

Un PSP sanctionné par la CNIL à hauteur de 180 000€

écrit par Marine de la Clergerie | 03/01/2022

Sur la délibération [SAN-2021-020](#) du 28 décembre 2021

La CNIL a sanctionné à hauteur de 180 000 € un prestataire de service de paiement (PSP) proposant aux marchands des services de paiement récurrents, mandats SEPA, etc.

Les bonnes pratiques à retenir :

1. Encadrer les relations avec ses sous-traitant par un [contrat conforme aux exigences de l'article 28§3 du RGPD](#)
2. Vérifier le niveau de sécurité de ses sous-traitants
3. Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque
4. En particulier sécuriser les serveurs : restriction d'accès aux seules personnes qui auraient dues être autorisées, mesure de journalisation des accès, etc.
5. Avoir des mots de passe d'accès aux interfaces utilisateurs robustes et conforme aux recommandations de la CNIL et de l'ANSSI
6. Éviter de conserver les RIB et IBAN et/ou sécuriser leur collecte et conservation : les RIB et IBAN sont des données « hautement personnelles » devant faire l'objet d'une vigilance particulière en ce qui concerne leur sécurisation

Références

- Délibération [SAN-2021-020](#) du 28 décembre 2021
- Articles 28 paragraphes 3 et 4, 32 et 34 du [RGPD](#)
- CNIL - [Sécurité : Chiffrer, garantir l'intégrité ou signer](#)
- CNIL - [Projet de recommandation mot de passe](#)
- CNIL - [Guide de la sécurité des données personnelles](#)

- ANSSI - [Recommandations relatives à l'authentification multi facteur et aux mots de passe](#)