15 minutes d'avance

Fiche conseil. 04

Quelles précautions prendre avec les messageries instantanées ?

Les messageries instantanées sont ces applications mobiles rapides et faciles pour communiquer du texte ou partager des documents, à 2 ou dans un groupe. On les connaît sous les noms de *Messenger*, *WhatsApp*, *Discord*, *Telegram*, *Signal*, *Olvid*, pour ne citer que les plus célèbres. Leurs fonctionnalités en font des outils de travail collaboratif très répandus. Mais que deviennent nos données partagées ?

Risques

1. Les DCP peuvent sortir de la zone de protection du RGPD : dans le cas où l'outil de messagerie n'est pas conforme au RGPD. C'est souvent le cas avec l'usage des messageries gratuites.

2. Les DCP peuvent être interceptées par des tierces personnes mal intentionnées : en l'absence de précautions, des pirates (hackeurs) peuvent s'immiscer dans la messagerie. C'est ce que l'on appelle de l'hameçonnage. Ce détournement fera l'objet d'une violation et pourra mener à une gestion de crise avec une notification auprès des personnes concernées.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité, limitation de la conservation
- Art. 5.1 sur l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement
- Art. 32 sur l'obligation d'assurer la sécurité des données personnelles
- Art. 45 et 46 sur les transferts hors UE

La sécurité est un principe essentiel de la protection des données à caractère personnel. Toute l'organisation de l'organisme est fondée et guidée par des « mesures organisationnelles et techniques » afin de protéger les données à caractère personnel. L'usage de la messagerie et la communication des documents sont donc soumis à ces mesures.

Bonnes pratiques

- Privilégier les **outils européens** qui présentent une conformité RGPD. Voir « privacy by design » ou « privacy by default ». Exemple : messagerie française Olvid recommandée par l'ANSSI.
- **Limiter** le nombre de destinataires.
- **Limiter** l'usage à des échanges sans données à caractère personnel.
- Préférer envoyer des documents officiels ou avec DCP par un autre canal, sécurisé, avec possibilité de **chiffrement ou de filigrane** (voir Fiche conseil. 02 : quelles précautions prendre pour envoyer un document officiel ou une pièce d'identité).
- **Supprimer** les documents au fur et à mesure de leur utilisation afin qu'ils ne restent pas stockés sur l'application.

Pour aller plus loin

CNIL – guide de sensibilisation au RGPD pour les associations

CYBERMALVEILLANCE – Apprendre à séparer ses usages pro-perso

BNP Paribas et Société Générale paient très cher pour avoir utilisé WhatsApp