15 minutes d'avance

Fiche conseil. 01

Comment partager un document contenant des données à caractère personnel ?

Dans les missions du quotidien, chacun est amené à partager des documents de travail avec ses collègues ou avec l'extérieur. Ex. les fiches d'adhésions des derniers bénévoles, les photos de la dernière action, la liste des inscrits pour tel événement ou telle formation, la liste des inscrits à la newsletter, etc.

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 envoyées à de «mauvais» destinataires par inadvertance (risque le plus courant).

3. Les DCP 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.

4. Les DCP risquent d'être conservées dans les boîtes email et échapper à la procédure de conservation des données mise en place.

5. Les DCP vont se retrouver en doublon (sauvegarde + boîte email), ce qui est contraire au principe de minimisation.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité, limitation de la conservation, minimisation
- 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

- 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.
- Préférer l'usage de services emails sécurisés aux messageries électroniques de type Google Mail ou Hotmail. 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.
- Chiffrer les pièces jointes avec des outils recommandés par les autorités de référence (ex. Cnil, ANSSI) et assurer la confidentialité en transmettant le mot de passe via un canal distinct.
- Sauvegarder les pièces jointes reçues et archiver/supprimer le message dès que possible. Une boite email n'est pas un espace de stockage.
- Éviter d'écrire des données à caractère personnel dans le corps du message.
- Limiter le nombre de destinataires.
- Définir des usages sécurisés conjointement avec le RSSI et le DPO, les inclure dans la charte informatique de l'organisme et veiller à leur mise à jour régulière selon l'évolution des pratiques.

Pour aller plus loin

CNIL – guide de sensibilisation au RGPD pour les associations

ANSSI – hameçonnage infographie

CNIL – sécuriser les échanges avec d'autres organismes

CNIL – guide pratique : les durées de conservation des données