

Nouvelle Loi sur la protection des données

I. Contexte

La nouvelle Loi sur la protection des données est entrée en vigueur ce 1er septembre 2023. C'est l'occasion de faire un bref état des lieux de certaines des principales nouveautés de cette loi et des premières mesures à prendre en vue de s'y conformer.

II. Les principales nouveautés de la nouvelle Loi sur la protection des données

Bien que les principes de traitement des données applicables jusqu'à présent (licéité, bonne foi, proportionnalité, respect des finalités de traitement et exactitude) demeurent d'actualité (art. 6 LPD), il faut désormais y ajouter ceux de Privacy by design et de Privacy by default et de sécurité des données (art. 7 et 8 LPD) qui prévoient en substance que les responsables de traitement doivent mettre en place des mesures techniques et organisationnelles appropriées pour assurer une sécurité adéquate des données et que, dès leur conception, le traitement respecte les prescriptions légales et que des prééglages appropriés limitent ce traitement au minimum requis par sa finalité.

Le nouveau droit prévoit que les responsables de traitement et leurs sous-traitants devront chacun tenir un registre des activités de traitement (art. 12 al. 1 LPD), lequel devra contenir à tout le moins les indications listées par la loi. Cette obligation ne s'applique pas aux entreprises employant moins de 250 collaborateurs et aux personnes physiques, à moins qu'elles ne traitent des données sensibles à grande échelle ou que leur activité de traitement ne constitue un profilage à risque élevé (art. 24 OPDo).

Avant de procéder à un traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne

DOCUMENTATION

www.athemis.ch



concernée, qui existe notamment en cas de traitement de données sensibles à grande échelle ou de surveillance systématique de grandes parties du domaine public, le responsable de traitement devra procéder à une analyse d'impact (art. 22 LPD).

La nouvelle loi prévoit désormais un devoir d'annonce au PFPDT en cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 24 LPD). En outre, lorsque cela est nécessaire à sa protection ou si le PFPDT l'exige, le responsable de traitement devra également informer la personne concernée.

Le responsable de traitement aura également l'obligation d'informer la personne concernée lors de la collecte de données personnelles sur son identité, la finalité du traitement et les destinataires auxquels les données personnelles sont transmises ainsi que le nom de l'État par une éventuelle communication à l'étranger et les éventuelles garanties permettant d'assurer un niveau de protection adéquat des données transmises (art. 19 LPD).

Ces devoirs d'informations sont complétés par les droits des personnes concernées, et notamment les droits d'accès et à la portabilité des données (art. 25 et 28 LPD), qui prévoient, en substance, que toute personne a le droit d'avoir accès, en principe gratuitement, aux données personnelles la concernant traitées par un responsable de traitement ainsi qu'à la remise de celles-ci sous un format électronique couramment utilisé. En outre, il est rappelé que la personne concernée a également le droit à s'opposer au traitement de ses données personnelles, de faire effacer et détruire des données en cas de traitement illicite, de faire rectifier des données inexacts ou d'en faire mentionner le caractère litigieux.

III. Quelques mesures à mettre en œuvre rapidement

Dans un premier temps, il est important pour chaque responsable de traitement d'identifier les traitements de données qu'il effectue et d'évaluer les risques qu'ils peuvent représenter.

Pour ce faire, la mise en place d'un registre des activités de traitement, lorsqu'il n'est pas obligatoire, peut s'avérer utile.

En outre, il est également conseillé de vérifier, et d'éventuellement adapter la déclaration de protection des données et les différents contrats, notamment de sous-traitance, contenant des clauses en matière de protection des données.

Enfin, il est recommandé de mettre en place des directives et des processus internes permettant de répondre aux potentielles demandes d'accès des personnes concernées ainsi qu'en cas de violations



de la sécurité des données. A cet égard, il serait judicieux d'accompagner ces mesures d'une sensibilisation des collaborateurs à la question de la protection des données.

Athemis Avocats Sàrl se tient volontiers à votre disposition pour vous renseigner sur vos différentes obligations en matière de protection des données ainsi que pour vous accompagner dans votre processus de mise en conformité sur le plan juridique à la LPD.

La présente newsletter n'a aucune prétention d'exhaustivité et elle ne dispense pas chaque responsable de traitement de vérifier qu'il respecte les nouvelles normes en vigueur. Athemis Avocats Sàrl décline toute responsabilité à cet égard.

La Chaux-de-Fonds le 1er septembre 2023, Me Laurent Burkhard

