de continuité d'activité			✓	✓	✓	✓	✓
Dispositif de traitement des incidents de sécurité	Sauvegarde des données		✓	✓	✓	✓	✓	✓
Dispositif de traitement des incidents de sécurité	Mise en œuvre d'un système de détection d'incident				✓	✓	✓	✓
Audits du service numérique étudié	Réalisation d'audits de sécurité avant la mise en œuvre du service numérique étudié (audit/Bug bounty/etc.)				✓	✓	✓	✓
Audits du service numérique étudié	Existence d'une procédure d'audits de sécurité réguliers du service numérique étudié (audit/Bug bounty/etc.)					✓	✓	✓
Sensibilisation aux risques cyber et lutte anti-fraude	Actions de sensibilisation aux risques de cybersécurité pour les employés de l'entreprise fournissant le service numérique étudié				✓	✓	✓	✓
Sensibilisation aux risques cyber et lutte anti-fraude	Actions de sensibilisation aux risques de cybersécurité pour les administrateurs du service numérique étudié			✓	✓	✓	✓	✓
Sensibilisation aux risques cyber et lutte anti-fraude	Mise en place d'une politique de lutte contre la fraude et les escroqueries pour les services proposés aux usagers				✓	✓	✓	✓
Sensibilisation aux risques cyber et lutte anti-fraude	Avertissement des usagers sur les risques cyber d'escroqueries et de fraudes et recommandations de précautions				✓	✓	✓	✓
Développement sécurisé	Prise en compte des règles de l'OWASP			✓	✓	✓	✓	✓
Développement sécurisé	Formation aux développements sécurisés							✓

Les critères présentés ci-dessus se décomposent en sous critères qui peuvent eux-mêmes se décomposer en différents points de contrôles.

Il est proposé d'inclure les enjeux de localisation de données directement dans le cyber score par soucis de lisibilité et compte tenu de la difficulté technique d'afficher au consommateur la localisation des données.

L'obtention d'un palier est conditionnée à la positivité de l'ensemble des critères de ce palier.

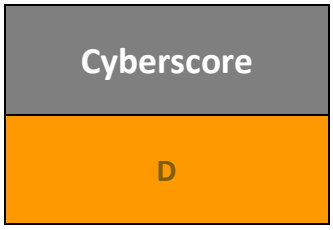
ANNEXE 2

Modalité d'affichage d'un cyberscore au sens de la Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public

Proposition de visuel de la notation du rapport d'audit :

Niveau	Critères atteints par niveau	Avancée	Avancée
A+	0/62	0%	Palier non atteint
A	0/59	0%	Palier non atteint
B	0/55	0%	Palier non atteint
C	0/46	0%	Palier non atteint
D	0/21	0%	Palier non atteint
E	0/10	0%	Palier non atteint
F	-	-	Palier atteint

Proposition de visuel pour le cyberscore



Proposition d'apposition du cyberscore

Le marquage visuel cyberscore devra être apposé de manière visible sur l'écran d'accueil du service en ligne visé par le présent décret.

Le score d'audit cyberscore ainsi que la date d'audit devra apparaitre de manière visible dans les mentions légales du service en ligne visé par le présent décret