Association des boursiers de La Côte

16 mars 2023 - Gilly

1

Yves Guichoud

- Formateur indépendant
  - Cybercriminalité
  - Sécurité informatique
  - Gestion de projet
  - Outils informatiques

GYConsulting.ch
yves.guichoud@gyconsulting.ch

Partner CYBER SAFE

2

Ordre du jour

- nLPD, nouvelle loi fédérale sur la protection des données
- LPrD, Loi cantonale vaudoise sur la protection des données
- Secret de fonction
- Charte informatique
- Sensibilisation et formation des collaborateurs

3

nLPD
Loi fédérale sur la protection des données

4

Entrée en vigueur

- Entrée en vigueur et pleine applicabilité le :

1er septembre 2023

Aucune disposition transitoire

5

Définition

- Données personnelles :
  - Toutes les informations concernant une personne physique identifiée ou identifiable ;
- Données personnelles sensibles (données sensibles) :
  - les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
  - les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
  - les données génétiques,
  - les données biométriques identifiant une personne physique de manière univoque,
  - les données sur des poursuites ou sanctions pénales et administratives,
  - les données sur des mesures d'aide sociale ;

6

- **Traitement :**
  - toute opération relevant de la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données ;
- **Communication :**
  - le fait de transmettre des données personnelles ou de les rendre accessibles ;
- **Responsable du traitement :**
  - personne privée ou organe fédéral qui détermine les finalités et les moyens du traitement de données personnelles ;

7

- **Profilage :**
  - toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique,
    - Par exemple : pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

8

Principaux changements

- Seules les données des personnes physiques sont dorénavant couvertes, et non plus celles des personnes morales.
- Les données génétiques et biométriques entrent dans la définition des données sensibles.
- Les principes de "Privacy by Design" et de "Privacy by Default" sont introduits.
  - le principe de "Privacy by Design" (protection des données dès la conception) implique d'intégrer la protection et le respect de la vie privé des utilisateurs dans la structure même du produit ou du service.
  - Le principe de "Privacy by Default" (protection des données par défaut) assure le niveau de sécurité le plus élevé dès la mise en circulation du produit ou du service, en activant sans intervention des utilisateurs, toutes les mesures nécessaires à la protection des données.

9

- Des analyses d'impacts doivent être menées, en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.
- 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.
- La tenue d'un registre des activités de traitement devient obligatoire :
  - Une exemption pour les PME dont le traitement des données présente un risque limité d'atteinte à la personnalité.

10

- Une annonce rapide est requise en cas de violation de la sécurité des données, à adresser au Préposé fédéral à la protection des données et à la transparence (PFPDT).
- La notion de profilage (soit le traitement automatisé de données personnelles) fait son entrée dans la loi.

11

Sanctions

- La nouvelle LPD prévoit des amendes de 250'000 francs au plus à l'encontre de personnes privées.
  - Seul les comportements et les omissions intentionnels seront punis, et non la négligence.
  - Le non-respect du devoir d'informer, de renseigner et d'annoncer et la violation des devoirs de diligence et celle du devoir de discrétion seront punis sur plainte seulement.
  - L'insoumission à une décision du PFPDT sera poursuivie d'office.
- C'est en principe la personne physique responsable qui sera punie.
  - L'entreprise elle-même pourra toutefois nouvellement l'être aussi, à hauteur de 50'000 francs maximum, si l'identification de la personne punissable au sein de l'entreprise ou de l'organisation nécessite des actes d'enquête disproportionnés.
  - Le nouveau droit n'accorde toujours pas de pouvoir de sanction au PFPDT

12

Pour être en conformité avec la nLPD, ce qu'il vous reste à faire :

- Recenser les données personnelles et évaluer les risques afin de déterminer les exigences de mise en conformité ;
- Ajouter, mettre à jour les différentes déclarations sur la protection des données sur votre site web, vos contenus publicitaires et marketing, vos contrats, etc. ;
- Mettre en place des procédures internes pour être en mesure de répondre rapidement aux demandes des prospects et clients en lien avec leurs données ;

13

- Etablir un registre de traitement des données ;
- Mettre en place un processus pour les analyses d'impact ;
- Examiner les contrats actuels (sous-traitants) pour veiller à ce que la sécurité des données soit assurée ;
- Nommer un conseiller à la protection des données personnelles (DPO) en interne ou bien faire appelle à une entreprise externe spécialisée.

14

LPrD
Loi sur la protection des données personnelles

15

Entrée en vigueur

- Aucune date n'a été définie pour l'entrée en vigueur de la nouvelle loi cantonale vaudoise sur la protection des données personnelles.

- En discussion :
  - La responsabilité des personnes privées

16

Règles

Au sein des communes le traitement des données doit respecter les principes suivants

- Légalité :
  - Les données personnelles ne peuvent être traitées que si :
    - une base légale l'autorise
    - leur traitement sert à l'accomplissement d'une tâche publique.
  - Les données sensibles ne peuvent être traitées que si :
    - une loi au sens formel le prévoit expressément,
    - l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument,
    - la personne concernée y a consenti ou a rendu ses données accessibles à tout un chacun.

17

- Finalité :
  - Les données ne doivent être traitées que dans le but indiqué lors de leur collecte, tel qu'il ressort de la loi ou de l'accomplissement de la tâche publique concernée.
- Proportionnalité :
  - Le traitement des données personnelles doit être conforme au principe de la proportionnalité.
- Transparence :
  - La collecte des données personnelles doit être reconnaissable pour la personne concernée.

18

- Exactitude :
  - Les entités soumises à la présente loi s'assurent que les données personnelles traitées sont exactes.
- Sécurité :
  - Le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, notamment contre leur perte, leur destruction, ainsi que tout traitement illicite.

19

Le registre des fichiers

- Le registre des fichiers permet aux citoyens et aux personnes morales de faire valoir leurs droits en matière de protection des données personnelles, en mettant à leur disposition des fiches signalétiques des fichiers qui sont détenus par les entités soumises à la loi.
- Chaque fiche comporte les rubriques suivantes :
  - le descriptif du fichier (nom, nature, base légale, but, personnes concernées, provenance des données, durée de conservation, etc.)
  - le responsable du fichier (entité qui détermine le contenu ainsi que les finalités du fichier)
  - les coordonnées de contact pour l'exercice du droit d'accès (les contacts de l'entité à solliciter pour l'exercice du droit d'accès)
  - transmission à des tiers (s'il y a lieu)

20

Responsabilité

- il appartient au responsable de traitement de s'assurer de la conformité à la LPrD.
  - Par exemple : en lien avec le principe de sécurité, celui-ci implique que le responsable doit prendre toutes les mesures appropriées (techniques, physiques et organisationnelles) pour garantir la sécurité des fichiers et des données personnelles
  - Si tel n'est pas le cas, un traitement illicite pourrait être constaté.

21

Surveillance

- L'autorité de protection des données et de droit à l'information peut :
  - Ouvrir une procédure formelle de surveillance à l'encontre du responsable du traitement
  - Emettre des recommandations (publiques et non contraignantes)
    - Permet l'ouverture de la voie du Tribunal cantonal

22

Sanctions

- Si un collaborateur ne respecte pas la loi, il appartient au responsable du traitement de prendre les mesures qui s'imposent, d'un point de vue RH de la part de leur autorité d'engagement.
  - Par exemple : l'utilisation des données à des fins privées.
- Les conséquences, peuvent être de plusieurs ordres :
  - Administratives
  - Civiles
  - Pénales

23

Secret de fonction qualifié

24

Registre cantonal des contribuables

- Les personnes habilitées à disposer d'accès aux applications fiscales, sont les personnes chargées de l'application de la législation fiscale.
- A savoir le boursier communal ainsi que le municipal en charge des finances.

25

- Les personnes chargées de l'application de la législation fiscale ou qui y collaborent doivent garder le secret sur les faits dont elles ont connaissance dans l'exercice de leurs fonctions ainsi que sur les délibérations des autorités, et refuser aux tiers la consultation des dossiers fiscaux.
- Le secret fiscal couvre tous les renseignements personnels, professionnels et financiers que le contribuable a remis aux autorités fiscales.

26

- Le Chef de l'autorité administrative, ayant accès à la base de données, est responsable de communiquer tout changement intervenant dans le corps des utilisateurs et utilisatrices disposant d'un droit d'accès, et que l'utilisation des données doit se faire uniquement dans le cadre de l'accomplissement des tâches légales dévolues à l'entité concernée.
- L'obligation de tenir le secret fiscal est illimité dans le temps et perdure après la fin des rapports de travail.

27

- La Municipalité doit tout entreprendre pour qu'aucun renseignement couvert par le secret fiscal ne soit porté à la connaissance de tiers.
  - Les dossiers physiques doivent être conservés dans les locaux de l'administration, en sécurité et à l'abri des regards.
  - Les données numérisées doivent quant à elles être adéquatement stockées et protégées des cyberattaques.

28

Charte informatique

29

- Toute entité, doit définir une charte informatique où sont répertoriés les règles et comportements attendus de la part des collaborateurs avec les outils informatiques.
- Elle doit comporté au minimum :
  - Les règles d'utilisation de l'infrastructure informatique
  - La politique des mots de passe
  - Les règles et les comportements à respecter sur Internet, avec la messagerie électronique et la téléphonie
  - Les dispositions lors du départ d'un collaborateur
  - Etc.

30

Sensibilisation et formation des collaborateurs

31

Sensibilisation

- Dans le processus de sécurisation des données au sein d'une administration ou d'une entreprise, les collaborateurs doivent être sensibilisés aux règles mise en place et aux bonnes pratiques.
- La sensibilisation doit porté sur les sujets professionnels mais aussi sur les sujets privés
- Les bons réflexes doivent être pris autant au travail qu'à la maison.

32

Formation

- Les collaborateurs d'une administration ou d'une entreprise doivent se voir proposer des formations afin de s'adapter aux outils qu'ils leurs sont mis à disposition.
- Ces formations sont un excellent moyen de valoriser et motiver des équipes.

33

Questions ?

34

GYConsulting

Je vous remercie de votre attention

35