A l'attention de Mme. F,
DSI de la MS2R
A SAINT-DENIS, 97490 Réunion

Le 09/12/2022

Objet : Gestion de la Cybersécurité

L'application développée ne rentre pas dans le cadre de la RGPD, car elle ne fournit pas les mentions obligatoires imposées par le Règlement Général sur la Protection des Données.

"*Le règlement général sur la protection des données (RGPD) impose une information concise, transparente, compréhensible et aisément accessible des personnes concernées. Cette obligation de transparence est définie aux articles 12, 13 et 14 du RGPD.*"

Doivent être renseignées : l'identité de l'entreprise dont la dénomination sociale, la forme juridique, l'adresse du siège social, le montant du capital social, le numéro d'immatriculation au RCS, le numéro d'identification à la TVA, l'identité de l'hébergeur (nom ou dénomination sociale, adresse et numéro de téléphone). Outre ces obligations générales, l'organisme collecteur doit obligatoirement fournir certaines informations concernant la collecte et le traitement des données personnelles.

Les risques potentiels d'un piratage de la base de données sont le plus souvent : des dommages financiers, la perte de données (Ex: Le vol d'informations clients peut entraîner une perte de confiance et une érosion de la clientèle) , l'interruption des systèmes et/ou des applications (Ex : Si un système ne remplit pas sa fonction première, il est possible que les employés ne soient pas en mesure de faire leur travail ou de communiquer, etc), et même des conséquences juridiques(Ex : Si quelqu'un vole des données d'une bases de données, même si ces données ne sont pas particulièrement précieuses, nous pouvons encourir des amendes et d'autres frais juridiques pour ne pas avoir respecté les exigences de sécurité).

Afin de protéger les données de la MS2R nous pouvons :

- Mettre en place une politique stricte de mot de passe (au moins 12 caractères dont minuscule, majuscule, chiffre et caractères spéciaux) ;
- Mettre en place des accès restreints aux données ;
- Sauvegarder très régulièrement les données de l'entreprise ;
- Utiliser un VPN professionnel ;
- Chiffrer les données de l'entreprise ;
- Sécuriser les postes de travail ;