CYLAR

Cyber-Lares

Simple regard pratique sur l'obligation de sensibilisation dans le cyber score

Par

Antoine Fournier, CEO

CYLAR

Cyber-Lares

› Article L111-7-3

Version en vigueur depuis le 01 octobre 2023

Création LOI n°2022-309 du 3 mars 2022 - art. 1

Les opérateurs de plateformes en ligne mentionnés à l'article L. 111-7 du présent code et les personnes qui fournissent des services de communications interpersonnelles non fondés sur la numérotation, au sens du 6° quater de l'article L. 32 du code des postes et des communications électroniques, dont l'activité dépasse un ou plusieurs seuils définis par décret réalisent un audit de cybersécurité, dont les résultats sont présentés au consommateur dans les conditions prévues au dernier alinéa du présent article, portant sur la sécurisation et la localisation des données qu'ils hébergent, directement ou par l'intermédiaire d'un tiers, et sur leur propre sécurisation, dans les conditions prévues au présent article.

L'audit mentionné au premier alinéa est effectué par des prestataires d'audit qualifiés par l'Agence nationale de la sécurité des systèmes d'information.

Un arrêté conjoint des ministres chargés du numérique et de la consommation, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les critères qui sont pris en compte par l'audit prévu au même premier alinéa et ses conditions en matière de durée de validité ainsi que les modalités de sa présentation.

Le résultat de l'audit est présenté au consommateur de façon lisible, claire et compréhensible et est accompagné d'une présentation ou d'une expression complémentaire, au moyen d'un système d'information coloriel.

CYLAR

Cyber-Lares

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							✓

CYLAD

Cyber-Lares

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

Cyberscore
D

CYLAR

Cyber-Lares

Qu'implique l'obligation ou de sensibilisation dans le **cyber score** ?

I – Le contenu de la prestation

A – La nature de la prestation

B – Les thèmes abordés dans la prestation

II – La délivrance de la prestation

A – Le niveau d'exigence attendu de la prestation

B – La responsabilité du formateur en cas de non-conformité de la prestation

CYLAR
Cyber-Lares

I – Le contenu de la prestation

A – La nature de la prestation

Que signifie le terme de « sensibilisation » ?

Que signifie le terme de « formation » ?

Article 39 du RGPD	ISO 27001	Projet d'arrêté pour le Cyberscore
Les missions du délégué à la protection des données sont au moins les suivantes: [...] b) [...] la **sensibilisation** et la **formation** du personnel participant aux opérations de traitement, et les audits s'y rapportant ; »	**Directement** Art. 7.3 ISO 27001 « Sensibiliser le personnel aux **répercussions** et aux **conséquences** du non-respect des exigences du SMSI ». **Indirectement** Article 8.2 ISO 27001 « Apprécier les risques de sécurité de l'information régulièrement »	« Actions de sensibilisation aux risques de cybersécurité pour les employés de l'entreprise fournissant le service numérique étudié » « Actions de sensibilisation aux risques de cybersécurité pour les administrateurs du service numérique étudié » « Mise en place d'une politique de lutte contre la fraude et les escroqueries pour les services proposés aux usagers »

	Article 7.4 ISO 37001 « L'organisation détermine les communications internes et externes relatives au système de gestion de la lutte contre la corruption ».	« Avertissement des usagers sur les risques cyber d'escroqueries et de fraudes et recommandations de précautions »

CYLAR
Cyber-Lares

I – Le contenu de la prestation

B – Le contenu de la prestation

Quelles informations sur les bonnes pratiques doivent être transmises à tous les employés ? Aux administrateurs du SI ? Concernant l'escroquerie ou la fraude ?

Quelles compétences doivent être acquises conformément aux règles de l'OWASP et dans le cadre d'une formation aux développements sécurisés ?

Article 39 du RGPD	ISO 27001	Projet d'arrêté sur le cyberscore
(A condition que le développement implique la manipulation de données à caractère personnel).	**Directement** Article 7.2 ISO 27001 « Déterminer les compétences nécessaires des personnes concernées S'assurer que ces personnes sont compétentes Mener des actions pour acquérir et tenir à jour les compétences nécessaires Conserver des informations documentées sur les compétences » **Indirectement** Article 8.2 ISO 27001 « Apprécier les risques de sécurité de l'information régulièrement »	« Prise en compte des règles de l'OWASP » « Formation aux développements sécurisés »

CYLAR
Cyber-Lares

II – La délivrance de la prestation

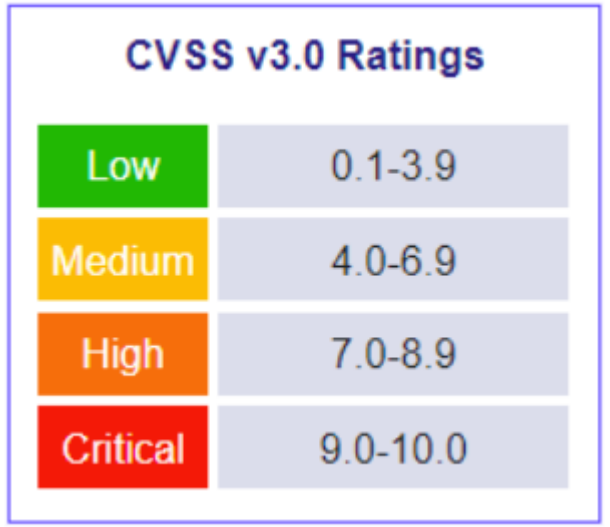
A – Le niveau d'exigence de la prestation

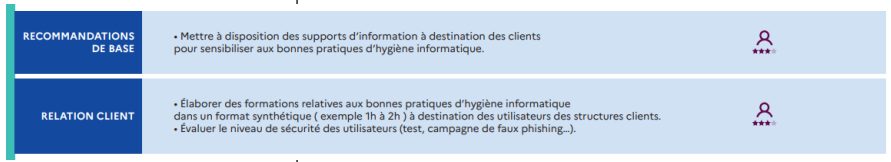
La formation délivrée doit-elle obéir à une forme particulière ?

Comment évaluer la qualité d'une formation ou d'une sensibilisation ?

Nom		Poids	Progrès	Valeur	Mesure	Cible
Préparation à la protection des données		1	96%	96	%	100
Nomination d'un responsable de la protection des données		1	100%	Oui	Oui/Non	Oui
Suivi du consentement explicite		1	100%	Oui	Oui/Non	Oui
Procédure de notification des violations de données		1	80%	80	%	100
Droit d'accès, de rectification, d'effacement mis en œuvre		1	100%	Oui	Oui/Non	Oui
Droit à la portabilité des données		1	100%	Oui	Oui/Non	Oui
Indice de risque pondéré		100	69.77%	66.7	%	100
Événements à risque critique		70	75%	1	#	0
Événements à risque importants		20	55.56%	5	#	1
Événements à risque de niveau moyen		7	40%	14	#	5
Événements à faible risque		3	112%	12	#	15
Processus d'affaires internes		1	88.69%	71.333	%	100
Détection précoce et réponse rapide aux risques liés aux données		1	88.69%	71.333	%	100

Article 39 du RGPD	ISO 27001	Projet d'arrêté sur le cyberscore
(A condition que le développement implique la manipulation de données à caractère personnel).	**Directement** Article 7.2 ISO 27001 « Déterminer les compétences nécessaires des personnes concernées S'assurer que ces personnes sont compétentes Mener des actions pour acquérir et tenir à jour les compétences nécessaires Conserver des informations documentées sur les compétences » **Indirectement** Article 8.2 ISO 27001 « Apprécier les risques de sécurité de l'information régulièrement »	« Prise en compte des règles de l'OWASP » « Formation aux développements sécurisés »





CYLA
Cyber-Lares

II – La délivrance de la prestation

B – La responsabilité du formateur en cas de non-conformité de la prestation

Faut-il être agréé par l'ANSSI pour délivrer une sensibilisation ou une formation prise en compte dans le cyberscore ?

Peut-il exister un conflit d'intérêt entre le formateur et la PASSI (prestataire d'audit de sécurité des systèmes d'information ?

Peut-on engager la responsabilité du prestataire de formation lorsque la note obtenue n'est pas celle attendue ?

› **Article 1217**

Version en vigueur depuis le 01 octobre 2018

Modifié par LOI n°2018-287 du 20 avril 2018 - art. 10

La partie envers laquelle l'engagement n'a pas été exécuté, ou l'a été imparfaitement, peut :

- refuser d'exécuter ou suspendre l'exécution de sa propre obligation ;

- poursuivre l'exécution forcée en nature de l'obligation ;

- obtenir une réduction du prix ;

- provoquer la résolution du contrat ;

- demander réparation des conséquences de l'inexécution.

Les sanctions qui ne sont pas incompatibles peuvent être cumulées ; des dommages et intérêts peuvent toujours s'y ajouter.

NOTA :
Conformément aux dispositions du I de l'article 16 de la loi n° 2018-287 du 20 avril 2018, les modifications apportées par ladite loi aux dispositions de l'article 1217 ont un caractère interprétatif.

CYLA
Cyber-Lares

conclusion

Quelle place pour **l'intelligence artificielle** dans la sensibilisation et la formation en cyber sécurité ?

Merci !

Antoine.fournier@cy-la.net