Baker McKenzie.

Tips & Tricks
Cybersécurité

Comment réagir en cas de violation de données ?

Pandémie et télétravail peuvent être synonymes de baisse de vigilance et de désorganisation. Les risques de violation de données s'accroissent d'autant. Nous vous rappelons quelques bons réflexes à avoir.

S'organiser

Anticiper les risques en sensibilisant et formant les salariés, en organisant la remontée d'information, en créant une cellule de crise. **Ex.: créer une adresse email à contacter en cas d'identification d'une tentative de phishing.**

Qualifier les faits

S'agit il d'une violation de données ? La destruction, la perte, l'altération ou la divulgation de données personnelles de manière accidentelle ou illicite? **Ex.: transfert d'un email contenant des données personnelles au mauvais destinataire.**

Evaluer les risques pour les personnes

Quels critères ? La probabilité et la gravité du risque, le type et le volume des données touchées, l'éventuelle vulnérabilité des personnes. **Ex.: la divulgation rend possible une tentative de fraude concernant des patients.**

En cas de risques, notifier à la CNIL

Notifier dans les 72h après en avoir pris **connaissance de la violation**. L'entreprise n'a pas «connaissance» de la violation pendant qu'elle **enquête sur les faits**. Pour les traitements **transfrontaliers**, notifier à l'autorité de contrôle de l'établissement **principal**.

En cas de risques élevés, notifier aux personnes

Notifier aux personnes concernées dans les **meilleurs délais**. Anticiper les conséquences sur la **réputation de l'entreprise** en préparant sa communication

Documenter

Documenter les **causes**, les faits et les données personnelles concernées, les **conséquences** de la violation, les **mesures** prises, le **raisonnement** justifiant l'absence de notification à la CNIL ou aux personnes.

Tenir un registre

Tenir un **registre** de **toutes** les violations de données, notifiées ou non, avec la documentation associée pour pouvoir le présenter à la CNIL sur demande.

Organiser la défense de l'entreprise

Enquêter et **collecter les preuves** afin d'être en mesure de **porter plainte** si la violation est due à une **cyberattaque** ou pour engager la **responsabilité contractuelle** d'un sous-traitant si la violation résulte d'une faute de sa part.

Notre équipe est N°1 en **IT & Internet et protection des données** - *Chambers Global & Legal 500 2020* : elle vous accompagne en matière contractuelle, réglementaire et contentieuse, dans vos projets innovants, complexes et souvent internationaux, la transformation digitale, la communication électronique, les données personnelles et la cybersécurité.

Nous contacter : paritc@bakermckenzie.com

www.bakermckenzie.com