suisse.ing

Schweizerische Vereinigung Beratender Ingenieurunternehmungen
Union Suisse des Sociétés d'Ingénieurs-Conseils
Unione Svizzera degli Studi Consulenti d'Ingegneria
Uniun svizra dals biros d'inschigneria consultativs
Swiss Association of Consulting Engineers

Berne, juin 2023

FACT-SHEET RELATIVE À LA RÉVISION DU DROIT DE LA PROTECTION DES DONNÉES

La nouvelle loi fédérale sur la protection des données (nLPD) entre en vigueur le 1er septembre 2023. La révision s'est fixé les objectifs suivants:

- *rapprocher en partie la loi du règlement général sur la protection des données (RGPD) de l'Union européenne;*
- *assurer la protection des données plus en amont;*
- *sensibiliser davantage les personnes concernées au fait des risques que représentent les nouvelles technologies pour la protection de la personnalité;*
- *améliorer la transparence des traitements de données;*
- *améliorer le contrôle et la maîtrise des données après leur divulgation; et*
- *protéger les mineurs.*

La présente fact-sheet se propose de donner un aperçu des principales nouveautés avancées par la révision et de relever certains points à retenir pour l'activité spécifique des bureaux d'ingénieurs.

Limitation du champ d'application aux personnes physiques

La loi en vigueur sur la protection des données régit le traitement des données concernant les personnes physiques aussi bien que morales (art. 2, al. 1, LPD). Autrement dit, le traitement de données commerciales tombe également sous le coup de la loi actuelle. S'adossant au RGPD et soulignant le manque de pertinence pratique du champ d'application aux données des personnes morales, la révision prévoit de supprimer ce champ d'application partiel. En conséquence, la nouvelle loi ne concernera plus que le traitement des données personnelles des personnes physiques (art. 2, al. 1, nLPD).

Nota bene: Étant donné que les bureaux d'ingénieurs traitent des **données personnelles** (i.e. toutes les informations concernant une personne physique identifiée ou identifiable [art. 5, let. a, nLPD], telles que nom, date de naissance, adresses, photos ou toute autre indication sur la personne, indépendamment de la forme et du contenu), ils sont tenus de respecter les prescriptions de la LPD révisée. Il est entendu par **traitement** notamment la collecte, l'utilisation, la conservation, mais aussi l'effacement de données (cf. art. 5, let. d. nLPD). Les données sans référence à des personnes, c'est-à-dire plans, calculs et autres, ne constituent pas des données personnelles et ne sont donc pas soumises à la législation sur la protection des données.

Protection des données dès la conception et par défaut

Les principes de «privacy by design» (protection des données dès la conception) et de «privacy by default» (protection des données par défaut) sont nouvellement inscrits dans la loi révisée (art. 7 nLPD). Ils contraignent les entreprises, et partant les bureaux d'ingénieurs, à mettre en œuvre dès la conception des projets les principes de traitement prévus par la loi (art. 6 nLPD) en prenant des mesures de protection techniques et organisationnelles appropriées. Selon le principe de la protection des données dès la conception, entreprises et bureaux d'ingénieurs devront concevoir leurs applications (p. ex. leur site Internet) de sorte que, entre autres, les données soient systématiquement anonymisées ou effacées. La protection des données par défaut, quant à elle, préserve les utilisateurs d'offres en ligne privées qui ne prévoient pas de conditions d'utilisation ni les droits d'opposition des personnes concernées qui en découlent: seules sont traitées les données absolument nécessaires à la finalité poursuivie.

Nota bene: Pour les bureaux d'ingénieurs, l'introduction des principes de protection des données dès la conception et par défaut sera surtout pertinente pour ce qui est du **site Internet de l'entreprise**, où tous deux doivent être implémentés. Il est primordial que le traitement se limite au minimum de données requises (traiter autant de données que nécessaire, mais aussi peu que possible). Il convient, autant que faire se

peut, de recourir à l'anonymisation et à la pseudonymisation. Une fois atteinte la finalité du traitement des données, celles-ci doivent en outre être effacées, à moins que des délais de conservation légaux ne s'y opposent.

Conseiller à la protection des données

L'art. 10 nLPD permet aux entreprises de désigner un conseiller à la protection des données. Ce dernier sert d'interlocuteur pour les personnes concernées par le traitement des données et pour les autorités. Il forme l'entreprise aux aspects liés à la protection des données et concourt à l'application des prescriptions en la matière.

Nota bene: La désignation d'un conseiller à la protection des données reste facultative. La démarche n'a d'ailleurs de sens que pour les très grands bureaux d'ingénieurs. Si l'entreprise ne nomme pas de conseiller à ce titre, la déclaration de protection des données devra néanmoins mentionner une **personne de contact** auprès de laquelle les personnes concernées puissent s'adresser en cas de questions ou de demande d'exercice de leurs droits.

Analyse d'impact relative à la protection des données personnelles

Si le traitement de données envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, l'art. 22 nLPD prévoit que soit effectuée au préalable une analyse d'impact. L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe surtout lorsqu'un profilage (i.e. le traitement automatisé de données personnelles dans le but d'évaluer certains aspects personnels relatifs à une personne physique [art. 5, let. f, nLPD]) à risque élevé ou un traitement à grande échelle de données sensibles est prévu. L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures propres à protéger la personnalité et les droits fondamentaux de cette dernière.

Nota bene: Les bureaux d'ingénieurs n'auront à procéder à une analyse d'impact relative à la protection des données personnelles que dans des cas exceptionnels. En effet, ils ne traitent pratiquement jamais de données personnelles sensibles, telles des informations concernant la santé, les mesures d'aide sociale, les opinions religieuses, philosophiques, politiques ou syndicales, etc. (voir art. 5, let. c, nLPD).

Pourraient constituer des exceptions l'utilisation de nouvelles technologies pour le traitement des données ou la réalisation de profilages et/ou d'analyses de marché au moyen de données personnelles à des fins de positionnement sur le marché ou d'optimisation des ventes.

Registre des activités de traitement

En vertu de l'art. 12 nLPD, les responsables du traitement (i.e. la personne ou l'entreprise qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles [art. 5, let. j, nLPD]) ainsi que les sous-traitants (i.e. la personne ou l'entreprise qui traite des données personnelles pour le compte du responsable du traitement [art. 5, let. k, nLPD]) tiendront à l'avenir chacun un registre de toutes leurs activités de traitement. Les entreprises employant moins de 250 collaborateurs au 1er janvier de l'année concernée ainsi que les personnes physiques sont quant à elles déliées de cette obligation, à moins que le traitement porte sur des données sensibles à grande échelle ou que le traitement constitue un profilage à risque élevé (art. 24 de la nouvelle ordonnance sur la protection des données [OPD]).

Nota bene: L'obligation de tenir un tel registre est susceptible d'entraîner une charge administrative énorme pour les entreprises. Aussi faut-il saluer la dérogation prévue au niveau de l'ordonnance, et dont la plupart des bureaux d'ingénieurs pourront probablement profiter sachant qu'ils ne traitent que peu de données personnelles sensibles. Il conviendra d'examiner au cas par cas si la disposition dérogatoire s'applique ou non à une entreprise.

Devoir d'informer consolidé

Afin de répondre à l'objectif de transparence visé par la révision, l'art. 19 nLPD consolide le devoir d'information pour les entreprises. Désormais, une entreprise qui envisage de collecter des données personnelles doit en principe en informer au préalable et de manière adéquate la personne concernée. Concrètement devront être communiqués l'identité et les coordonnées du responsable du traitement, de même que la finalité du traitement et, le cas échéant, les destinataires des données personnelles. Si les données ne sont pas collectées directement auprès de la personne concernée, les catégories de données personnelles traitées devront, de plus, lui être communiquées. En cas de transmission de données à l'étranger, il convient (contrairement au RGPD) également de fournir des informations sur l'État destinataire et les éventuelles garanties visant à assurer un niveau de protection des données approprié au sein de l'État tiers.

Nota bene: Compte tenu de ce qui précède, les entreprises et les bureaux d'ingénieurs sis en Suisse devront vraisemblablement réviser ou compléter la plupart de leurs **déclarations de protection des données** – surtout si des données personnelles sont communiquées à l'étranger (ce qui au demeurant, au vu de l'implémentation de services tels que Google Analytics, sera pratiquement toujours le cas lors de l'utilisation de sites Internet, d'applications, etc.). À noter que le devoir d'informer ne s'appliquera pas aux données personnelles qui ne sont saisies qu'accessoirement ou par hasard. L'art. 20 nLPD mentionne, outre celle-ci, de nombreuses autres exceptions (p. ex. si les personnes concernées disposent déjà des informations ou si le traitement des données est prévu par la loi). Relevons ici encore qu'une personne concernée devra justifier de son identité (moyennant une pièce officielle) pour que son droit à l'information puisse être pris en considération.

Droit d'accès

Le droit d'une personne concernée à demander si des données personnelles la concernant sont traitées est consolidé dans le cadre de la révision de la LPD. L'art. 25 nLPD dresse une liste étendue des informations que le responsable du traitement aura au moins à transmettre (p. ex. la durée de conservation des données personnelles traitées). Cette disposition prévoit par ailleurs que la personne concernée devra en principe recevoir toutes les informations nécessaires pour qu'elle puisse faire valoir les droits qui lui sont accordés selon la nouvelle LPD. En règle générale, les renseignements doivent être fournis gratuitement.

Nota bene: Si le droit d'accès de la personne concernée n'est pas nouveau au regard de la loi suisse sur la protection des données, il voit toutefois son champ d'application étendu – avec le surcroît de travail qui en découle pour les entreprises et les bureaux d'ingénieurs. Ces derniers auront donc tout intérêt à mettre en place une **procédure** simple pour traiter ce type de demandes (lesquelles devraient se multiplier à l'avenir). Il faut en l'occurrence tenir compte du fait que le droit d'accès (comme tous les autres droits des personnes concernées) peut être refusé, limité ou différé sous certaines conditions (p. ex. sur la base de dispositions légales, d'intérêts publics ou privés prépondérants, etc.).

Devoir d'annoncer les violations de la sécurité des données

Aux termes de l'art. 24 nLPD, le responsable du traitement devra nouvellement annoncer au Préposé fédéral à la protection des données et à la transparence (PFPDT) les cas de violation de la sécurité des données entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. L'annonce au PFPDT doit être faite dans les meilleurs délais et indiquer au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées.

Nota bene: Le devoir d'annoncer les violations de la sécurité des données constitue une nouvelle obligation pour les responsables du traitement des données. Alors que la nLPD soumet cette obligation à un «risque élevé» d'atteinte à la personnalité ou aux droits fondamentaux des personnes concernées, le seuil d'annonce du RGPD est en revanche plus bas et s'applique déjà à un «risque simple». Sachant que les bureaux d'ingénieurs n'ont (du moins en règle générale) que rarement à traiter des données personnelles sensibles, il y a fort à supposer qu'ils ne se verront confrontés à de tels devoirs d'annonce que dans des situations exceptionnelles.

Conclusion

Les modifications relatives à la révision de la loi sur la protection des données, présentées ici de façon non exhaustive, étendent principalement les droits des personnes concernées par le traitement des données personnelles. L'extension de ces droits induit en parallèle une charge de travail supplémentaire non négligeable pour les entreprises traitant des données. Aux fins de ramener ce surcroît de travail autant que possible à une tâche unique, il leur est vivement recommandé de mettre en place les structures et procédures internes ad hoc. Cet investissement certes important permet néanmoins, outre le fait de contenir à long terme la charge de travail de l'entreprise ou du bureau d'ingénieurs dans des limites raisonnables, de garantir simultanément le respect des dispositions légales. Compte tenu enfin du nouveau régime de sanctions prévoyant des amendes pouvant atteindre jusqu'à 250 000 francs (art. 60 nLPD), les entreprises et les bureaux d'ingénieurs seront fort avisés de prendre cette thématique à bras le corps et d'effectuer tous les préparatifs requis avant l'entrée en vigueur de la nLPD au 1er septembre 2023.