Form PRO-06.10

FORMULAIRE RGPD ACTED France

Date :

Appel d'Offres N° :

A remplir par le soumissionnaire (OBLIGATOIRE)

Détails sur la société soumissionnaire :

1. Nom de la société : (_____)
2. Nom, Prénom & Qualité du représentant : (_____)
3. Nom, Prénom & E-mail du DPO[1] de la société : (_____)
   (_____@_____)

REF.	THEME	POINT A VERIFIER	REPONSE Oui/Non/Non applicable (N/A)	COMMENTAIRE
Fiche 1	Risques	Établir un registre des traitements de données à caractère personnel mis en œuvre par la solution proposée		
		Documentation détaillant l'intégration des principes de *Security By Design* et de *Privacy By Design* dans la solution proposée		
		Procédure détaillant l'aide apportée à Acted en cas d'exercice de ses droits par une personne concernée		
		Déterminer les menaces et leurs impacts sur la vie privée des personnes		
		Procédure en cas de violation des données à caractère personnel		
		Procédure de restitution des données en cas de fin de contrat		
		Mettre en œuvre des mesures de sécurité adaptées aux menaces		
Fiche 2	Authentification des utilisateurs	Définir un identifiant (login) unique à chaque utilisateur		
		Adopter une politique de mot de passe utilisateur rigoureuse (mots de passe de 8 caractères minimum avec des caractères de types différents et de 10 caractères minimum pour les comptes administrateurs)		
		Changer de mot de passe régulièrement		
		Obligez l'utilisateur à changer son mot de passe après réinitialisation		
		Stockage des mots de passe dans un fichier crypté		
		Choix des mots de passe sans lien avec soi		
		Ne pas communiquer son mot de passe		
Fiche 3	Habilitations	Définir des profils d'habilitation		
		Supprimer les permissions d'accès obsolètes		

[1] Data Protection Officer (Responsable de la Protection des Données)

		Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles aux utilisateurs concernés		
		Rédiger une charte informatique (annexée au règlement intérieur)		
		Définir des comptes nominatifs (pas de comptes partagés par plusieurs personnes)		
		Etablir, documenter et réexaminer une politique de contrôle d'accès en rapport avec la finalité du traitement		
		Classifier les informations de manière à indiquer si celles-ci sont des données sensibles et cloisonnement de celles-ci		
		Envoyer régulièrement à tous les utilisateurs les mises à jour des politiques et procédures pertinentes pour leur fonction		
		Sensibiliser et informer à la sécurité de l'information		
		Prévoir la signature d'un engagement de confidentialité		
Fiche 4	**Sécurité des postes de travail**	Limiter le nombre de tentatives d'accès à un compte (distinction utilisateurs/administrateurs)		
		Installer un «pare-feu» (firewall) logiciel		
		Utiliser des antivirus régulièrement mis à jour		
		Prévoir une procédure de verrouillage automatique de session		
		Ne pas utiliser des comptes d'exploitation obsolètes		
		Installer les mises à jour critiques des systèmes d'exploitation sans délai		
		Limiter les applications nécessitant des droits de niveau administrateur pour leur exécution		
		Limiter les services du système d'exploitation s'exécutant sur le poste de travail à ceux strictement nécessaires		
		Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées		
Fiche 5	**Sécurisation de l'informatique mobile**	Prévoyez des moyens de chiffrement pour les ordinateurs portables et Prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…)		
		Ne pas conserver des données personnelles dans les équipements mobiles lors de déplacement à l'étranger		
		Verrouillage automatique des appareils mobiles après quelques minutes d'inactivité		
Fiche 6	**Sauvegardes et continuité de d'activité**	Effectuer des sauvegardes régulières		
		Stocker les supports de sauvegarde sur un site extérieur situé sur le territoire de l'Union européenne et dans l'idéal sur le territoire français		
		Sécuriser le lieu de stockage des sauvegardes par au moins une des solutions suivantes : chiffrement des sauvegardes, chiffrement des données, stockage dans un lieu sécurisé		
		Mettre en place des détecteurs de fumée		

		Les matériels informatiques ne doivent pas être mis au sol mais surélevés		
		Utilisation d'onduleur pour les matériels critiques		
		Prévoir une redondance de matérielle des unités de stockage		
		Prévoir et tester régulièrement la continuité d'activité		
Fiche 7	**Maintenance**	Garantir que les données ne seront pas compromises lors d'une intervention de maintenance par une au moins des solutions suivantes : enregistrement des interventions dans une main courante, encadrement des interventions par des tiers, ne pas autoriser la télémaintenance sans autorisation		
		Effacer les données de tout matériel avant sa mise au rebut		
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste		
		Ne pas installer des applications pour la maintenance vulnérables (http://www.cert.ssi.gouv.fr/site/CERTA2009-AVI-035/)		
		Restreindre, voire interdire l'accès physique et logique, aux ports de diagnostic et de configuration à distance		
Fiche 8	**Traçabilité et gestion des incidents**	Prévoir un système de journalisation des activités des utilisateurs, des anomalies et des évènements liés à la sécurité avec au minimum l'identifiant, la date et l'heure de connexion et de déconnexion		
		Ne pas utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique		
		Synchronisation des horloges à l'aide d'une source de temps fiable et préalablement définie		
		Le candidat doit se tenir informé des vulnérabilités techniques des systèmes et entreprendre les actions appropriées		
Fiche 9	**Sécurité des locaux**	Restreindre les accès aux locaux au moyen de portes verrouillées		
		Installer des alarmes anti-intrusion et vérifiez-les périodiquement		
		Vérifier et entretenir le matériel de climatisation		
		Mettre en place des dispositifs d'authentification pour accéder aux zones dans lesquelles des informations sensibles sont traitées ou stockées		
		A l'intérieur des zones d'accès réglementé, exiger le port d'un moyen d'identification visible		
		Les visiteurs doivent avoir un accès limité (la date et heure de leur arrivée doivent être consignées)		
		Réexaminer et mettre à jour régulièrement les permissions d'accès aux zones sécurisées et les supprimer si nécessaire		
Fiche 10	**Sécurité du réseau informatique**	Limiter les flux réseau au strict nécessaire		
		Sécuriser les accès distants des appareils informatiques nomades par VPN		

		Utiliser le protocole SSL avec une clé de 128 bits pour les services web		
		Ne pas utiliser le protocole telnet pour la connexion à distance aux équipements actifs du réseau (préférer SSH)		
		Mettre en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi		
		Cloisonner le réseau (segmenter le réseau en sous-réseaux logiques)		
		Mettre en place des systèmes de détection d'intrusion (IDS)		
		Mettre en place l'identification automatique de matériels comme moyen d'authentification des connexions à partir de lieux et matériels spécifiques		
Fiche 11	**Sécurité des serveurs et des applications**	Adoptez une politique de mot de passe administrateur rigoureuse (mots de passe de 10 caractères minimum avec des caractères de types différents pour les mots de passe d'administration)		
		Changer de mot de passe au départ d'un administrateur		
		Installer les mises à jour critiques des systèmes d'exploitation sans délai		
		Ne pas utiliser les serveurs à d'autres fins que celles prévues (naviguer sur internet, accéder à la messagerie…)		
		Utiliser des comptes nominatifs pour l'accès aux bases de données		
		Mettre en œuvre des mesures et/ou installer des dispositifs pour se prémunir des attaques par injection de code SQL, scripts		
		Prévoir des mesures particulières pour les bases de données sensibles		
		Assurer une continuité de disponibilité des données		
		Mettre à jour les applications lorsque des failles critiques ont été identifiées et corrigées		
		Ne pas utiliser des services non sécurisés (authentification en clair, flux en clair…)		
		Ne pas placer des bases de données dans une zone directement accessible depuis internet		
		Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé)		
		Utilisation d'outils de détection des vulnérabilités (http://nmap.org/, http://www.tenable.com/products/nessusvulnerability-scanner, https://cirt.net/nikto2)		
		Assurer l'intégrité des traitements par le recours à des signatures garantissant qu'il n'a subi aucune altération		
Fiche 12	**Sous-traitance**	Prévoir dans les contrats une clause de confidentialité et une clause protection des données à caractère personnel intégrant, a minima, les obligations de sécurité présentées dans le présent document		
		Prendre des dispositions (audits de sécurité, visite des installations…) afin de s'assurer de l'effectivité des		

		garanties offertes par le sous-traitant en matière de protection des données		
		Prévoir les conditions de restitution des données et leur destruction en cas de rupture ou à la fin du contrat		
		Ne pas avoir recours à des services offrant des fonctionnalités d'informatique répartie (cloud) sans garantie quant à la localisation géographique effective des données		
Fiche 13	**Archivage**	Mettre en œuvre des modalités d'accès spécifiques aux données archivées		
		Prévoir un système de configuration des durées de conservation des données à caractère personnel distinguant durée active de la donnée et durée d'archivage		
		Détruire les archives obsolètes de manière sécurisée		
		Ne pas utiliser des supports présentant une garantie de longévité suffisante (CD, DVD…)		
Fiche 14	**Echange d'informations avec d'autres organismes**	Chiffrer les données avant leur envoi		
		S'assurer qu'il s'agit du bon destinataire		
		Transmettre le secret lors d'un envoi distinct et via un canal différent		
		Ne pas transmettre des données personnelles en clair via des messageries web du type Gmail		
		Utiliser des calculs d'empreintes pour s'assurer de l'intégrité des données		
		Utiliser des signatures électroniques pour garantir l'origine de la transmission		

Signature autorisée & tampon : _____

***Fin ***