Thèmes : Surveillance (sens large)
Métiers: Employé-e
Types de données: Professionnelles

Mon employeur peut-il mener une campagne de vérification de la complexité des mots de passe à mon insu ?

Depuis quelques mois, l'entreprise X est dirigée par une nouvelle personne, férue de sécurité informatique et
sensibilisée aux enjeux en la matière.
Connaissant les solutions de facilité que tout être humain adopte si on lui en laisse l'occasion, elle suspecte que la politique, comme la pratique, au sein de l'entreprise en matière de mot de passe laisse à désirer, ce qui fragilise la sécurité de l'information.
Elle mandate donc une entreprise de hacking éthique et la charge de vérifier le niveau de complexité des mots de passe de tous ses collaboratrices et collaborateurs.
Les trois-quarts reçoivent alors un message les informant du trop bas niveau de sécurité des mots de passe choisis.
Y compris les gestionnaires RH, qui s'offusquent de cette manière de faire et sollicitent un entretien avec la
nouvelle direction.
Lors de l'entretien, il apparaît que, si le souci de la direction est légitime, la méthode utilisée laisse à désirer
et viole les principes applicables au traitement des données personnelles.
Le test aurait pu être fait de manière conforme après en avoir averti le personnel et lui avoir donné un délai pour modifier, cas échéant, les mots de passe dans le sens requis.

Recommandations
A moins qu'un règlement ne prévoit clairement les règles en matière d'utilisation des outils bureautiques,
les mesures de sécurité à prendre et ne mentionne les contrôles pouvant être effectués,
il n'est pas licite de contrôler le niveau de sécurité des mots de passe à l'insu des collaborateurs.
La transparence de la collecte et la bonne foi imposent de ne pas surveiller les collaborateurs à leur insu,
et de leur indiquer les contrôles à venir.

Principes de base
Art. 4, 12 LPD

Licéité, bonne foi et transparence de la collecte

Ressources
Arrêt de la Cour administrative du canton du Juras, ADM 92/2009, du 25 février 2013. L'analyse des données de connexion à l'insu des employés correspond à une collecte illicite de données. Voir pdf disponible ici

https://thinkdata.numerich.ch/ressources/ADM-92_2009_campagne_mots-de-passe.pdf

https://www.jura.ch/JUST/Instances-judiciaires/Tribunal-cantonal/Revue-jurassienne-de-jurisprudence/2013.html