Cas concret en entreprise

Imaginez que vous travaillez dans une PME. Un collègue vous demande de lui transférer une bdd contenant des noms, adresses mails, et numéros de téléphone de clients.

-A votre avis, cette bdd contient-elle des données personnelles au sens du RGPD ? Pourquoi ?

Noms -> Identification

Adresses mails -> Numérique, identification et informatif

Numéros de téléphones -> Identification et Communication

-Le collègue vous a-t-il donné un objectif clair pour l'utilisation de ces données ? Pourquoi est-ce important de connaître la finalité avant le traitement ?

Non le collègue ne m'a pas informé de son objectif. Il est important de connaitre la finalité pour la sécurité, le contrôle d'accès, la protection de l'environnement, de respecter la politique interne à l'entreprise ainsi que la règlementation en vigueur, et de réagir en cas de violation de données.

-L'entreprise a-t-elle obtenu le consentement des personnes concernées pour que leurs données soient utilisées à cette fin ? Où et comment vérifier cette information ?

Dans le registre des traitements, les conditions générales ou la politique de confidentialité.

-Ce collègue est-t-il autorisé à accéder à cette base ? Que devez-vous vérifier pour vous en assurer ?

Dans les droits d'accès des systèmes internes, auprès du responsable informatique ou du DPO (Délégué à la Protection des Données).

-Savez-vous si la base est stockée dans un système sécurisé ? Quels outils ou méthodes pourriez-vous utiliser pour sécuriser le transfert (ex : chiffrement, protocole sécurisé, mot de passe séparé, etc…) ?

Chiffrement des données (AES, SSL/TLS), protocole sécurisé (SFTP, VPN), mot de passe séparé et gestion des accès (ACL), clé USB interne à l'entreprise.

-Est-ce que vous devez enregistrer quelque part le fait que vous avez transféré ces données ? Si oui, où et pourquoi ? (Notion de traçabilité/journalisation)

Il se trouve dans le registre des accès et transferts ou dans un outil de journalisation. Dont on peut tracer la sécurité et la responsabilité, la conformité au RGPD, la prévention des abus et la gestion des incidents.

-Quelles seraient les conséquences pour l'entreprise (et pour vous) si cette base de données était interceptée ou utilisée de manière abusive après l'envoi ?

Pour la PME : Amendes RGPD (jusqu'à 20M€ ou 4% du CA), perte de confiance, atteinte à la réputation.

Pour moi : Responsabilité professionnelle, sanctions internes, risque juridique en cas de faute grave.

-Si vous avez un doute sur la légitimité ou la sécurité de la demande, à qui devez-vous vous adresser dans l'entreprise ?

Responsable informatique, DPO, direction juridique

-En quoi le principe de « minimisation des données » peut-il influencer votre décision dans cette situation ?

Pour transmettre uniquement les données adéquates, pertinentes et limitées à ce qui est nécessaire pour leur but, et éviter toute surcharge inutile.

-Comment réagiriez-vous si votre collègue insiste pour que vous envoyez la base malgré vos réserves ?

Je lui explique les risques liés au RGPD et à la sécurité. Puis je refuse le transfert sans autorisation claire et documentée. Enfin je signale la demande suspecte au DPO ou au responsable informatique. Devoir d'alerte.

AES = Advanced Encryption Standard, algorithme de chiffrement pour protéger les données sensibles

SSL = Secure Sockets Layer, protocole de sécurisation des échanges sur internet

TLS = Transport Layer Security, assure une sécurisation renforcée des connexions

SFTP = Secure File Transfer Protocol, version sécu du FTP, utilisée pour transférer des fichiers sur un serveur de manière chiffrée

VPN = Virtual Private Network, permet de chiffrer la connexion internet et de masquer l'adresse IP

ACL = Access Control List, liste définissant qui peut accéder à un fichier ou système informatique