



DIE SPITÄLER DER SCHWEIZ  
LES HÔPITAUX DE SUISSE  
GLI OSPEDALI SVIZZERI

## Département fédéral de justice et police

Office fédéral de la justice  
Bundesrain 20  
CH-3003 Berne

Par courriel à: [jonas.amstutz@bj.admin.ch](mailto:jonas.amstutz@bj.admin.ch)

Lieu, date	Berne, le 14 octobre 2014	N° direct	031 335 11 59
Interlocutrice	Cheryl von Arx	Courriel	<a href="mailto:cheryl.vonarx@hplus.ch">cheryl.vonarx@hplus.ch</a>

### Révision de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) Réponse de H+ à la procédure de consultation

Madame la Conseillère fédérale,  
Madame, Monsieur,

Lors de sa séance du 23 juin 2021, le Conseil fédéral a ouvert la procédure de consultation sur la révision totale de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Notre association, H+ Les Hôpitaux de Suisse, vous remercie de nous donner la possibilité de s'exprimer. Par la présente, nous vous soumettons notre prise de position.

H+ Les Hôpitaux de Suisse est l'association nationale des hôpitaux, cliniques et institutions de soins publics et privés. Elle regroupe, en tant que membres actifs, 208 hôpitaux, cliniques et établissements médico-sociaux répartis sur 343 sites et quelque 150 membres partenaires, autorités, institutions, firmes et particuliers. Elle représente environ 200'000 collaborateurs.

#### Sommaire de la prise de position

Modifications et projets de loi	Position de H+	Page
1. Introduction	H+ rejette le présent projet mis en consultation.	2
2. Sécurité des données	H+ rejette les dispositions de ce chapitre, dans la mesure où elles ne reposent pas sur une base légale, resp. elles sont contraires à la volonté du législateur.	4
3. Obligations du responsable du traitement ou du sous-traitant	Les dispositions commentées contredisent la loi. En outre, les réglementations ne sont pas applicables dans la pratique. H+ les rejette pour ces motifs.	5

## 1. Introduction

Lors de la session d'automne 2020, le Parlement a adopté la nouvelle loi sur la protection des données (nLPD). Le délai référendaire est échu en janvier 2021 sans qu'une demande n'ait été déposée. La loi peut ainsi entrer en vigueur et les dispositions d'application doivent être adaptées dans l'ordonnance relative à la loi fédérale sur la protection des données (OLPD).

Le projet de nouvelle ordonnance se fonde sur de nombreuses normes de délégation de la nLPD et concrétise des dispositions de cette loi. À l'instar de cette dernière, il poursuit les objectifs suivants: amélioration de la transparence lors de la collecte et du traitement des données, renforcement de l'autodétermination des individus sur leurs données. Dans le même temps, la révision totale de la législation sur la protection des données en Suisse permet de ratifier la nouvelle version de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe (Convention 108) ainsi que la Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins pénales, qui s'inscrit dans le cadre de l'accord de Schengen. Les modifications prévues des dispositions d'application concernent les exigences minimales en matière de sécurité des données, les modalités du devoir d'informer et des droits d'accès ainsi que l'annonce des violations de la sécurité des données.

De manière générale, H+ approuve les nouvelles dispositions qui adaptent le droit de la protection des données à l'évolution des conditions technologiques et sociales et qui garantissent la compatibilité avec le droit européen. H+ constate cependant que le projet d'OLPD comprend de nombreuses normes dépourvues de base légale ou contraires à la volonté du législateur.

*«La compétence d'édicter des ordonnances au nom de la loi implique l'existence d'une norme de délégation dans cette même loi (art. 164 al. 2 Cst). Même lorsque le législateur a omis de confier à l'exécutif de telles fonctions législatives (limitées), il appartient au Conseil fédéral de mettre en œuvre la législation (art. 182 al. 2 Cst). Le domaine des ordonnances d'application se limite donc à préciser les dispositions de la loi fédérale concernée et de contribuer ainsi à une exécution plus aisée. Il se fonde sur le sens et le but de la loi, qu'exprime fondamentalement la disposition formelle de la loi.» (ATF 141 II 169, c. 3.3).*

L'administration excède sa compétence législative lorsque, par voie d'ordonnance, elle tente d'étendre l'ensemble de la gouvernance en matière de protection des données largement au-delà de la LPD au titre de la sécurité des données. Ainsi, le projet d'OLPD est souvent inutilement restrictif. Il conduirait à un supplément massif de travail pour les hôpitaux et, par exemple, alourdirait encore inutilement l'obligation, déjà inscrite dans la loi, de sécurité, d'amélioration et de développement des traitements médicaux<sup>1</sup>. H+ n'admet pas un tel procédé. C'est témoigner d'un respect limité du processus politique que d'introduire par le biais d'une ordonnance dépendante des règles qui devraient être prévues au niveau de la loi.

En outre, des articles de l'OLPD actuelle ont été repris ou sont inspirés directement du Règlement général de l'UE sur la protection des données (RGPD).

Finalement, le projet d'OLPD ne parvient pas à concrétiser les exigences minimales sous une forme correspondant à la terminologie et aux défis actuels de la sécurité des données. L'activité bureaucratique liée à la mise en œuvre de ce texte ne correspond pas au principe de la proportionnalité. Il en résulte pour les responsables du traitement un degré de détail qui ne prend pas du tout en compte la réalité des hôpitaux.

---

<sup>1</sup> Informations supplémentaires sous: [Le développement de la qualité requiert un cadre légal approprié et des prescriptions fédérales uniformes](#)

H+ s'engage en faveur d'un cadre légal propre à favoriser des traitements médicaux de haute qualité et un système hospitalier efficient. Les aspects relevant du droit de la protection des données jouent un rôle important à cet égard. **Dans le cas présent, les prescriptions vont largement au-delà de ce qui est souhaité et indiqué. Elles entraînent ainsi une charge administrative inutile qui aura une influence importante sur les tâches quotidiennes des hôpitaux. Une fois de plus, les fondamentaux politiques de la démocratie sont ignorés. H+ rejette le présent projet d'ordonnance pour ces motifs.** Cela vaut en particulier pour les dispositions suivantes qui ne règlent pas des détails mais revêtent une importance équivalente à celles de la nLPD:

- Règlement de traitement des personnes privées (art. 4 P-OLPD)
- Informations lors de la communication des données personnelles (art. 15 et 16 P-OLPD)
- Obligations de documentation (p. ex. art. 19 al. 5 et art. 20 al. 5 P-OLPD)

## 2. Sécurité des données

### 2.1. Dispositions générales

Par les dispositions relatives à la sécurité des données, le Conseil fédéral remplit le mandat consistant à préciser les exigences minimales en matière de sécurité au niveau de l'ordonnance (art. 8 al. 3 nLPD). La norme pénale (art. 61 let. c nLPD) se rapporte en outre à ces exigences minimales. Le degré de sécurité qui doit être respecté afin de ne pas violer la norme pénale est déterminé selon les principes et les critères de ce premier chapitre. Le projet d'ordonnance renonce à un régime rigide d'exigences minimales car on ne peut pas fixer des exigences générales valables pour toutes les branches. La P-OLPD adopte – conformément à la loi – une approche fondée sur les risques: plus la mise en danger des droits de la personnalité et des droits fondamentaux est élevée, plus les exigences sont grandes.

**H+ rejette les dispositions de ce chapitre, dans la mesure où elles ne reposent pas sur une base légale, respectivement elles contredisent la volonté du législateur.** Elles sont trop détaillées et ne prennent pas en compte la diversité des activités de traitement et des situations. Les réglementations obéissant au principe de l'arrosage ne contribuent pas à la sécurité du droit mais aboutissent plutôt à l'opposé. Pour H+, il est incompréhensible qu'il soit largement admis que des contrôles plus serrés, et donc une augmentation massive du travail administratif, entraînent automatiquement une meilleure application de la protection des données. Dans l'idée que «l'arbre cache la forêt», H+ estime que les présentes dispositions manquent l'objectif consistant à améliorer la sécurité des données et que l'impact négatif, encore impossible à évaluer aujourd'hui, l'emportera.

### 2.2. Partie spéciale

#### Art. 3 al. 1: Journalisation

Commentaire: Selon la lettre de l'art. 3 al. 1 P-OLPD, les entreprises doivent établir un protocole des opérations de traitement des données lorsque l'analyse d'impact révèle qu'en dépit des mesures prises, un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées subsiste. Selon le rapport explicatif, l'objectif de cette «journalisation» est de pouvoir vérifier après coup le traitement des données, afin de déterminer si des données ont été perdues, effacées, détruites, modifiées ou si elles ont été divulguées. Il s'agit également de garantir la conformité au but. La journalisation peut ainsi fournir des renseignements permettant de savoir si les données personnelles ont été traitées conformément aux finalités. Elle sert en outre à déceler et à faire la lumière sur les violations de la sécurité des données. Elle n'est en revanche pas destinée à surveiller les utilisateurs qui traitent les données personnelles.

Du point de vue des hôpitaux, cette disposition est préoccupante à plusieurs égards:

- Si cette disposition devait être appliquée telle quelle, elle nécessiterait un immense appareil de contrôle qui mobiliserait de vastes ressources (en argent et en personnel).
- La disposition ne prévoit pas au premier chef une journalisation afin de garantir la sécurité des données mais bien davantage pour constater a posteriori le traitement conforme des données. Elle va à l'encontre de la loi parce qu'elle ne se prête pas à la détection d'une violation de la sécurité des données<sup>2</sup> et ne respecte donc pas le principe de la proportionnalité.
- En règle générale, une analyse d'impact relative à la protection des données personnelles ne révélera pas un risque élevé en matière de sécurité des données mais plutôt dans la

<sup>2</sup> L'art. 8 nLSP, qui constitue la base légale de cette disposition, ne traite que de la sécurité des données au sens propre. Selon l'al. 3, le Conseil fédéral devrait édicter uniquement des prescriptions sur les exigences minimales en la matière. Seule la violation de celles-ci peut aboutir à une sanction pénale.

manière de traiter les données. Cela n'a rien à voir avec la sécurité des données. Par conséquent, le résultat d'une telle analyse n'est pas un indicateur approprié pour constater le risque de violation de la sécurité des données.

**Une obligation ponctuelle de journalisation peut être tout à fait pertinente (p. ex. afin d'évaluer des logs à des fins d'analyse); cependant, H+ rejette une telle norme générale car elle est totalement disproportionnée. Les explications du rapport (cf. aussi art. 3 al. 3) confirment d'ailleurs qu'il s'agit (aussi) de garantir un traitement conforme. Cette intention contredit clairement le mandat du législateur.**

#### Art. 4: Règlement de traitement des personnes privées

Commentaire: L'art. 4 P-OLPD introduit une obligation d'établir un règlement de traitement. Selon l'approche fondée sur le risque, il faut toujours établir un tel règlement lorsque le risque est élevé. Ainsi, les responsables du traitement privés doivent établir un règlement pour les traitements automatisés, notamment lorsqu'ils traitent des données sensibles à grande échelle (let. a).

D'un point de vue systématique, cette obligation est régie dans la sécurité des données, mais un règlement des données n'est manifestement pas une mesure visant la sécurité. Il vise au contraire à garantir le respect des principes de traitement et ainsi la protection des données. Cette disposition est donc également dépourvue de base légale (voir plus haut). Le travail important nécessaire pour la gestion d'un tel règlement des données est disproportionné (extension massive des obligations de documentation qui vont largement au-delà de ce qui est indiqué).

En outre, les points suivants prêtent le flanc à la critique:

- Les indications essentielles sont déjà documentées dans le cadre de l'analyse d'impact relative à la protection des données qui est nécessaire dans de tels cas et le reste dans l'inventaire qui doit être dressé de toute façon.
- Le RGPD ne prévoit pas non plus une telle règle (qui relève du «perfectionnisme helvétique»).
- Des traitements des données particulièrement sensibles peuvent sans aucun doute nécessiter un règlement interne à l'entreprise. Cet aspect est suffisamment régi par l'art. 7 nLPD.

**Cette disposition est donc inutilement restrictive et doit être supprimée selon H+.**

### 3. Obligations du responsable du traitement et du sous-traitant

#### 3.1. Partie générale

Les devoirs d'information et d'annonce sont concrétisés au chapitre 2. L'art. 13 al. P-OLPD implique un devoir d'information du sous-traitant, ce qui ressort aussi explicitement du rapport explicatif (p. 29). La loi révisée ne prévoit pourtant pas une telle obligation: selon l'art. 19 nLPD, ce devoir n'incombe – à juste titre – qu'au responsable du traitement. Une obligation à l'égard du sous-traitant ne peut donc pas être imposée par l'ordonnance. Cette remarque vaut pour tous les articles du 2<sup>ème</sup> chapitre dans la mesure où ils régissent les devoirs d'informer.

## 3.2. Partie spéciale

Art. 15 et 16: Informations lors de la communication des données personnelles ainsi que de la rectification, de l'effacement, de la destruction et de la limitation du traitement

Commentaire: Outre «l'actualité» et la «fiabilité» des données personnelles, l'*art. 15* mentionne désormais également «l'exhaustivité» dans le cadre de la communication des données personnelles. En d'autres termes, les données qui sont communiquées ne doivent pas être lacunaires. Avec cette prescription, le serpent se mord la queue: le destinataire lui-même est tenu de respecter les règles de traitement et de prendre des mesures adaptées ainsi que de s'assurer de l'exactitude des données. Une information appropriée de la part de la personne qui transmet l'information y porte contournée ou fait de l'une des mesures de vérification possibles la seule norme valable. Ce dispositif est en contradiction avec la loi. En outre, la réglementation n'est pas applicable en pratique; si les informations sont lacunaires, le sous-traitant ne devrait pas les délivrer, respectivement il devrait annoncer quelque chose dont il ne dispose pas.

Le devoir du responsable du traitement d'informer le destinataire sur toutes les modifications des données personnelles (rectification, effacement, destruction), tel que prévu à l'*art. 16* P-OLPD, est contraire à la volonté du législateur. Cette disposition figurait déjà dans le projet de révision de la LPD et a été supprimée par le Parlement. Elle ne peut donc pas être réintroduite par voie d'ordonnance.

Si cette règle devait être appliquée comme prévu, elle entraînerait un travail énorme, pratiquement insurmontable, pour les hôpitaux.

**Ces deux normes doivent être supprimées selon H+, car elles représentent un immense travail et ne sont pratiquement pas applicables.**

Art. 19 al. 5

Commentaire: Le message sur la révision de la LPD constatait déjà qu'aucun devoir général de documenter ne devait être prévu (p. 6601). Et voilà que celui-ci est réintroduit par la petite porte au moyen de l'ordonnance. Cela contreviendrait aux principes généraux en matière législative.

De plus, l'utilité du devoir de documenter et d'informer demeure obscure dans la mesure où il découle de la systématique que seules des violations du devoir d'informer doivent être documentées. Si une violation est annoncée et qu'elle présente un intérêt pour le Préposé fédéral à la protection des données et à la transparence (PFPDT), celui-ci va enquêter sur le cas mais ne reviendra guère dessus. Cela ne présente donc aucune utilité pour le PFPDT.

***Il en va de même, par ailleurs, à l'art. 20 al. 5 concernant la documentation des motifs où la communication est refusée, restreinte ou différée après une demande de renseignement. Cette norme n'est guère appropriée. La personne concernée reçoit une réponse à sa demande. Si elle ne s'en contente pas, elle peut saisir la voie judiciaire. Cette disposition ne fait qu'entraîner un travail supplémentaire (temps de conservation plus long, resp. fréquence des réponses plus élevée que nécessaire).***

**Les deux dispositions n'apportent aucune plus-value, elles sont particulièrement gourmandes en ressources au niveau opérationnel et ne reposent pas sur une base légale. Il convient donc d'y renoncer.**

## 4. Autre

Pour le reste, nous nous rallions à la prise de position générale de la Verein für Unternehmens-Datenschutz (VUD).

\* \* \* \* \*

Nous vous remercions de prendre en compte nos demandes et nous tenons à votre disposition pour toute information complémentaire.

Nous vous prions d'agréer, Madame la Conseillère fédérale, Madame, Monsieur, l'expression de nos sentiments distingués.

A handwritten signature in black ink, appearing to read 'A. Bütikofer', with a stylized flourish at the end.

Anne Bütikofer  
Directrice