# Aide-mémoire & checklist

**Mise en œuvre de la nouvelle loi sur la protection des données par les aérodromes suisses**

**Etat des lieux au 1er août 2023**

La loi actuelle sur la protection des données est encore en vigueur jusqu'au 31 août 2023. Le 1er septembre 2023, la loi suisse révisée sur la protection des données (appelée « nLPD ») entrera en vigueur. Les aérodromes devront également se pencher sur les dispositions légales. L'ASA résume ci-après les aspects les plus importants du point de vue des aérodromes pour les opérations préparatoires en vue de l'introduction de la nouvelle loi. Cela ne prend en compte que les situations standard sur un aérodrome qui ne présentent pas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (cela signifie qu'en règle générale, il n'y a pas de traitement automatisé de données personnelles [appelé « profilage »] et qu'une analyse d'impact sur la protection des données ne doit par conséquent pas être effectuée).

La nouvelle loi sur la protection des données se trouve ici : https://www.fedlex.admin.ch/eli/cc/2022/491/fr

Le nouveau règlement d'exécution, l'Ordonnance sur la protection des données (nOPDo), est disponible ici : https://www.fedlex.admin.ch/eli/oc/2022/568/fr

Le nouveau droit de la protection des données se caractérise par les nouveaux **éléments** suivants :

- Des **formalités plus strictes**, notamment par l'obligation de tenir un registre des activiés de traitement des données. La nLPD allège toutefois cette obligation pour les entreprises et organisations de moins de 250 collaborateurs. Les entreprises de moins de 250 collaborateurs sont en principe dispensées d'établir un registre des activités de traitement, sauf si des données personnelles sensibles sont traitées à grande échelle ou si un profilage à haut risque est effectué. Il faut cependant toujours respecter les directives concernant le **transfert de données à l'étranger**.
- de **nouvelles obligations pour les entreprises** : Le devoir d'informer est étendu et il existe un droit à la portabilité des données (le droit des personnes concernées de recevoir leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine) et des analyses d'impact sur la protection des données doivent être réalisées dans certaines conditions (voir introduction ci-dessus).
- **l'introduction de comportements sanctionnés** : Afin de renforcer son effet, la nLPD contient plusieurs dispositions pénales visant à sanctionner les manquements aux devoirs. Les peines encourues peuvent aller jusqu'à CHF 250'000.
- Une **annonce** rapide est requise en cas de violation de la sécurité des données.

Les principales **notions** de la nLPD sont brièvement décrites ci-dessous :

- **Définition des « données personnelles » ;** toutes les informations concernant une personne physique identifiée ou identifiable (les personnes morales ne sont pas protégées par la nLPD). Cela inclut donc par exemple les adresses e-mail (cf. art. 5 let. a. nLPD) ;
- **Définition de « traitement » (de données personnelles) ;** toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données (cf. art. 5 let. d. nLPD) ;
- **Définition « responsable du traitement » ;** la personne privée (p. ex. un exploitant d'aérodrome) qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles (cf. art. 5 let. j. nLPD) ;
- **Définition du « sous-traitant » ;** personne privée (p. ex. un fournisseur de logiciels) qui traite des données personnelles pour le compte du responsable du traitement, p. ex. au moyen d'un logiciel en nuage (cf. art. 5, let. k, nLPD) ;

**CHECKLIST** : Quels sont les points auxquels un propriétaire/exploitant d'aérodrome doit prêter attention en vue de l'introduction de la nLPD et **quelles démarches doivent éventuellement encore être effectuées** ?

☑ **Mesures techniques et organisationnelles, dites « MTO »** (cf. art. 8 nLPD et art. 3 nOPDo) : le propriétaire/l'exploitant d'aérodrome responsable et son sous-traitant doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Les MTO devraient par exemple contenir des indications sur le contrôle de l'accès aux données/aux locaux et aux installations/contrôle d'utilisation, des indications concernant les technologies de cryptage utilisées ainsi que sur la minimisation des données (seules les données personnelles absolument nécessaires devraient être collectées et enregistrées), des contrôles de sécurité réguliers, des mises à jour, de la formation des collaborateurs de l'aérodrome, un plan d'intervention en cas d'incident (procédure en cas d'incident de protection des données), des déclarations sur la gestion des contrats existants conformément à la nLPD resp. sur les accords avec les prestataires de services (p. ex. fournisseurs de logiciels).

☑ Contrat de sous-traitance des données dit « CSTD » (cf. art. 9 nLPD) : il y a sous-traitance de données personnelles lorsque l'entreprise confie le traitement de données personnelles à des prestataires de services externes tels que des hébergeurs web, à des sociétés fiduciaires ou au support informatique**.** Un CSTD de l'aérodrome avec le prestataire de services externe doit donc être disponible sous forme de texte (également possible par voie électronique) et répondre aux exigences légales. Contrairement au règlement général européen sur la protection des données (RGPD), la nLPD ne prescrit pas de contenu minimal pour ce contrat. Il est possible d'intégrer une telle réglementation en tant que partie intégrante d'une relation contractuelle existante ou dans des conditions générales de vente CGV. En vue de l'entrée en vigueur de la nLPD, il est nécessaire de vérifier la conformité du nouvel ou existant CSTD avec la nLPD. **Remarque :** en cas de violation intentionnelle des conditions de la nLPD, l'exploitant d'aérodrome responsable risque désormais une amende pouvant aller jusqu'à CHF 250'000. Les responsables d'aérodrome ont donc tout intérêt à obliger le sous-traitant à respecter les dispositions de la nLPD**.**

☑ **Devoir d'informer et déclaration de confidentialité actualisée** (cf. art. 19 nLPD) : la nLPD élargit le devoir d'informer : L'exploitant d'aérodrome responsable informe la personne concernée de manière adéquate de la collecte de données personnelles, que celle-ci soit effectuée auprès d'elle ou non. **Allègement :** l'obligation d'informer selon l'art. 19 n'est pas nécessaire si les personnes concernées (p. ex. les membres d'une association ou d'un club) disposent déjà des informations correspondantes. L'obligation d'informer signifie toutefois que les personnes concernées, par exemple les visiteurs du site web d'un aérodrome, ont désormais un droit étendu à savoir à quelles fins leurs données sont traitées et quelles parties tierces reçoivent les données. Cela devrait se faire au moyen d'une déclaration de confidentialité mise à jour et conforme à la nLPD : Concrètement, cela signifie que les visiteurs du site web doivent être informés d'une part sur les données personnelles collectées, sur la manière dont elles sont traitées, sur leur finalité et sur le lieu où elles sont transmises. Il s'agit par exemple d'informations sur l'utilisation de cookies, de fichiers journaux des serveurs, des balises web, mais aussi sur l'utilisation de formulaires de contact, de newsletters et de services de Google et d'autres tiers, tels qu'ils sont couramment utilisés sur les sites web.

☑ **Mesures en cas de communication de données à l'étranger** (cf. art. 16 et 17 nLPD et art. 8 nOPDo) : si des données sont transférées à l'étranger (p. ex. par un hébergement de données sur un serveur étranger ou par l'utilisation d'un service en nuage), la nLPD prévoit des obligations particulières afin que les droits de la personnalité soient également protégés de manière adéquate dans les systèmes juridiques étrangers : Le transfert de données entre des Etats offrant un niveau de protection adéquat est possible (**comparer avec l'annexe 1 de la nOPDo**). Si le niveau adéquat n'est pas atteint, comme par exemple dans le cas d'un transfert de données vers les États-Unis, le transfert ne peut avoir lieu que si d'autres mesures offrent une sécurité adéquate. On peut citer par exemple un traité international, des clauses type de protection des données reconnues par le PFPDT (préalablement approuvées par le PFPDT) ou des règles de protection des données internes à l'entreprise (préalablement reconnues par le PFPDT et contraignantes).

---