Mémento : nouvelle loi sur la protection des données

La nouvelle loi sur la protection des données est entrée en vigueur le 1er septembre 2023. Elle renforce les exigences posées aux petites et moyennes entreprises concernant la protection des données et la conformité en la matière.

Le principe de l'approche basée sur les risques continue de s'appliquer. Autrement dit, plus les données sont sensibles, plus les précautions à prendre pour leur traitement sont importantes. Que ce soit au cours d'un entretien téléphonique avec un client, au moment de payer une facture ou dans le cadre d'un entretien d'embauche, les données personnelles font partie du quotidien des entreprises. Toutes les PME sont donc concernées par la nouvelle loi sur la protection des données (LPD) et par les changements qui en découlent. Il importe qu'à l'avenir, les directions accordent davantage d'attention à la protection des données et en fassent un enjeu stratégique.

La nouvelle loi sur la protection des données se limite à la protection des données des personnes physiques. Elle ne couvre plus la protection des personnes morales. La nouvelle loi sur la protection des données (LPD) ne prévoit pas d'obligation de tenir un registre des traitements de données personnelles pour les PME qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.

La Confédération suisse conseille aux entreprises de prendre en compte au minimum les huit points suivants et, le cas échéant, de mettre en œuvre des mesures correspondantes ou de procéder à leur adaptation.

1. Seules les données des personnes physiques sont encore couvertes, et plus celles des personnes morales.
2. Les données génétiques et biométriques entrent désormais dans la définition des données sensibles.
3. Les principes de « Privacy by Design » et de « Privacy by Default » sont désormais d'application. Le principe de « Privacy by Design » (protection des données dès la conception) signifie, pour les développeurs, qu'ils doivent intégrer la protection et le respect de la vie privée des utilisatrices et utilisateurs dans la structure même du produit ou du service qui collecte des données personnelles. Le principe de « Privacy by Default » (protection des données par défaut) assure quant à lui le niveau de sécurité le plus élevé par défaut dès la mise en circulation du produit ou du service, c'est-à-dire en activant, sans aucune intervention des utilisatrices et utilisateurs, toutes les mesures nécessaires à la protection des données et à la limitation maximale de leur utilisation. Autrement dit, tous les logiciels, le matériel et les services doivent être configurés de manière à protéger les données et à respecter la vie privée des utilisateurs.
4. Des analyses d'impacts doivent être menées en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

5. Le devoir d'informer est étendu : la collecte de toutes les données personnelles (et non plus uniquement de données dites sensibles) doit donner lieu à une **information** préalable de la personne concernée.
6. La tenue d'un registre des activités de traitement devient obligatoire. L'ordonnance d'application prévoit toutefois une exemption pour les PME dont le traitement des données comporte un risque limité d'atteinte à la personnalité des personnes concernées.
7. Une annonce rapide est requise en cas de violation de la sécurité des données. Elle doit être adressée au Préposé fédéral à la protection des données et à la transparence (PFPDT).
8. La notion de profilage (soit le traitement automatisé de données personnelles) fait son entrée dans la loi.

Pour déterminer si des mesures doivent être prises dans votre entreprise, il convient de clarifier les questions suivantes :

- Quelles données personnelles sont traitées dans l'entreprise et dans quel but ?
- Existe-t-il une déclaration de protection des données et est-elle conforme aux nouvelles dispositions ?
- Comment les personnes concernées seront-elles informées à l'avenir du traitement de leurs données, conformément à la loi ?
- Quels sont les risques individuels dans l'entreprise et comment peuvent-ils être minimisés ?
- Qui est responsable de quoi ?
- Les collaboratrices et collaborateurs ont-ils été sensibilisés au traitement des données personnelles et, le cas échéant, formés à leur utilisation ?

AM Suisse recommande à ses membres d'adapter spécifiquement les documents mis à disposition par l'Union suisse des arts et métiers (usam) à la situation de leur entreprise et aux processus internes et, le cas échéant, de confier le traitement des données de commande à des prestataires externes. Pensez à tenir compte des remarques préliminaires figurant au début des modèles.

Vous trouverez les documents ici :

https://www.sgv-usam.ch/fr/grands-axes-politiques/politique-économique/sous-pages/nouveau-droit-de-la-protection-des-données

Il peut éventuellement être indiqué de recourir aux services d'experts en protection des données pour la vérification et la mise en œuvre. AM Suisse se fera un plaisir de vous mettre en contact avec des spécialistes appropriés.

CZE 30.08.23