

ANNEXE 1 au contrat

Obligations en matière de protection des données et de sécurité

Conformément à l'article 6.4 du Contrat, le Titulaire met en œuvre les mesures techniques et organisationnelles suivantes :

Sujet	Mesure de sécurité	Niveaux de maturité	Réponse
Gestion des habilitations des utilisateurs des applications fournies par France Travail en cohérence avec l'activité réalisée	Le prestataire titulaire doit s'assurer régulièrement que les habilitations des utilisateurs des applications fournies par France Travail sont en cohérence avec l'activité qu'ils réalisent.	Avancé	Une revue est réalisée tous les 3 mois, avec un procès-verbal (PV) établi et transmis à France Travail. Les habilitations sont, quant à elles, traitées au fil de l'eau.
		Basique / Minimal	Revue réalisée tous les 3 mois avec PV réalisé et transmis à FT
		Non conforme	Pas de mise à jour

Procédure en cas d'incidents	Le prestataire titulaire doit avoir une procédure et communiquer tout incidents affectant les données fournies par France Travail dans les 48 heures après avoir pris connaissance de l'incident.	Basique / Minimal	Le prestataire dispose d'une procédure, fournit la procédure et l'applique en cas d'incident
	Réf clause RGPD : 6.4 - <i>Violation de données personnelles</i>	Non conforme	Le prestataire ne dispose d'aucune procédure ou n'applique pas la procédure existante
Sécurisation des échanges entre le Titulaire et tout intervenant prenant part à l'exécution du marché	Le prestataire doit mettre en œuvre un moyen sécurisé et conforme au RGPD pour assurer les échanges entre lui-même et les différents intervenants prenant part à l'exécution des prestations.	Avancé	Envoi par mail des fichiers chiffrés par un outil qualifié par l'ANSSI (Primx zed! par ex.) ou mise à disposition des fichiers sur un portail avec authentification à deux facteurs.
		Intermédiaire	Pas d'envoi par courriel, utilisation d'un système d'information (propre ou externalisé)
		Basique / Minimal	Transmission du fichier chiffré par courriel à l'aide d'un outil de chiffrement standard.
		Non conforme	L'envoi se fait par courriel, sans chiffrement.
Stockage des données	Il est interdit d'utiliser les offres publiques des plateformes de stockage non maîtrisée (Google Drive, Dropbox,	Basique / Minimal	Aucune plateforme de ce type utilisée

	etc.) pour y transférer les données transmises par France Travail.	Non conforme	Utilisation de plateformes de stockage non maîtrisée
Destruction des données personnelles	Le prestataire doit régulièrement détruire les données obtenues il y a plus de 6 mois. Il doit fournir un procès-verbal de destruction. Réf clause 6.4 e) du Contrat : - Sort des données	Basique / Minimal	Purge avec PV de destruction transmis à France Travail tous les 6 mois
		Non conforme	Purge tous les 6 mois
		Non conforme	Pas de purge
Condition de détention du matériel informatique dans des locaux appropriés et sécurisés	Le prestataire doit héberger le matériel informatique dans des locaux appropriés et sécurisés.	Avancé	Datacenter pour les serveurs soutenant la messagerie les espaces de stockage partagé, et l'AD.
		Intermédiaire	Salle technique avec contrôle d'accès
		Basique / Minimal	Armoire technique avec contrôle d'accès

		Non conforme	Armoire/salle simple ou Armoire technique sans contrôle d'accès
Utilisation de messageries électroniques accessibles via Internet	En cas d'utilisation de messageries électronique accessible via Internet, par exemple par un <i>webmail</i> , Le prestataire doit disposer d'une authentification sécurisée à ce service.	Avancé	Utilisation de la 2FA sur deux supports différents
		Basique / Minimal	Politique de mot de passe robuste
			Mécanisme de protection contre les attaques par force brute
			Mécanisme d'oubli de mot de passe qui ne transfère pas le mot de passe mais laisse la possibilité unique à l'utilisateur de le choisir.
		Non conforme	Politique de mot de passe simple
Utilisation d'application, de service de partage de fichiers, etc. accessible via Internet	En cas d'utilisation d'application, de service de partage de fichiers, etc. accessible via Internet, le prestataire doit disposer d'une authentification sécurisée à ce service.	Avancé	Authentification multi facteurs reposant sur l'utilisation de plusieurs facteurs d'authentification appartenant à une catégorie de facteurs différente parmi les facteurs de connaissance, de possession et inhérent
		Basique / Minimal	Politique de mot de passe robuste
			Mécanisme de protection contre les attaques par force brute

			Mécanisme d'oubli de mot de passe qui ne transfère pas le mot de passe mais laisse la possibilité unique à l'utilisateur de le choisir.
		Non conforme	Politique de mot de passe simple
Configuration du Wifi	Le prestataire doit mettre en place une configuration du WiFi à l'état de l'art. https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_WIFI_NoteTech.pdf	Avancé	Désactivation de la diffusion SSID + WPA2
		Basique / Minimal	Configurer le point d'accès pour utiliser un chiffrement robuste. Utilisation du mode WPA2 avec l'algorithme de chiffrement AES-CCMP.
		Non conforme	Mode d'authentification WPA-PSK avec un mot de passe long (> 20 caractères).
Moyens de protection de la connexion et navigation sur Internet	Le prestataire doit mettre en œuvre des moyens de protection depuis Internet et de la navigation web.	Avancé	Proxy web de sortie avec liste de blocage
		Basique / Minimal	Disposer d'un pare-feu entrant sur la connexion internet
		Non conforme	Absence de proxy Web , accès libres aux sites
Connaissance par le Titulaire de son système d'information	Le prestataire doit disposer de la connaissance de son système d'information	Non conforme	Pas de cartographie des SI
		Basique / Minimal	Cartographie existante et à jour

Protection de tous les terminaux	Le prestataire doit disposer de moyen de protection des terminaux utilisés.	Avancé	Maitrise de la flotte mobile via MDM
		Intermédiaire	EDR sur les postes de travail
		Basique / Minimal	Antivirus à jour des signatures sur tous les postes de travail
		Non conforme	Utilisation d'équipements personnels (BYOD) sans inscription MDM/EMM, sans chiffrement et sans contrôle d'accès.
Formation et sensibilisation du personnel aux bonnes pratiques de sécurité des systèmes d'information (SSI).	Le prestataire doit sensibiliser et former son personnel aux bonne pratiques SSI	Non conforme	Aucun programme de sensibilisation n'est en place. Le personnel n'a pas conscience des risques liés à la cybersécurité, ce qui expose l'organisation à des vulnérabilités importantes.
		Basique / Minimal	Le personnel intervenant dans le cadre du marché est formé et sensibilisé aux risques liés à la cybersécurité.
		Avancé	Un programme de sensibilisation est formalisé et diffusé régulièrement à l'ensemble du personnel. La démarche est proactive.

Gouvernance des nouvelles technologies (IA)	Le prestataire doit encadrer l'usage de l'IA pour éviter les risques de sécurité, de confidentialité et de dérives.	Non conforme	L'usage de l'IA n'est pas encadré. Les collaborateurs peuvent utiliser librement des outils d'IA sans directives ni sensibilisation aux risques, notamment en matière de cybersécurité.
		Basique / Minimal	L'usage de l'IA est encadré par une politique formelle, intégrée à la gouvernance SSI et des actions de sensibilisation sont menées.
		Avancé	L'usage de l'IA est encadré par une politique claire, intégrée à la gouvernance SSI. Les contenus sont régulièrement mis à jour, des campagnes de sensibilisation ciblées sont menées, et des référents accompagnent les utilisateurs. L'usage est audité et les risques sont évalués de manière proactive.

Dès la notification du marché, le Titulaire est tenu de mettre en œuvre, *a minima*, l'ensemble des mesures minimales définies.

Six mois après la date de notification du marché, le Titulaire rend compte à France Travail de cette mise en œuvre en lui retournant, au format Excel, le questionnaire Cybersécurité remis lors de la réunion de lancement. Ce questionnaire permet de définir le type de mesures effectivement mises en œuvre (minimal, intermédiaire, avancé).

Un plan de progrès pourra être demandé suivant les résultats issus du questionnaire.