Thèmes : Application RGPD
Métiers: Cadre, Direction des systèmes d'information
Types de données: Professionnelles

Quelles précautions prendre comme DSI à l'achat de nouveaux produits ?

X dirige une entreprise de construction et travaux publics.
Pour mener certaines activités de manière efficiente, comme la gestion des chantiers, le chef de projet lui propose un nouvel outil, très performant, qui permettra un partage de l'information en ligne.
Validé par X, cet achat est bloqué par Y, nouvel adjoint de X, qui se targue de s'y connaître en conformité et essaie de sensibiliser X à l'importance de rester « dans les clous » de loi, pour des raisons d'image. Or, il doute de la conformité du logiciel proposé car il s'agit d'une solution de cloud américaine.
Agacé, mais conscient que c'est précisément le rôle de son adjoint de la mettre en garde, X fait vérifier la conformité du l'outil en question, d'autant plus qu'il envisage d'ouvrir une succursale en France.
Il s'avère que le logiciel est conçu par une société américaine, signataire du bouclier de protection (Privacy Shield), certifiée ISO 27001, et que les conditions générales prévoient le respect des principes applicables en protection des données tant en Suisse qu'en Union européenne. L'achat peut être validé.

Recommandations
La loi fédérale sur la protection des données donne un cadre pour le traitement des données personnelles effectué en Suisse. Lorsque des données personnelles sont transmises à l'étranger, il faut vérifier qu'elles seront soumises à une législation assurant un niveau de protection adéquat. Font partie des vérifications de base, pour un sous-traitant américain, celle de savoir si celle-ci est signataire du cadre de sécurité mis en place avec les autorités américaines pour garantir le respect des principes légaux tant de la LPD que du RGPD. Ensuite, les conditions générales et spécifiques du contrat doivent être analysées et cas échant complétées de sorte que la sécurité des données, mais aussi le droit d'accès des personnes concernées soient garanties. Par ailleurs, le règlement européen s'appliquera au traitement de données personnelles effectué par la succursale en France, qu'elle soit responsable de traitement ou sous-traitant, selon les cas, de l'entreprise suisse.

Principes de base
art. 4 LPD (proportionnalité), art. 6 (transmission à l'étranger), art. 7 Sécurité (confidentialité, disponibilité, intégrité), art. 8 LPD, Droit d'accès ; RGPD.

Ressources
Voir la page du PFPDT et les différents liens concernant toute information sur la communication de données personnelles à l'étranger ainsi que la liste des Etats, et le Privacy Shield :

https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html