Thèmes : Accès aux données
Métiers: Direction des ressources humaines (DRH), Employé-e, Citoyen-ne
Types de données: Privées

Quelles précautions prendre pour garantir la sécurité des données ?

X reçoit un SMS de Y lui indiquant l'avoir rencontré-e récemment, et lui proposant de prendre un café pour mieux faire connaissance.
X est très intrigué-e, car le nom de son interlocuteur ne lui est pas connu. Un échange de messages s'ensuit.
Le lieu et le jour de leur « première rencontre », ne peut être que la veille au café restaurant Z. Mais X se souvient très bien ne pas avoir engagé de conversations avec le personnel de l'établissement, encore moins d'avoir communiqué son numéro de téléphone. X en déduit que Y a dû prendre connaissance de sa fiche d'inscription, exigé par les règles applicables durant la pandémie.
Ulcéré-e - bien que secrètement flatté-e de susciter l'intérêt -, X retourne dans l'établissement et s'entretient avec le patron. Il résulte de cet entretien qu'en effet les fiches d'inscription sont conservées dans le tiroir-caisse, accessible à tout le personnel.
Le patron de l'établissement prend des mesures immédiates en conservant lui-même toutes les fiches inscription, dans le coffre du bureau, et durant 14 jours exclusivement. Il les détruit ensuite à l'aide de sa déchiqueteuse. X fait comprendre à Y par un dernier message que tout autre relance finira par le dépôt d'une plainte pénale.

Recommandations
Selon le principe de licéité, le traitement de données personnelles doit reposer sur une base légale, sur le consentement, ou sur un intérêt privé et public prépondérant. Selon le principe de finalité, le but de la collecte doit être annoncé, et respecté. Enfin, les droits de la personnalité sont protégés par la loi, et l'employeur en est le garant vis-à-vis de ses employés. Utiliser une information reçue à titre professionnel dans un but privé viole les principes susmentionnés. Quant au principe de sécurité, il contraint le responsable de traitement, en l'occurrence, à conserver les fiches individuelles d'inscription de manière sûre, confidentielles. Le délai de 14 jours, prévue par l'ordonnance COVID19, permet de respecter le principe de proportionnalité. La suppression des données doit également être effectué de manière sécurisée.

Principes de base
art. 4 et 7 LPD : licéité, finalité, sécurité (confidentialité)

Ressources
voir le guide du PFPDT sur le mesures techniques et organisationnelles:

https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/guides/mesures-techniques-et-organisationnelles-de-la-protection-des-do.html