Swico
Josefstrasse 218
CH-8005 Zurich

Tél. +41 44 446 90 90
www.swico.ch
info@swico.ch

Département fédéral de
justice et police DFJP
Mme la Conseillère fédérale Simonetta Sommaruga
Bundesrain 20
3003 Berne

Par e-mail à: jonas.amstutz@bj.admin.ch

Zurich, le 3. April 2017

Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales

Madame la Conseillère fédérale, Mesdames, Messieurs,

Au nom de Swico, nous vous remercions de la possibilité qui nous est offerte de vous présenter notre point de vue sur l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales.

1. Légitimation et impact

Swico est l'organisation des entreprises du secteur informatique en Suisse. Swico défend les intérêts de 450 fournisseurs de prestations du secteur TIC, qui emploient à leur tour 56 000 collaborateurs, réalisant un chiffre d'affaires annuel de 40 milliards de CHF.

La protection des données joue un rôle véritablement central dans le secteur des TIC, dont Swico défend les intérêts. Les entreprises du secteur des TIC ont ainsi fortement besoin d'un règlement axé sur la pratique et favorable à l'économie et sont donc directement concernées par ce projet proposé à la consultation.

2. Consultation

2.1 Principes

Un alignement sur la situation juridique dans l'Union européenne n'est judicieux que dans la mesure où il est nécessaire à l'activité économique des entreprises de Suisse, à l'accès à l'espace européen et à l'échange sur ce territoire, ainsi qu'à un niveau de protection des données adéquat. La promotion de l'autorégulation est donc à encourager dans ce sens. Il convient cependant de refuser catégoriquement toute obligation nouvelle ou élargie par l'avant-projet, dépassant le cadre de la protection des données européenne harmonisée par le RGPD, dit le «Swiss Finish».

2.2 Prise de position sur certains articles

Pour la prise de position sur les articles de l'avant-projet devant, selon nous, être remaniés, nous renvoyons au formulaire officiel de prise de position joint en annexe, faisant partie intégrante de la présente prise de position.

3. Conclusion et demande

Nous demandons le renvoi de l'avant-projet pour réexamen au sens des considérations indiquées dans le formulaire de prise de position.

Les points suivants nécessitent une attention toute particulière:

- Notions
- Recommandations de bonnes pratiques
- Devoir d'informer lors de la collecte de données personnelles
- Analyse d'impact du traitement
- Obligation de déclarer les atteintes à la protection des données
- Profilage
- Préposé à la protection des données en entreprise
- Dispositions pénales

De nombreux points d'interrogation subsistent quant à la faisabilité de cet avant-projet dans le cadre de la structure économique suisse, notamment pour les PME, les microentreprises et les start-ups, dont l'importance est non négligeable dans notre branche. Celles-ci risquent d'être confrontées à d'importants coûts supplémentaires ainsi qu'à des contraintes administratives inutiles, telles que les obligations de déclaration et de notification aux autorités responsables de la protection des données, qui entraveraient fortement l'innovation.

Nous vous remercions de bien vouloir prendre nos suggestions en considération.

Cordialement,

Swico

Dr Peter K. Neuenschwander
Président de la commission Droit de l'informatique

Christa Hofmann
Head Legal & Public Affairs

Annexe: formulaire officiel de prise de position

Loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales (avant-projet)

Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive européenne (UE) n°2016/680, relative à la protection des données personnelles dans le domaine de la poursuite pénale et de l'entraide judiciaire en matière pénale

Projet de révision de la Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Observations générales

Nom/société	Remarque/suggestion
Swico	Légitimation et impact Swico est l'organisation des entreprises du secteur informatique en Suisse. Swico défend les intérêts de 450 fournisseurs de prestations du secteur TIC, qui emploient à leur tour 56 000 collaborateurs, réalisant un chiffre d'affaires annuel de 40 milliards de CHF. La protection des données joue un rôle véritablement central dans le secteur des TIC, dont Swico défend les intérêts. Les entreprises du secteur des TIC ont ainsi fortement besoin d'un règlement axé sur la pratique et favorable à l'économie et sont donc directement concernées par ce projet proposé à la consultation.
Swico	La loi fédérale sur la protection des données en vigueur a accompagné la numérisation de la Suisse et a pleinement rempli son but. Il convient maintenant de ne pas nuire à cette évolution positive par une réglementation suisse excessive. Principale demande: La **non-entrée en matière** sur l'«avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales» et le renvoi pour réexamen au sens des considérations indiquées, notamment sans la clause démesurée du «Swiss Finish». Un délai de consultation assorti d'une nouvelle possibilité de prise de position doit ensuite être prévu.

Loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales (avant-projet)					
Nom/société	**Loi**	**Art.**	**Al.**	**Let.**	**Remarque/suggestion**
Swico	LPD	3		a	Certains termes sont parfois imprécis et trop largement décrits. Ces termes doivent être précisés. Données personnelles: Les données personnelles sont toutes les informations concernant une personne identifiée ou identifiable. Il convient de définir plus précisément ce que l'on entend par «identifiable».
Swico	LPD	3		f	Profilage: selon l'AP, le profilage comprend toute exploitation de données (sans même se limiter à des données à caractère personnel), même le profilage «manuel». Demande: le terme «profilage» doit être limité à l'analyse automatique des données personnelles, comme dans le cas du RGPD et de l'E-STE 108.
Swico	LPD	4	6		Consentement express du profilage Un comportement tacite doit également être considéré comme un consentement valide pour que les conditions générales (CG) indispensables puissent toujours être utilisées dans le traitement de masse. Demande: L'exigence d'un consentement exprès pour le profilage doit être supprimée.
Swico	LPD	5			Constatation par le responsable du traitement – non par le Conseil fédéral La nouvelle constatation par le Conseil fédéral de la protection suffisante des données à l'étranger représente une restriction indue et inutile. Cette constatation ne doit pas être faite par le Conseil fédéral, mais par le responsable du traitement, en fonction de ses propres vérifications et connaissances.

Loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales (avant-projet)

Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'UE concernant la reprise de la directive européenne (UE) n°2016/680, relative à la protection des données personnelles dans le domaine de la poursuite pénale et de l'entraide judiciaire en matière pénale

Projet de révision de la Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Swico	LPD	5	3	d	Règles d'entreprise contraignantes Les règles d'entreprise contraignantes doivent être approuvées par le PFPDT. Cependant, ces règles représentent une sous-catégorie de garanties spécifiques, et seule une obligation d'informer est prévue pour les garanties. Ces clauses sont contradictoires. Une distinction doit être faite entre les contrats standard et les autres contrats/garanties; les obligations doivent faire l'objet d'ajustements correspondants.
Swico	LPD	5	5		Le délai de six mois accordé au PFPDT pour l'approbation des règles d'entreprise contraignantes est beaucoup trop long et irréaliste, et implique une incertitude juridique trop importante. Il faut revenir ici à la règle des 30 jours.
Swico	LPD	6	2		Cette obligation d'informer le PFPDT implique que les entreprises devraient également lui communiquer des secrets d'affaires sensibles, même dans les cas dans lesquels l'exportation de données est justifiée dans le cadre de la conclusion ou l'exécution du contrat, ou d'une procédure judiciaire étrangère. Par ailleurs, ces documents transmis au PFPDT peuvent être consultés publiquement, conformément à la loi fédérale sur le principe de la transparence dans l'administration. L'obligation de déclarer va également trop loin en ce sens qu'elle ne se limite pas au responsable du traitement, mais oblige également le sous-traitant à faire une déclaration. Demande: cette disposition, également absente du droit de l'Union européenne, doit être purement et simplement supprimée.
Swico	LPD	7	2		Le responsable du traitement doit désormais en particulier s'assurer que le sous-traitant est en mesure de garantir la sécurité des données personnelles et les droits de la personne concernée. Cette obligation de vérification entraîne un surcroît de travail administratif considérable en cas

					d'externalisation du traitement de données. Nous ne connaissons pas non plus les obligations assumées par le sous-traitant. Demande: Supprimer l'alinéa 2
Swico	LPD	7	3		Cette disposition relative à l'accord écrit préalable du responsable du traitement est déconnectée de la pratique et n'est pas non plus prévue par l'Union européenne. Il ne peut s'agir de la forme écrite au sens de l'art. 13 CO. L'accord donné de manière générale par écrit, par voie électronique ou similaire, de transmettre les données à un autre sous-traitant, et une information dans un cas concret suffisent.
Swico	LPD	8 et 9			Recommandations de bonnes pratiques Le problème réside dans le fait que des recommandations propres des parties intéressées ne peuvent être définies qu'avec l'autorisation du PFPDT. Le PFPDT est par ailleurs habilité à édicter lui-même des recommandations de sa propre initiative. On ne sait au juste si l'autorisation doit avoir la forme d'une disposition; aucun moyen juridique n'est par exemple prévu contre l'adoption ou le rejet de l'approbation du PFPDT. Le RGPD prévoit une élaboration de codes de conduite exclusivement par les associations et autres fédérations. Cela doit également être le cas ici; l'initiative doit donc obligatoirement venir des associations. Comme l'indique le terme, les «recommandations de bonnes pratiques» viennent de la pratique, c'est-à-dire d'un processus de bas en haut, ou «bottom-up».
Swico	LPD	13	4		Devoir d'informer lors de la collecte de données personnelles L'AP LPD dépasse le cadre du RGPD: l'art. 13 al. 4 AP LPD prévoit que lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement communique à la personne concernée son identité et ses coordonnées. Cette disposition doit être supprimée dans la version Swiss Finish.
Swico	LPD	13	5		Si les données personnelles ne sont pas collectées auprès de la personne concernée, la personne concernée doit être informée au plus tard lors de leur enregistrement. Cette disposition est insensée et déconnectée de la pratique. Dans la pratique, les données sont enregistrées au

					moment de leur collecte, et ne sont lues que par la suite. Demande: Disposition similaire à celle du RGPD: délai d'un mois maximum.
Swico	LPD	16			Analyse d'impact relative à la protection des données Sous-traitant: le sous-traitant doit s'acquitter des mêmes obligations que le responsable du traitement. Le sous-traitant n'est cependant généralement pas en mesure de respecter ces obligations de sa propre initiative ou de sa propre responsabilité. Le sous-traitant dépend pour cela du responsable du traitement. Demande: suppression du «sous-traitant» de cette disposition, qui n'est d'ailleurs pas prévu aux termes de l'art. 35 RGPD en ce sens.
Swico	LPD	16	1-3		Analyse d'impact relative à la protection des données L'art. 16 AP instaure une obligation de procéder à une analyse d'impact du traitement dès que «le traitement envisagé est susceptible d'engendrer un risque accru» pour la personnalité des personnes concernées. Cette définition extrêmement large entraînerait des vérifications complexes préalables à la plupart des traitements de données. Pour les entreprises, cela signifie que chaque projet contenant un traitement de données pouvant se révéler problématique requerrait un délai préalable de quelques mois, permettant de satisfaire aux exigences éventuelles du PFPDT en plus des vérifications propres. Cela représente une charge insensée pour les entreprises et entraînerait des coûts importants. Demande: la référence aux droits fondamentaux doit être supprimée. Dans le domaine privé, la LPD sert exclusivement à la protection de la personnalité des personnes concernées.

					Demande: si le traitement des données prévu est susceptible d'engendrer un risque élevé (~~accru~~) pour la personnalité de la personne concernée, le responsable du traitement doit au préalable procéder à une analyse d'impact du traitement.
Swico	LPD	16	4		Les résultats de l'analyse d'impact doivent être communiqués au PFPDT. Le PFPDT dispose de trois mois pour informer le responsable du traitement de toutes objections éventuelles concernant les mesures envisagées. Demande: suppression ou remplacement par un délai adéquat de 1 mois. Possibilité d'exception La possibilité de faire intervenir un préposé à la protection des données de l'entreprise doit être prévue comme option pour les entreprises, combinée à l'exemption des obligations de notification vis-à-vis du PFPDT (dans le cas de l'analyse d'impact du traitement, par exemple). Elle s'avère judicieuse comme moyen de décharger le PFPDT. Demande: dans ce contexte, le recours à un préposé à la protection des données en entreprise doit se faire sur une base volontaire, avec des facilitations correspondantes pour les entreprises dans le cadre de la LPD.
Swico	LPD	17	1		Notification des violations de la protection des données (Data Breach Notifications) Cette obligation de notification est beaucoup trop vaste et dépasse nettement le cadre de la disposition du RGPD. L'AP instaure l'obligation de notifier au PFPDT tout traitement des données qui enfreint la LPD, tel que toute utilisation détournée ou excessive des données. De ce fait, toute irrégularité mineure dans les processus quotidiens de traitement des données représenterait une violation de la protection des données, devant être notifiée. Cela entraînerait un flux de notifications au PFPDT irréalisable et serait insensé, disproportionné et compterait également nettement plus de cas d'application que ne le prévoit la législation en termes de notification à l'autorité de surveillance au sens du RGPD. Par ailleurs, le SCI interne aux entreprises est déjà en charge de ce type d'irrégularités mineures. L'obligation de notification au PFPDT doit donc être limitée aux atteintes à la protection des données susceptibles d'entraîner des conséquences

					graves. Demande: l'obligation de notification au PFPDT doit être limitée aux atteintes à la protection des données susceptibles d'entraîner des conséquences graves.
Swico	LPD	17	4		L'obligation de notification «sans délai» est inapplicable, car il convient d'abord de recueillir suffisamment d'informations. Tout agissement dans la précipitation risque par ailleurs d'entraîner une violation du secret commercial ou professionnel. Le RGPD prévoit un délai maximum de 72 heures. Demande: délai similaire à celui du RGPD.
Swico	LPD	19		b	Désormais, le responsable du traitement et le sous-traitant sont tenus d'informer les destinataires auxquels des données ont été communiquées de toute rectification, effacement, ou destruction des données personnelles, etc., à moins qu'une telle information s'avère impossible ou exige des efforts disproportionnés. L'AP dépasse nettement le cadre du RGPD. Il est difficile d'établir si seules les violations de la protection des données soumises à notification sont visées, ou si toutes les violations de la protection des données le sont (cf. libellé). Cette obligation d'informer le destinataire des données n'est ni utile, ni praticable. Dans ce cas, toute entreprise serait tenue de contrôler en continu à qui les données ont déjà été transmises lors du nettoyage de ses archives, voire lors de toute suppression de données. Demande: limiter la notification aux cas dans lesquels cette information successive est bel et bien justifiée.

Swico	LPD	23	2	d	Constitue notamment une atteinte à la personnalité le fait de faire du profilage sans le consentement exprès de la personne concernée. Contrairement au RGPD, le profilage manuel (traitement manuel) est également couvert (lorsqu'une personne remplit une évaluation des collaborateurs, par exemple). Cette disposition est excessive et va trop loin. Demande: l'exigence d'un consentement exprès lors du profilage doit être supprimée. Le profilage doit être limité à l'évaluation automatisée des données personnelles (voir remarques relatives à l'art. 3 ci-dessus).
Swico	LPD	50-55			Dispositions pénales Les dispositions pénales doivent être rejetées: l'incrimination personnelle expose trop fortement les collaborateurs d'une entreprise aux sanctions. Ce risque est renforcé par la possibilité de l'application d'une peine en cas de faute non intentionnelle. Etant donné qu'il s'agit de sanctions pénales, il faut s'attendre à ce que ceux-ci ne puissent pas être assurés et à ce que l'entreprise ne puisse pas payer pour la personne condamnée. Par ailleurs, les dispositions pénales prévues aux termes de l'art. 50 ss. AP LPD contredisent le principe élémentaire du droit pénal «nulla poena sine lege scripta stricta praevia» (une peine ou une mesure ne peuvent être prononcées qu'en raison d'un acte expressément réprimé par la loi.), conformément aux dispositions de l'art. 1 CP. Les règles de la protection des données, imposant aux services traitant les données d'évaluer de manière fiable les cas d'obligations liées à la protection des données, ne sont pas adaptées à la mise en place d'une norme pénale en raison du «principe de légalité» régissant toute poursuite pénale. Selon l'opinion que nous défendons, ceci s'applique aux directives de protection des données suivantes et aux peines encourues correspondantes: - Art. 5 al. 1 conjointement avec l'art. 51 al. 1 let. a AP LPD Evaluation du risque pour la personnalité des personnes concernées lors d'une communication à l'étranger - Art. 7 al. 1 et 2 conjointement avec l'art. 51 al. 1 let. b AP LPD: Devoir de diligence lors de la passation d'un mandat pour l'externalisation du traitement des données

					- Art. 11 conjointement avec l'art. 51 al. 1 let. c AP LPD: Omission des mesures techniques et organisationnelles adéquates relatives à la sécurité des données - Art. 13 et art. 14 al. 2 conjointement avec l'art. 50 al. 1 let. a et b AP LPD: Peine encourue malgré l'exemption possible de l'obligation d'informer - Art. 15 al. 1 AP LPD: Evaluation de l'impact d'une décision individuelle automatisée, conjointement à la peine encourue selon l'art. 50 al. 1 let. b AP LPD - Art. 16 al. 1 AP LPD: Evaluation de l'existence d'une obligation d'exécution d'une analyse d'impact, conjointement avec l'art. 50 al. 1 let. c et avec l'art. 51 al. 1 let. d AP LPD - Art. 17 al. 1 et al. 4 AP LPD: Evaluation des conditions de notification des violations de la protection des données au préposé, conjointement avec l'art. 50 al. 2 let. e et al. 3 let. b AP LPD - Art. 18 conjointement avec l'art. 51 al. 1 let. e AP LPD: Omission de l'application des mesures de protection des données par défaut - Art. 19 let. b AP LPD: Obligation d'informer les bénéficiaires des données de toute violation de la protection des données, conjointement avec l'art. 50 al. 3 let. a AP LPD Il reste par ailleurs insatisfaisant qu'une loi sur le traitement des données personnelles applicable tant aux responsables du traitement et des sous-traitants privés, qu'aux employés de la Confédération, ne menace de sanctions pénales que les acteurs du traitement des données relevant du droit privé. Nous renvoyons par ailleurs à ce sujet à la proposition largement soutenue des associations

					économiques: Principe: sanctions administratives à l'encontre des entreprises La LPD doit prévoir la sanction de l'entreprise en cas de violation des dispositions de protection des données. Lien: manque d'organisation dans l'entreprise. Dans ce cas, seule une poursuite pénale subsidiaire des collaborateurs dans le cadre des dispositions pénales déjà disponibles dans le PS CP devrait être envisagée. Les plaintes doivent généralement être déposées par les entreprises elles-mêmes. En fin de compte, une modification de l'objectif des sanctions au sens d'une amélioration de la protection des données dans l'entreprise faciliterait considérablement la situation des personnes traitant les données. La sanction des collaborateurs: elle ne devrait être prévue qu'en cas de délit intentionnel direct contre les intérêts de l'entreprise ou de la personne concernée. Les dispositions pénales déjà prévues aux termes du PS CP devraient généralement suffire pour sanctionner les personnes physiques (violation du secret commercial et soustraction non autorisée de données, par exemple). Le cercle des collaborateurs potentiellement pénalement responsables devrait être limité d'emblée (conformément à l'art. 29 CP).
Swico	LPD	59			Dispositions transitoires: Demande: à l'instar de la disposition du RGPD, un délai transitoire de deux ans doit être prévu.