WilhelmGilliéron
AVOCATS

PROTECTION DES DONNÉES

La nouvelle loi fédérale sur la protection des données : faire preuve de pragmatisme !

Auteur: Wilhelm Avocats | Le : 2 octobre 2023

La nouvelle loi fédérale sur la protection des données : faire preuve de pragmatisme !

Le 1er septembre 2023, la nouvelle loi fédérale sur la protection des données est entrée en vigueur. Sa médiatisation, appuyée par le fort écho donné depuis 2018 au RGPD, a eu pour effet une prise de conscience soudaine et quasiment générale de la nécessité qu'il y a à s'intéresser à cette fameuse protection des données.

Ressentie comme une contrainte par certains, une usine à gaz par beaucoup, l'obligation de se mettre en conformité n'en est pas moins un devoir légal qui pèse désormais sur toute entité amenée à traiter des données. Le texte de la loi, tout comme l'expérience, souligne toutefois le fait que cette mise en conformité n'est pas aussi lourde qu'il n'y paraît.

Sans évidemment prétendre à l'exhaustivité, nous nous proposons ici de faire le tour de quelques questions pratiques que tout entrepreneur se pose :

1. Dans quel délai dois-je m'assurer que les traitements de données personnes que j'opère dans le cadre de mon activité sont conformes à cette nouvelle loi ?

Il n'y a aucun délai de grâce. L'entrée en vigueur de la nouvelle loi ayant été annoncée il y a de cela près de un an, le législateur a considéré que ceux qui y sont soumis avaient tout loisir de se mettre en conformité et que, partant, elle entrerait en vigueur et serait

dès lors appliquée dès le 1er septembre 2023.

Rassurez-vous cependant ; une grande partie des PME ont, tout comme vous, repoussé cet exercice et ne s'y intéresse que maintenant. Le Préposé fédéral ayant lui-même passablement à faire avec la mise en œuvre de cette nouvelle loi, vous disposez en pratique encore de quelques mois avant que d'éventuels contrôles ne soient susceptibles d'avoir lieu.

2. Suis-je censé être conforme à 100% ?

La réponse théorique serait oui. La réponse réaliste et pratique sera non. Quelle que soit la taille de l'entreprise, il est très difficile pour ne pas dire impossible d'assurer que tous les traitements de données personnelles et processus y relatifs soient 100% conformes à la nouvelle loi. Ce qui importe, c'est de démontrer que vous êtes conscients de l'importance de ces traitements et avez pris les mesures raisonnablement exigibles que l'on peut attendre de votre part pour être aussi conforme que possible aux exigences posées par la loi.

3. Quelles sont ces mesures raisonnables que je dois prendre ?

Le strict minimum consiste à vous assurer que vous avez la **documentation contractuelle** nécessaire pour assurer la **transparence nécessaire** quant aux traitements que vous opérez. En pratique, cela implique avant tout la mise sur pied des documents suivants :

- une politique en matière de confidentialité, généralement disponible sur votre site et séparée de vos conditions générales, qui définit les traitements opérés tant au travers du recours à votre site internet qu'en relation avec l'exécution de vos prestations.

- un accord en matière de traitement de données, qui prend généralement la forme d'une annexe aux contrats que vous êtes susceptibles de conclure avec vos prestataires en particulier. La loi impose en effet désormais que les traitements de données résultant de l'exécution d'un contrat fassent l'objet d'un accord entre les entités concernées. Le plus souvent, vos prestataires devraient en avoir un, mais il est de bon ton d'en avoir un sous la main et, de surcroît, d'en avoir un lorsque vous-même jouer le rôle de prestataire vis-à-vis de vos clients.

- Une bannière en matière de cookies qui, pour le moment, n'exige pas nécessairement un accord exprès en droit suisse, mais dont les bonnes pratiques et tendances – malheureuses – tendent à se diriger vers une telle formule, avec une granularité des cookies acceptables (essentiels, fonctionnels, analytiques, etc.)

- Une notice interne concernant les traitements de données relatif à votre personnel. Lorsque votre personnel est limité, des dispositions y relatives dans le contrat de travail peuvent suffire. Lorsque ce personnel atteint une certaine masse critique, il est préférable d'adopter une directive interne définissant le type de traitement opéré en relation avec les données des employés et de porter bien entendu cette directive à leur connaissance.

La seconde obligation la plus importante consiste en les **mesures de sécurité** que vous prenez pour assurer la confidentialité, l'intégrité et la disponibilité des données que vous traitez. Ces mesures comprennent deux facettes :

- Tout d'abord, il vous incombe de **prendre les mesures techniques nécessaires**, notamment sur le plan informatique, pour vous assurer que le niveau choisi est adéquat par rapport au type de données que vous traitez. Le niveau de ces attentes sera en effet différent suivant que vous évoluez dans un rapport *business-to-business* où les seules données

personnelles traitées résident en les nom prénom et adresse email de vos correspondants, ou que vous exploitez une clinique privée avec de nombreuses données de santé de vos patients.

- Ensuite, annoncer toute **violation en matière d'incident en matière de sécurité**. Ce point n'est pas à prendre à la légère puisque, aujourd'hui, on aime à dire que « la question n'est pas de savoir si l'on va être touché par un tel incident, mais quand ». En pratique, il est probable que vous recourriez dans le cadre de vos activités à des prestataires informatiques qui, eux, disposeront (ou devraient) disposer des processus nécessaires pour vous informer de tout incident, à charge ensuite pour vous de procéder à l'analyse nécessaire dudit incident en collaboration avec votre prestataire. Encore faut-il cependant que vous vous assuriez que l'accord de traitement de donnée susmentionné que vous avez avec eux définisse cette procédure ; en tant que responsable de traitement, c'est bien à vous qu'il incombe de vous assurer que vos obligations en la matière sont respectées vis-à-vis des individus dont vous traitez les données.

4. On m'a parlé d'un registre des activités de traitements. De quoi s'agit-il et suis-je obligé d'en avoir un ?

Le registre des activités des traitements a pour objectif de dresser un panorama des flux de données au sein de l'entreprise. Quelles sont les données traitées, dans quels buts, avec quels partenaires, y a-t-il des transferts à l'étranger et, si oui, sur quelle base ?

L'exercice, fastidieux, nécessite un travail qui doit être fait à l'interne d'inventaire. L'établissement d'un tel registre n'est toutefois pas obligatoire pour les entreprises qui ont moins de 250 employés et qui ne traitent pas à grande échelle des données sensibles comme le sont par exemple des données de santé (cas d'une clinique privée par exemple) ou n'établissent pas de profil à risque élevé.

C'est dire qu'en réalité, la grande majorité des PME ne sont pas tenues d'établir un tel registre. On ne saurait cependant ignorer que s'interroger sur les flux de données impliqués par nos activités et les partenaires auxquels nous recourrons pour ce faire sera un bon moyen de s'interroger notamment sur la transparence due aux individus dont nous traitons les données et l'existence – nécessaire – d'un accord de traitement de données avec ces partenaires.

5. Dois-je systématiquement demander le consentement pour traiter des données ?

Non, loin s'en faut. En réalité, il existe de nombreux motifs justificatifs prévus par la loi qui autorise un tel traitement sans nécessairement avoir à obtenir l'accord de la personne concernée, et ce même si l'on traite des données sensibles (comme des données de santé), une différence substantielle avec le RGPD.

En pratique, deux motifs sont importants :

- Tout d'abord, le fait que le traitement repose sur une base légale. Ainsi en va-t-il par exemple lorsque des données doivent être communiquées à une caisse-maladie ou un organisme LPP conformément à la loi.

- Ensuite, lorsque l'entreprise a un intérêt privé à traiter des données, qui doit être prépondérant par rapport à celui de l'individu dont les données sont traitées. Un tel intérêt est notamment présent lorsque ce traitement est exigé pour permettre la conclusion et l'exécution d'un contrat.

Ces deux motifs justificatifs pourront donc régulièrement être invoqué en pratique pour se passer du délicat exercice consistant, entre autres choses, à devoir le cas échéant obtenir le consentement de l'individu concerné, un consentement d'autant plus problématique qu'il doit pouvoir être librement consenti et être retiré en tout temps ce qui, en pratique, n'est pas sans poser quelque difficulté.

6. Qu’est-ce que je risque si je viole la loi ?

S’il est loisible à un individu qui s’estime lésé par un traitement de saisir le juge civil, une telle probabilité apparaît minime au vu des coûts exigés par l’ouverture d’une telle action. En pratique, le risque résultera donc le plus souvent soit d’une intervention du Préposé (suite à une inspection ou une dénonciation d’un particulier), soit d’une éventuelle plainte pénale.

L’intervention du Préposé peut résulter en une interdiction de continuer à procéder au traitement des données concerné jusqu’à ce qu’il soit remédié à la situation ce qui, suivant les cas, représente un véritable risque opérationnel pour la continuité des affaires. Sans doute s’agit-il là, en réalité, du risque le plus important.

Les sanctions pénales exigent le dépôt d’une plainte qui, en pratique, devra émaner de l’individu concerné et qui ne peut porter que sur un certain nombre d’obligations. Une telle plainte peut en théorie résulter en la condamnation personnelle de l’organe (soit de la personne physique et non de la société) à une amende pouvant aller jusqu’à CHF 250’000.–. Même si l’on ignore la manière dont les autorités pénales appliqueront ces dispositions, leur pouvoir coercitif risque d’être limité dans la mesure où le manquement au devoir doit être intentionnel et qu’un tel montant apparaît *a priori* comme un maximum, et non comme la moyenne.

1. Au final, à quoi je dois penser ?

Si l’on devait résumer la nouvelle loi fédérale sur la protection des données en deux mots, je choisirais ceux de **transparence** et de **sécurité**.

Plus vous **renseignez** les individus dont vous traitez les données de manière transparente, moins vous vous exposez. Il convient dès lors de vous interroger sur vos flux de données : quelles données ? de qui ? dans quels buts ? où sont-elles stockées ? recourrez-vous à des partenaires ? y a-t-il à un moment ou l’autre des transferts à l’étranger ? Combien de temps les conservez-vous ? Répondre à ces questions puis les mettre en forme dans vos documents contractuels vous permettra d’accomplir un bon bout de chemin.

Prendre les **mesures organisationnelles adéquates** en vue d’assurer la sécurité de vos données, ce n’est pas seulement s’interroger sur la sécurité informatique, mais également sur des mesures simples mais essentielles, comme la formation, même basique, des employés, ou éviter que des écrans et autres postes de travail faisant état de données personnelles ne soient visibles par votre clientèle ou restent allumés et accessibles à chacun.

En conclusion, si la loi fédérale sur la protection des données fait peur, il n’est pas nécessaire de paniquer. Un certain nombre de mesures simples et faciles à mettre en œuvre vous permettront de témoigner des efforts raisonnablement exigibles que l’on peut attendre de votre part. Les prendre, ce n’est pas seulement remplir ses obligations légales, c’est aussi démontrer aux individus toujours plus sensibilisés à ce sujet que vous vous en préoccupez.

Source :
https://www.wg-avocats.ch/actualites/protection-des-donnees/la-nouvelle-loi-federale-sur-la-protection-des-donnees-faire-preuve-de-pragmatisme/