Association suisse des institutions de prévoyance (ASIP)

Mise en œuvre de la nouvelle loi sur la protection des données (nLPD) – Questions posées lors du séminaire sur la protection des données le 20 mars 2023	
Questions	**Réponses**
PLATEFORME DE DÉCLARATION PFPDT	
Le contenu figurant sur la plateforme de déclaration au PFPDT peut-il être consulté à tout moment par le public?	Oui. Le PFPDT publie les déclarations des organes fédéraux, conformément à l'art. 56 nLPD, dans un registre accessible au public, le DataReg (obligation de déclarer uniquement pour les registres des organes fédéraux [art. 12 al. 4 nLPD]). *Voir https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/declaration-des-fichiers.html*
RÈGLEMENT D'ORGANISATION	
Les règlements d'organisation et de prévoyance devront-ils être formellement approuvés au 1er septembre 2023?	Le règlement d'organisation devra être formellement approuvé par l'organe suprême au 1er septembre 2023. Le règlement de prévoyance ne suffit pas à lui seul.
RÈGLEMENT DE TRAITEMENT	
Est-il possible de se doter de plusieurs règlements de traitement des données?	Oui: un règlement de traitement des organes fédéraux en cas de traitement automatisé, notamment de données personnelles particulièrement sensibles, ou en cas d'établissement automatisé d'un profilage (art. 6 nOPDo); un règlement de traitement des personnes physiques, c.-à-d. d'institutions de prévoyance non enregistrées, en cas de traitement automatisé de données personnelles particulièrement sensibles à grande échelle ou en cas d'établissement automatisé d'un profilage à risque élevé (art. 5 nOPDo).
CONSENTEMENT DE LA PERSONNE ASSURÉE OU DU / DE LA BÉNÉFICIAIRE DE RENTE	
Un consentement peut-il être acquis de manière générale par le biais du règlement de la CP?	En principe oui, lors de la remise du règlement de la CP. La clarification que proposait encore le Conseil fédéral, selon laquelle un consentement était absolument nécessaire, a été supprimée par le Parlement.

	Ainsi, dans la nouvelle loi sur la protection des données, «aucune autre norme ne s'applique au consentement […], comme c'était le cas auparavant et comme c'est par ailleurs le cas en droit suisse en ce qui concerne les déclarations de volonté.» Conformément à l'art. 6 al. 6 nLPD[1], aucun consentement n'est en principe requis; l'art. 6 al. 7 nLPD demande toutefois le consentement exprès pour: a) le traitement de données personnelles sensibles; b) un profilage à risque élevé effectué par une personne privée; ou c) un profilage établi par un organe fédéral (art. 6 al. 7 nLDP). Les données particulièrement sensibles au sens de la nLPD sont les suivantes: 1) données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; 2) données sur la santé, la sphère intime ou l'origine raciale ou ethnique; 3) données génétiques; 4) données biométriques identifiant une personne physique de manière univoque; 5) données sur des poursuites ou sanctions pénales et administratives; 6) données sur des mesures d'aide sociale (art. 5 let. c nLPD). La LPD précise dans quels cas un consentement est requis, resp. sert de motif justificatif dans les articles suivants: art. 17 al. 1 let. a nLPD (exportation de données); art. 21 al. 3 let. b nLPD (décision individuelle automatisée); art. 25 al. 3 nLPD (droit d'informer relatif aux données médicales); art. 31 al. 1 nLPD (motifs justificatifs); art. 34 al. 4 let. b nLPD (traitement sans base légale suffisante de la part des organes fédéraux); enfin, l'art. 36 al. 2 let. b nLPD (communication de données personnelles par l'organe fédéral). *Voir David Rosenthal, «Controller oder Processor: Die datenschutzrechtliche Gretchenfrage»,* Jusletter *du 17 juin 2019, ch. 30s. (version française 16 novembre 2020)*
FOURNISSEUR DE CLOUD: TRANSFERT DE DONNÉES À L'ÉTRANGER?	
Lorsque des données sont stockées dans le Cloud, on ne sait pas vraiment où elles sont conservées. S'agit-il d'un transfert de données à l'étranger?	Le fournisseur de Cloud (dans le cas d'un stockage de données sur le Cloud géré par le fournisseur d'informatique) est considéré comme un sous-traitant selon la nLPD, mais l'institution de prévoyance est toutefois la responsable. Elle doit régler par voie contractuelle l'ensemble des processus administratifs et informatiques (contrat de traitement de commande ou *Data Processing Agreement*). Toute la chaîne, de l'institution de prévoyance jusqu'aux fournisseurs de logiciels et de Cloud, doit être garantie par contrat.

[1] «Lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement que si elle exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée.»

	Par ailleurs, le sous-traitant ne peut transférer le traitement à un tiers qu'avec l'autorisation préalable de l'institution de prévoyance. Quiconque, par exemple, permet l'accès de données personnelles en provenance de la Suisse à sa propre filiale à l'étranger est tenu de respecter les règles contenues dans les art. 16s. nLPD et 8-12 nOPDo. Même chose, si une institution de prévoyance fait parvenir des données personnelles à son fournisseur de Cloud qui se trouve à l'étranger. L'institution de prévoyance doit, dans la déclaration de confidentialité, communiquer aux personnes concernées, c.-à-d. à la personne assurée et aux bénéficiaires de rente, le nom de l'État dans lequel le fournisseur de Cloud est domicilié (art. 19 al. 4 nLPD). *Voir David Rosenthal, «Controller oder Processor: Die datenschutzrechtliche Gretchenfrage»,* Jusletter *du 17 juin 2019, ch. 66 (version française 16 novembre 2020)*

PARTENAIRES EXTERNES	
Des partenaires externes peuvent-ils être en principe exemptés, en tant que sous-traitants, de la soumission à la nouvelle LPD, s'ils ne traitent que des données anonymes? (fournisseur d'informatique, experts, réviseurs, etc.)	Oui, mais les experts et les réviseurs – à la différence des fournisseurs d'informatique – sont considérés comme des responsables. Du point de vue du droit à la protection des données, une anonymisation des données personnelles a le même effet qu'une suppression de ces données; car si le droit à la protection des données ne s'applique pas aux données anonymes, leur suppression ne peut pas non plus être exigée. Ainsi, les données personnelles anonymisées, en tant que données anonymes, ne sont pas soumises au «droit à l'oubli».
SUPPRESSION OU ANONYMISATION DES DONNÉES – MISE EN ŒUVRE	
Comment la suppression de données des personnes assurées est-elle gérée? – p. ex. des informations sur le paiement d'une prestation de libre passage.	Si les personnes assurées ou les bénéficiaires de rente revendiquent le droit de «suppression» des données de prévoyance à l'égard de l'institution de prévoyance, au sens du «droit à l'oubli», celle-ci devra leur opposer les obligations légales de conservation des caisses de pension. Elles s'appliquent aussi bien aux institutions de prévoyance enregistrées qu'aux non-enregistrées. L'obligation de conserver les documents de prévoyance est régie par l'art. 27i–27k OPP2. La conservation des documents commerciaux s'oriente sur l'art. 47 al. 4 OPP2 ou l'art. 958f du droit des obligations (voir à ce sujet la circulaire de l'ASIP n° 130, p. 9s.; https://www.datatrust.ch/gesetzesgrundlagen/). Des données anonymisées sont des données ayant un lien avec une personne, mais pour lesquelles le rapport avec la personne a été sciemment supprimé (p. ex. anonymisation des données personnelles au moyen de leur agrégation). Le droit à la protection des données ne s'applique donc plus à ces données. Du point de vue du droit, le traitement de ces données n'est donc plus limité.

	Une anonymisation des données personnelles a, par conséquent, du point de vue du droit à la protection des données, le même effet qu'une suppression. Car, si le droit de protection des données ne s'applique pas aux données anonymes, leur effacement ne peut pas être exigé. Ainsi, les données personnelles anonymisées ne sont pas considérées comme des données anonymes soumises au «droit à l'oubli». Voir webinaire de l'ASIP sur la protection des données des 10/14/15 novembre 2022, diapos 23s.

ÉCHANGE DE DONNÉES AVEC LES PERSONNES ASSURÉES ET LES BÉNÉFICIAIRES DE RENTE	
Échange de données par courriel avec des personnes assurées, p. ex. des collaboratrices et collaborateurs sortis de l'institution de prévoyance: quelles sont les exigences relatives à l'envoi de certificats d'assurance personnels, etc.? Un envoi par courriel est-il autorisé, et si oui, d'autres exigences sont-elles requises?	Non. Avec la nLPD, pour la première fois en Suisse, une obligation de notifier une violation des données (*Data Breach Notification*) a été introduite: si un courriel a été envoyé à la mauvaise adresse ou si une perte de données ou un autre incident en matière de sécurité des données à caractère personnel se produit, selon les circonstances, cela devra désormais être annoncée au PFPDT. Une violation de la sécurité des données devra être signalée aussi vite que possible au Préposé, si cette violation est susceptible de présenter un risque élevé pour la personne concernée. Cette dernière devra également être informée, au cas où ce serait nécessaire pour sa protection ou si le PFPDT l'exige (art. 24 nLPD / art. 15 nOPDo). *Voir David Rosenthal, «Controller oder Processor: Die datenschutzrechtliche Gretchenfrage»,* Jusletter *du 17 juin 2019, ch. 160.*
CONSEILLER/CONSEILLÈRE À LA PROTECTION DES DONNÉES	
Est-ce que la nomination du conseiller / de la conseillère à la protection des données (art. 25 nOPDo) incombe impérativement à l'organe suprême, ou peut-elle être décidée par la Direction?	La nomination du conseiller / de la conseillère à la protection des données incombe à l'organe suprême de l'institution de prévoyance. En effet, premièrement, la protection des données (mise en œuvre de la nLPD) fait partie des tâches inaliénables et intransmissibles de l'organe suprême (art. 51a al. 1 en relation avec l'art. 49 al. 2 chif. 7 LPP); et, deuxièmement, cette exigence résulte également des tâches du conseiller ou de la conseillère à la protection des données (art. 10 al. 2 nLPD et art. 26 al. 2 nOPDo): a) former et conseiller l'organe suprême dans le domaine de la protection des données; b) concourir à l'application des prescriptions relatives à la protection des données (contrôler le traitement de données personnelles, proposer des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée); c) conseiller le responsable du traitement lors de l'établissement de l'analyse d'impact relative à la protection des données et vérifier son exécution; d) servir d'interlocuteur pour les personnes assurées et pour les autorités de protection des données. *Voir webinaire de l'ASIP sur la protection des données ASIP-des 10/14/15 novembre 2022, diapo 26.*