15 minutes d'avance

Fiche conseil. 02

Quelles précautions prendre pour envoyer un document officiel ou une pièce d'identité ?

Les messageries électronique et instantanées sont devenues des outils de communication et de partage de référence dans l'espace professionnel comme dans l'espace personnel. Chaque jour, nous envoyons et nous recevons de nombreux messages avec des données plus ou moins confidentielles. Ex. un bulletin de paie perdu, une copie de carte d'identité pour un déplacement, un CV pour une candidature, ...

Risques

1. Les documents peuvent sortir de la zone de protection du RGPD si l'outil n'est pas conforme au RGPD.

2. Les documents peuvent être interceptées par des tierces personnes mal intentionnées : sans précautions particulières, 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.

3. Les documents risquent d'être conservés dans les boîtes email et échapper à la procédure de conservation des données mise en place.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité, limitation de la conservation, information des personnes
- 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

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

- Demander la copie de pièce d'identité lorsque cela est **strictement nécessaire**. Pour identifier les personnes, privilégier d'autres outils (ex. se connecter sur un espace donateur, n° donateur).
- Quand il s'agit d'un partage en interne, privilégier la mise à disposition des documents sur **l'espace partagé**. Il est sécurisé et seules les personnes habilitées pourront accéder au document.
- Pour envoyer un document officiel, privilégier l'usage du **service de messagerie sécurisé** de votre organisme aux messageries électroniques (ex. Google Mail, Hotmail) ou messageries instantanées (ex. WhatsApp, Messenger). Généralement, les outils gratuits ne présentent pas de garanties suffisantes au regard du RGPD. Il est plus prudent de les réserver pour des communications non confidentielles ; note aux associations : attention aux messageries personnelles des bénévoles (voir Fiche conseil. 04 relative aux messageries instantanées).
- Éviter d'écrire des données à caractère personnel dans le corps du message.
- Rendre votre document **inutilisable** dans un autre contexte. Pour cela, vous pouvez :
  - Intégrer un filigrane. Par exemple avec l'outil gratuit « Filigrane facile » mis à disposition par le gouvernement;
  - À défaut, tagger votre document avec le nom du destinataire, l'utilisation prévue, la date (recommandation Cybermalveillance);
  - Gommer ou flouter les parties les informations sensibles non nécessaires au traitement.
- **Supprimer** le document dès qu'il n'est plus utile (voir registre des durées de conservation).
- Sauvegarder les pièces jointes reçues et **archiver/supprimer** le message dès que possible. Une boite email n'est pas un espace de stockage.
- Définir des usages sécurisés conjointement **avec le RSSI et le DPO** et les inclure dans la charte informatique de l'organisme.

Pour aller plus loin

CNIL – guide de sensibilisation au RGPD pour les associations

ANSSI – hameçonnage infographie

CNIL – guide pratique : les durées de conservation des données

CYBERMALVEILLANCE – sécurité numérique – fiche pratique