Umsetzung des revidierten Datenschutzgesetzes (DSG): Fragestellungen aus den Webinaren und Antworten **Mise en œuvre de la nouvelle loi sur la protection des données (LPD): questions du webinaire et réponses** ***Änderungen/Ergänzungen in kursiver Schrift***	
Fragen **Questions**	**Antworten** **Réponses**
VORSORGEEINRICHTUNGEN ALS BUNDESORGANE: WEITERE AUSWIRKUNGEN? **LES INSTITUTIONS DE PRÉVOYANCE EN TANT QU'ORGANES FÉDÉRAUX – AUTRES CONSÉQUENCES?**	
1. Wie ist vorzugehen, wenn im gleichen System sowohl eine umhüllende Kasse wie auch zwei überobligatorische Kassen des gleichen Arbeitgebers verwaltet werden und die Versicherten der einen überobligatorischen Kasse auch in der umhüllenden Kasse versichert sind? 1. Comment faire lorsque, dans un même système, une caisse de pension enveloppante et deux surobligatoires du même employeur doivent être gérées, et que les assurés de l'une des caisses su-	1. Lässt sich eine Datenbearbeitung nicht ausschliesslich dem Überobligatorium zuordnen, so muss sich eine umhüllende Pensionskasse an die für Bundesorgane geltenden Regeln des revDSG halten. Nur so weit eine Datenbearbeitung vollständig von der öffentlichen Aufgabe getrennt bzw. ausschliesslich dem Überobligatorium zuzuordnen ist, unterliegt die umhüllende Pensionskasse den für Private geltenden Bestimmungen des revDSG. *Siehe ASIP-Fachmitteilung Nr. 130, S. 3 (mit Beispielen).* Rein überobligatorische Kassen gelten gemäss revDSG jedoch als private Personen. Sie sind von der Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung befreit. *Siehe ASIP-Fachmitteilung Nr. 130, S. 8f.* 1. Si un traitement de données ne peut pas être exclusivement attribué à la part surobligatoire, une caisse de pension enveloppante doit respecter les dispositions de la nLPD valables pour les organes fédéraux. Si un traitement de données n'a rien à voir avec les tâches publiques de la Confédération, autrement dit qu'il relève uniquement du domaine surobligatoire, la caisse de pension enveloppante sera soumise aux dispositions de la nLPD en vigueur pour les particuliers. *Voir la circulaire de l'ASIP n° 130, p. 3 (avec exemples concrets).* Les caisses purement surobligatoires sont toutefois considérées, selon la nLPD, comme des personnes privées. Elles sont donc dispensées de l'obligation de procéder à une analyse d'impact relative à la protection des données. *Voir la circulaire de l'ASIP n° 130, p. 8s.*

robligatoires sont aussi assurés dans la caisse enveloppante?	
2. Gibt es allfällige Besonderheiten zu beachten, wenn man überobligatorische Kassen wie ein Bundesorgan behandeln will?	2. Nicht registrierten (überobligatorischen) Pensionskassen ist die Ernennung eines Datenschutzberaters freigestellt. *Siehe ASIP-Fachmitteilungen Nr. 130, S. 6, und Nr. 131, S. 1f.*
2. Faut-il tenir compte de certaines particularités si l'on veut traiter les caisses surobligatoires comme des organes fédéraux?	2. Les caisses de pension non enregistrées (régime surobligatoire) sont libres de nommer un conseiller à la protection des données. *Voir les circulaires de l'ASIP n° 130, p. 6, et n° 131, p. 1s.*
DATENAUSTAUSCH MIT VERSICHERTEN UND RENTNERINNEN UND RENTNERN ÉCHANGE DE DONNÉES AVEC LES PERSONNES ASSURÉES ET LES BÉNÉFICIAIRES DE RENTE	
Datenaustausch mit Versicherten z.B. ausgetretenen Mitarbeiterinnen und Mitarbeitern via Email: Was sind die Anforderungen bezüglich des Versands von persön-	Ja, unter der Voraussetzung, dass geeignete technische und organisatorische Massnahmen für die Gewährleistung einer angemessenen Datensicherheit vorgekehrt werden. Mit dem revidierten DSG wird in der Schweiz erstmals eine Pflicht zur einer sog. Data Breach Notification eingeführt: Wird eine Email falsch versandt oder kommt es anderweitig zu einem Datenverlust oder einem anderen Datensicherheitsvorfall, muss dies neu unter Umständen dem EDÖB gemeldet werden. Eine Verletzung der Datensicherheit ist dem EDÖB so rasch als möglich zu melden, falls die Verletzung voraussichtlich zu einem hohen Risiko für die betroffene Person führt. Die betroffene Person muss ebenfalls informiert werden, falls dies zu ihrem Schutz erforderlich ist oder der EDÖB dies verlangt (Art. 24 revDSG/Art. 15 revDSV). Auch ist bei einer Verletzung der Datensicherheit der Datenschutzberater zu informieren (Art. 27 Abs. 1 lit. b DSV).

lichen Versicherungsausweisen etc. Ist ein Email-Versand zulässig und, falls ja, welcher Anforderungen bedarf es?	*Siehe David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 160.*
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?	Oui, à condition que des mesures techniques et organisationnelles appropriées soient prises pour garantir une sécurité des données adéquate. La révision de la LPD introduit pour la première fois en Suisse l'obligation d'une notification de violation de données: Si un e-mail est envoyé de manière erronée ou si une perte de données ou un autre incident concernant la sécurité des données se produit, il faut désormais, dans certaines circonstances, le notifier au PFPDT. Une violation de la sécurité des données doit être annoncée au PFPDT dans les meilleurs délais si la violation est susceptible d'entraîner un risque élevé pour la personne concernée. La personne concernée doit également être informée si cela est nécessaire pour sa protection ou si le PFPDT l'exige (art. 24 nLPD/art. 15 nOPDo). De même, en cas de violation de la sécurité des données, le conseiller à la protection des données doit être informé (art. 27, al. 1, let. b, nOPDo). *Voir David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, ch. 160.*
DER VERANTWORTLICHE GEMÄSS REVDSG LE RESPONSABLE SELON LA NOUVELLE LPD	
Was ist unter dem «Verantwortlichen gemäss revDSG» zu verstehen?	Als Verantwortlicher gilt jene Person oder jenes Bundesorgan, welche bzw. welches allein oder zusammen mit anderen über den Zweck (Wieso findet eine Datenbearbeitung statt?) und die Mittel (Wie wird der Zweck erreicht?) der Datenbearbeitung entscheidet. Es handelt sich dabei um diejenige Person bzw. um dasjenige Bundesorgan, die/das die wesentlichen datenschutzrechtlichen Parameter einer Datenbearbeitung festlegt (ASIP-Fachmitteilung Nr. 130, S. 6, Anm. 31). Ein Beispiel ist die Gesundheitsprüfung. Sie bezweckt die Durchsetzung der Anzeigepflicht, d.h. der Deklaration einer gesundheitlichen Beeinträchtigung. Der Zweck wird mittels eines durch den Antragsteller (Versicherten) zuhanden des Ver-

	antwortlichen auszufüllenden Fragebogens oder durch sonstiges schriftliches Befragen des Antragstellers durch den Verantwortlichen erreicht (Mittel). *Dabei empfehlen wir die Anwendung von DSAT (ASIP-Fachmitteilung Nr. 131, S. 5): Formular «Compliance Check II – Anforderungen an eine Datenbearbeitung (für Verantwortliche)» unter https://dsat.ch/download/.*[1]
Qu'entend-on par «responsables» selon la nLPD?	Toute personne ou tout organe fédéral qui décide, p. ex., seul ou avec d'autres, du but (Pourquoi un traitement de données a-t-il lieu?) et des méthodes (Comment ce but sera-t-il atteint?) est considéré comme responsable. Il s'agit en l'occurrence de la personne ou de l'organe fédéral qui définit les paramètres déterminants en matière de protection des données dans le cadre de leur traitement (circulaire de l'ASIP n° 130, p. 6, note 31). L'examen médical en est un exemple. Il a pour but l'application de l'obligation de notifier, c'est-à-dire la déclaration d'une atteinte à la santé. L'objectif sera atteint au moyen d'un questionnaire qui sera remis au responsable par la personne en ayant fait la demande (l'assuré) ou en interrogeant par écrit la personne responsable (méthode). *Nous recommandons à cet égard l'application de DSAT (circulaire de l'ASIP n° 131, p. 5): formulaire «Compliance CheckII – exigences concernant un traitement de données (pour les responsables)», téléchargeable sous https://dsat.ch/download/.*[1y]
Welche Rechtsgrundlage erlaubt einer VE die Bearbeitung von Anlagedaten (Miete / Darlehen)?	Dies ist das revDSG. Dabei gilt die Vorsorgeeinrichtung – auch die registrierte als Vorsorgeeinrichtung (Bundesorgan) – für diese Anlagearten als private Person gemäss revDSG. Dies gilt auch für öffentlich-rechtliche Vorsorgeeinrichtungen, wobei die öffentlich-rechtlichen Vorsorgeeinrichtungen der Kantone stets private Personen (keine Bundesorgane!) sind, auch wenn sie das BVG (Obligatorium der beruflichen Vorsorge) durchführen.
Quelle est la base juridique permettant à une institution de pré-	C'est la nLPD. Dans ce contexte, l'institution de prévoyance - même celle qui est enregistrée en tant qu'institution de prévoyance (organe fédéral) - est considérée comme une personne privée pour ces types de placement selon la nLPD. Cela vaut également pour les institutions de prévoyance de droit public, les institutions de prévoyance de droit public des

[1] DSAT ist ein Datenschutz Self Assessment Tool, bestehend aus einem Satz von Formularen, der eine strukturierte Selbstbeurteilung der Datenschutz-Compliance eines Unternehmens erlaubt, d.h. die «Überprüfung, inwieweit die Bestimmungen des Datenschutzes sowohl unter dem revidierten DSG als auch der DSGVO eingehalten sind» (https://dsat.ch/einfuehrung/).

[1] Le DSAT est un instrument d'auto-évaluation de la protection des données composé d'un set de formulaires permettant une auto-évaluation structurée de la conformité d'une entreprise en matière de protection des données – autrement dit de «superviser» dans quelle mesure les dispositions de la nLPD ainsi que du Règlement européen sur la protections des données (RGPD) sont respectées» (https://dsat.ch/einfuehrung/).

voyance de traiter des données d'investissement (location / prêt)?	cantons étant toujours des personnes privées (pas des organes fédéraux!), même si elles appliquent la LPP (prévoyance professionnelle obligatoire).
EINWILLIGUNG DER VERSICHERTEN PERSON ODER DES RENTNERS/DER RENTNERIN CONSENTEMENT DE LA PERSONNE ASSURÉE OU DU / DE LA BÉNÉFICIAIRE DE RENTE	
Kann eine Einwilligung generell via PK-Reglement erfolgen?	Grundsätzlich ja, bei Abgabe des PK-Reglements. Die vom Bundesrat noch vorgeschlagene Klarstellung, wonach eine Einwilligung eindeutig erfolgen muss, wurde vom Parlament gestrichen. Somit gilt im neuen Datenschutzrecht «kein anderer Standard für Einwilligungen […], wie bisher und sonst im Schweizer Recht für Willenserklärungen.» Gemäss dem massgebenden Art. 6 Abs. 6 revDSG ist zwar grundsätzlich keine Einwilligung erforderlich, Art. 6 Abs. 7 revDSG fordert jedoch eine ausdrückliche Einwilligung für: a. die Bearbeitung von besonders schützenswerten Personendaten; b. ein Profiling mit hohem Risiko durch eine private Person; oder c. ein Profiling durch ein Bundesorgan (Art. 6 Abs. 7 revDSG). Besonders schützenswerte Daten i.S. des revDSG sind: 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren, 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe (Art. 5 lit. c revDSG). In welchen Fällen eine Einwilligung erforderlich ist bzw. als Rechtfertigungsgrund dient, legt das DSG in folgenden Artikeln fest: Art. 17 Abs. 1 lit. a revDSG (Datenexport), Art. 21 Abs. 3 lit. b revDSG (automatisierte Einzelfallentscheide), Art. 25 Abs. 3 revDSG (Auskunftsrecht betreffend Gesundheitsdaten), Art. 31 Abs. 1 revDSG (Rechtfertigungsgründe), Art. 34 Abs. 4 lit. b revDSG (Bearbeitung ohne hinreichende Rechtsgrundlage durch Bundesorgane) und Art. 36 Abs. 2 lit. b revDSG (Bekanntgabe von Personendaten durch Bundesorgane). *Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 30f.*
Un consentement peut-il être acquis de manière générale par le biais du règlement	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

de la CP?	volonté.» Conformément à l'art. 6 al. 6 nLPD1, 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)*
BEARBEITUNGSVERZEICHNISSE **REGISTRES DE TRAITEMENT**	
Sind die Bearbeitungsverzeichnisse, die beim EDÖB aufgeschaltet werden, öffentlich einsehbar? Les registres de traitement qui sont enregistrés auprès du PFPDT, sont-ils accessibles au public?	Ja. Die Meldepflicht beschränkt sich auf die Verzeichnisse von Bundesorganen (Art. 12 Abs. 4 revDSG): https://www.edoeb.admin.ch/edoeb/de/home/meldeportale/datareg.html. Oui. L'obligation de déclarer se limite aux registres des organes fédéraux (art. 12 al. 4 nLPD): https://www.edoeb.admin.ch/edoeb/fr/home/meldeportale/datareg.html.

Festhalten der Identität des für die Bearbeitung Verantwortlichen im Bearbeitungsverzeichnis – namentliche Nennung oder reicht Funktionsbezeichnung?	Das Verzeichnis des Verantwortlichen enthält u.a. mindestens die Identität des Verantwortlichen (Art. 12 Abs. 2 lit. a revDSG). Die für die Bearbeitung verantwortliche Person muss identifizierbar sein. Dabei genügt die Funktionsbezeichnung. *Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folien 17f. (Muster eines Bearbeitungsverzeichnisses).*
Saisie des données personnelles du responsable du traitement dans le registre des activités de traitement – faut-il mentionner son nom ou suffit-il d'indiquer sa fonction?	La personne responsable du traitement doit être identifiable. Le registre des activités de traitement contient entre autres au moins l'identité du responsable (art. 12 al. 2 let. a nLPD). La dénomination de sa fonction suffit à cet égard. *Voir webinaire sur la protection des données des 10/14/15 novembre 2022, diapositive 17s. (Modèle d'un registre de traitement).*
Benötigt es einen formalen Stiftungsratsbeschluss für das Bearbeitungsverzeichnis? Das Bearbeitungsverzeichnis wurde nicht in das Organisationsreglement integriert.	Für das Erstellen des Bearbeitungsverzeichnisses braucht es unseres Erachtens keinen Beschluss des obersten Organs, da das Bearbeitungsverzeichnis auf dem durch das obersten Organ zu erlassenden Organisationsreglement basiert, auch wenn es nicht im Organisationsreglement integriert ist. Eine Integration würde keinen praktischen Sinn machen, muss das Bearbeitungsverzeichnis doch periodisch aktualisiert werden. Die Pflicht zur Führung eines Bearbeitungsverzeichnisses trifft vorab registrierte Vorsorgeeinrichtungen, die als Bundesorgane qualifizieren. Diese werden ihre Verzeichnisse dem EDÖB melden müssen (Art. 12 Abs. 4 revDSG).

Une décision formelle du conseil de fondation est-elle nécessaire pour le registre des traitements? Le répertoire de traitement n'a pas été intégré dans le règlement d'organisation.	Nous estimons qu'aucune décision de l'organe suprême n'est nécessaire pour l'établissement du registre des traitements, étant donné que le registre des traitements se base sur le règlement d'organisation à édicter par l'organe suprême, même s'il n'est pas intégré dans le règlement d'organisation. Une intégration n'aurait aucun sens pratique, car le registre des traitements doit être mis à jour périodiquement. L'obligation de tenir un registre des traitements concerne en premier lieu les institutions de prévoyance enregistrées qui sont qualifiées d'organes fédéraux. Celles-ci devront annoncer leurs registres au PFPDT (art. 12, al. 4, nLPD).
IMPLEMENTIERUNG EINES PROZESSES ZUM FORTLAUFENDEN MONITORING DER DATENSCHUTZ-COMPLIANCE **IMPLÉMENTATION D'UN PROCESSUS POUR LA SURVEILLANCE EN COURS DE LA CONFORMITÉ À LA LPD**	

Soll das Monitoring an eine bestimmte Rolle geknüpft sein?	Das Monitoring ist Teil des IKS, d.h. Teil der Organisation der Vorsorgeeinrichtung, die zu den undelegierbaren Aufgaben des obersten Organs gehört (Art. 51a Abs. 1 und 2 lit. f BVG/Art. 49 Abs. 2 Ziff. 7 BVG). Dabei wirkt der Datenschutzberater (Art. 10 revDSG/Art. 25ff. revDSV) bei der Anwendung der Datenschutzvorschriften mit. Dieser ist gegenüber dem Verantwortlichen, d.h. dem obersten Organ der Vorsorgeeinrichtung, nicht weisungsgebunden Die Vorsorgeeinrichtung hat dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten zu gewähren, die er zur Erfüllung seiner Aufgaben benötigt (Art. 27 Abs. 1 lit. a revDSV), vorausgesetzt, es stehen keine BVG-Bestimmungen entgegen. Mehrere Bundesorgane können auch gemeinsam einen Datenschutzberater ernennen (Art. 25 revDSV). Das IKS ist Gegenstand der Prüfung der Organisation und Geschäftsführung der Vorsorgeeinrichtung durch die Revisionsstelle, welche die Existenz einer angemessenen internen Kontrolle im Prüfbericht bestätigen muss (Art. 35 Abs. 1 BVV2). *Siehe Marc Hürzeler/Raffaella Biaggi, Art. 52c BVG, in: Marc Hürzeler/Hans-Ulrich Stauffer (Hgg.), Basler Kommentar. Berufliche Vorsorge, Basel 2021, N. 9.*
La surveillance doit-elle être liée à un certain rôle?	La surveillance fait partie du système de contrôle interne (SCI), et donc de l'organisation de l'IP qui compte parmi les tâches de l'organe suprême ne pouvant être déléguées (art. 51a al. 1 et 2 let. f LPP / art. 49 al. 2 chif. 7 LPP). Le conseiller à la protection des données participe à l'application des prescriptions en matière de protection des données (art. 10 nLPD / art. 25ss nOPDo). Il ne doit obéir à aucune instruction de la part du responsable, à savoir l'organe suprême de l'IP. Cette dernière doit garantir au conseiller à la protection des données l'accès à toutes les informations, aux documents et aux registres des activités de traitement ainsi qu'aux données personnelles requises pour l'exercice de ses tâches (art. 27 al. 1 let. a nOPDo), à condition qu'aucune disposition de la LPP ne s'y oppose. Plusieurs organes fédéraux peuvent également désigner ensemble un conseiller à la protection des données (art. 25 nOPDo). L'organisation et la gestion de l'IP sont vérifiés par l'organe de révision, lequel doit attester l'existence d'un contrôle interne approprié dans son rapport (art. 35 al. 1 OPP2). *Voir Marc Hürzeler/Raffaella Biaggi, art. 52c LPP, in: Marc Hürzeler/Hans-Ulrich Stauffer (éd.), Basler Kommentar. Berufliche Vorsorge, Bâle 2021, N° 9.*
Muss das Organisations- oder Vorsorgereglement formell per 01.09.2023 genehmigt sein?	Das Organisationsreglement muss per 01.09.2023 formell durch das oberste Organ genehmigt sein. Das Vorsorgereglement allein genügt nicht.

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.
LÖSCHUNG ODER ANONYMISIERUNG DER DATEN: UMSETZUNG SUPPRESSION OU ANONYMISATION DES DONNÉES : MISE EN ŒVRE	
Wie kann die Anforderung der Löschung oder Anonymisierung der Daten für Vorsorgeeinrichtungen umgesetzt werden? Wie werden Sie die Löschung von Versichertendaten handhaben? Z.B. Informationen über die Zahlung einer FZL-Leistung.	Beanspruchen die Versicherten bzw. Rentnerinnen und Rentner gegenüber der Vorsorgeeinrichtung das «Recht auf Löschung» von Vorsorgedaten i.S. des «Rechts auf Vergessen», hat die Vorsorgeeinrichtung diesen die gesetzlichen Aufbewahrungspflichten der Pensionskassen entgegenzuhalten. Diese gelten sowohl für registrierte als auch für nicht registrierte Vorsorgeeinrichtung gleichermassen. Die Pflicht zur Aufbewahrung von Vorsorgeunterlagen ist in Art. 27i–27k BVV2 geregelt. Die Aufbewahrung von Geschäftsunterlagen richtet sich nach Art. 47 Abs. 4 BVV2 bzw. Art. 958f OR (siehe dazu ASIP-Fachmitteilung Nr. 130, S. 9f.; https://www.datatrust.ch/gesetzesgrundlagen/). «Anonymisiert» sind Daten, die Personenbezug hatten, bei denen der Personenbezug aber bewusst aufgehoben wurde (z.B. Anonymisierung der Personendaten durch Aggregation derselben). Das Datenschutzrecht gilt für diese Daten deshalb nicht mehr. Datenschutzrechtlich ist die Bearbeitung dieser Daten daher nicht mehr eingeschränkt. Eine Anonymisierung von Personendaten hat demzufolge datenschutzrechtlich dieselbe Wirkung wie eine Löschung derselben. Denn wenn das Datenschutzrecht für anonyme Daten nicht gilt, kann auch nicht ihre Löschung verlangt werden. Somit fallen anonymisierte Personendaten als anonyme Daten nicht unter das «Recht auf Vergessen». *Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folien 23f.*
Comment la demande de suppression ou d'anonymi-sation des données peut-elle être mise en œuvre par les IP? Comment la suppression de données des	Si des personnes assurées ou retraitées exigent de l'IP qu'elle leur accorde le droit à la «suppression» de données de prévoyance au sens du «droit à l'oubli», l'IP doit leur signaler qu'elle est tenue de respecter les obligations légales d'archivage des caisses de pension. Elles s'appliquent aussi bien aux IP enregistrées qu'aux non-enregistrées. L'obligation de conserver les documents de prévoyance est réglementée dans l'art. 27i–27k OPP2. La conservation des documents commerciaux est régie par les art. 47 al. 4 OPP2 ou l'art. 958f CO (voir à ce sujet la circulaire de l'ASIP n° 130, p. 9s.; https://www.datatrust.ch/gesetzesgrundlagen/). Les données qui ont un lien avec une personne précise mais qui ont été sciemment supprimées sont «anonymisées» (p. ex. anonymisation des données personnelles au moyen de leur agrégation). La LPD ne s'applique plus à ces données. Du

personnes assurées est-elle gérée? – p. ex. des informations sur le paiement d'une prestation de libre passage.	point de vue du droit à la protection des données, le traitement de ces données n'est plus limité. Une anonymisation de données personnelles a donc, du point de vue légal, les mêmes effets que leur suppression. Car, si le droit à la protection des données ne s'applique pas aux données anonymes, on ne peut pas non plus exiger leur suppression. Ainsi, les données personnelles anonymisées, en tant que données anonymes, n'entrent pas dans la catégorie des données ayant le «droit à l'oubli». *Voir webinaire de l'ASIP sur la protection des données des 10/14/15 novembre 2022, diapositive 23s.*
AUTOMATISIERTE DATENVERARBEITUNGSPROZESSE **PROCESSUS DE TRAITEMENT DES DONNÉES AUTOMATISÉ**	
Welche Datenverarbeitungsprozesse gelten im Pensionskassenbereich als automatisiert?	Unter «Automatisierung» sind «automatisierte Einzelentscheide» zu verstehen. Dabei trifft die Maschine eine Entscheidung aufgrund einer von der Maschine sich antrainierten oder von einem Menschen einprogrammierten Bewertung der der Maschine vorliegenden Personendaten. Im Hinblick auf die Datensicherheit (Art. 8 revDSG) sind geeignete technische und organisatorische Massnahmen für die Gewährleistung einer angemessenen Datensicherheit vorzukehren. Die Datensicherheit zielt auf den Schutz der Vertraulichkeit (keine unbefugten Zugriffe), der Integrität (Korrektheit bzw. Unversehrtheit) sowie der Verfügbarkeit (Zugriff auf Daten) von Daten. Neu sind datenschutzfreundliche Voreinstellungen («privacy by design and default»[2]) erforderlich (Art. 7 Abs. 3 revDSG). Die Vorsorgeeinrichtung hat mit Blick auf das Profiling bzw. das Profiling mit hohem Risiko abzuklären, welche Datenverarbeitungsprozesse im Pensionskassenbereich als automatisiert gelten, da der Datenschutz auch technisch gewährleistet

[2] «Privacy by design» beinhaltet die Pflicht, Prozesse und Projekte so zu gestalten, dass die Einhaltung des Datenschutzes von Anfang an berücksichtigt wird. Im Sinne von «privacy by default» ist mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

[2] La protection des données dès la conception (*privacy by design*) inclut l'obligation de concevoir les processus et les projets de manière à ce que le respect de la protection des données soit pris en compte dès le début. Protéger les données par défaut (*privacy by default*) consiste à garantir, au moyen de paramètres par défaut appropriés que le traitement des données personnelles se limitera au minimum nécessaire pour l'utilisation prévue, pour autant que la personne concernée n'en décide autrement.

Quels processus de traitement de données sont considérés comme automatisés dans le domaine des caisses de pension?	sein muss. Dabei gibt es beispielswiese folgende Möglichkeiten der Prozessautomatisierung (Entlastung der Mitarbeitenden bei der Bearbeitung: Robotic Process Automation [RPA]): 1. Zahlungseingangsprozess, 2. Eintrittsprozess, 3. Lohn- und Beschäftigungsgradänderung, 4. Einkaufsanfrage. Bei der Erstellung von Vorsorgeausweisen empfiehlt es sich, der Informationspflicht gemäss Art. 21 Abs. 4 revDSG nachzukommen und einen Verweis beispielsweise mit **dieses Dokument wurde automatisch erstellt** anzubringen (ASIP-Fachmitteilungen Nr. 130, S. 4, und Nr. 131, S. 9). Par «automatisation», il faut entendre des «décisions individuelles automatisées». La machine prend une décision sur la base d'une évaluation des données personnelles dont elle dispose et qu'elle a apprises, ou que ce processus d'évaluation a été programmé par un être humain. En ce qui concerne la sécurité des données (art. 8 nLPD), il convient de prendre des mesures visant à garantir une sécurité appropriée qui permette de protéger la confidentialité des données (aucun accès non autorisé), leur intégrité (exactitude et fiabilité) ainsi que leur disponibilité (accès aux données). Désormais, des paramètres de protection des données dès la conception et par défaut (privacy by design and default [2]) sont requis (art. 7 al. 3 nLPD). Dans la perspective d'un profilage, voire d'un profilage à haut risque, l'IP doit déterminer quels processus de données sont considérés comme automatisés dans le domaine des caisses de pension, car la protection des données doit être également assurée sur le plan technique. Il s'agit, p. ex., des possibilités suivantes d'automatisation des processus (allègement de la tâche des collaboratrices ou collaborateurs lors du traitement de données: Robotic Process Automation [RPA]): 1) processus de réception des paiements, 2) processus d'entrée, 3) modification du salaire / du taux d'activité, 4) demande de rachat. Lors de l'élaboration de certificats de prévoyance, il est conseillé de respecter le devoir d'informer selon l'art. 21 al. 4 nLPD et d'ajouter, p. ex., la mention «*Ce document a été généré automatiquement*» (circulaires de l'ASIP n° 130, p. 4, et n° 131, p. 9).
ABLAGE DER PROTOKOLLE ARCHIVAGE DES PROCÈS-VERBAUX	
Wie und in welcher	Das ist eine technische Frage, welche die Vorsorgeeinrichtungen mit ihren IT-Unternehmen regeln müssen.

Form sollten die Protokolle getrennt vom System abgelegt werden?	
Comment et sous quelle forme les procès-verbaux devraient-ils être classés séparément, en dehors du système?	C'est une question technique que les IP doivent régler avec leur fournisseur d'informatique.
MELDEPROZESS BEIM EDÖB **PROCESSUS DE DÉCLARATION AUPRÈS DU PFPDT**	
Gibt es bereits Detailinformationen zum Meldeprozess beim EDÖB?	Ja. Betroffen ist die Meldepflicht der Bearbeitungsverzeichnisse der registrierten Vorsorgeeinrichtungen (Art. 12 Abs. 4 revDSG). Es ist dieses neue Portal zu benutzen: https://datareg.edoeb.admin.ch/search. Um als Bundesorgan einen Benutzer-Zugang für die Erfassung und Pflege von Verzeichniseinträgen zu erhalten, muss sich die entsprechende Vorsorgeeinrichtung per E-Mail an info@edoeb.admin.ch wenden. *Siehe dazu https://www.edoeb.admin.ch/edoeb/de/home/meldeportale/datareg.html.* Daneben gibt es die Meldepflicht des Verantwortlichen von Datenschutzverletzungen, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen (Art. 24 revDSG).
Existe-t-il déjà des informations détaillées sur le processus de déclaration auprès du PFPDT?	Oui. Cela concerne l'obligation, pour les IP, de déclarer les registres de traitement de données (art. 12 al. 4 nLPD). Il convient d'utiliser ce nouveau portail: https://datareg.edoeb.admin.ch/search. Pour avoir accès à ce portail en tant qu'organe fédéral à des fins de saisie ou de mise à jour dans le registre, l'institution de prévoyance concernée doit s'adresser par e-mail à info@edoeb.admin.ch. *Voir à ce sujet https://www.edoeb.admin.ch/edoeb/fr/home/meldeportale/datareg.html.* En outre, le responsable est tenu de notifier les violations de la protection des données susceptibles d'engendrer un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 24 nLPD).
Ist der Inhalt auf der Meldeplattform EDÖB für die Öffentlichkeit	Ja. Der EDÖB veröffentlicht die Meldungen der Bundesorgane gemäss Art. 56 revDSG in einem öffentlich zugänglichen Register, dem DataReg (Meldepflicht nur für Verzeichnisse von Bundesorganen [Art. 12 Abs. 4 revDSG]). *Siehe https://www.edoeb.admin.ch/edoeb/de/home/meldeportale/datareg.html.*

jederzeit einsehbar? 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/meldeportale/datareg.html.*
UNTERSCHEIDUNG SCHÜTZENSWERTE UND BESONDERS SCHÜTZENSWERTE PERSONENDATEN DISTINCTION ENTRE DONNÉES PERSONNELLES SENSIBLES ET DONNÉES PERSONNELLES PARTICULIÈREMENT SENSIBLES	
Welche Daten werden als besonders schützenswert erachtet. (z.B. Zivilstand, IV-Grad usw.) Quelles données sont considérées comme particulièrement sensibles (p. ex. État civil, degré d'invalidité, etc.)?	Besonders schützenswerte Daten i.S. des revDSG sind: 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren, 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, 6. Daten über Massnahmen der sozialen Hilfe (Art. 5 lit. c revDSG). Données particulièrement sensibles au sens de la nLPD: 1) les données relatives aux opinions ou activités religieuses, idéologiques, politiques ou syndicales; 2) les données relatives à la santé, la sphère intime ou l'appartenance à une race ou à une ethnie; 3) les données génétiques; 4) les données biométriques qui permettent d'identifier clairement une personne physique; 5) les données relatives à des poursuites ou des sanctions administratives ou pénales; 6) les données relatives à des mesures d'aide sociale (art. 5 let. c nLPD).
BEARBEITUNGSREGLEMENT	

RÈGLEMENT DE TRAITEMENT	
Ist eine Mehrzahl von Bearbeitungs-reglementen möglich?	Ja: Bearbeitungsreglement von Bundesorganen bei automatisierter Bearbeitung u.a. von besonders schützenswerten Personendaten oder bei automatisierter Durchführung eines Profilings (Art. 6 revDSV); Bearbeitungsreglement von privaten Personen, d.h. von nicht registrierten Vorsorgeeinrichtungen, bei automatisierter Bearbeitung besonders schützenswerter Personendaten in grossem Umfang oder bei automatisierter Durchführung eines Profilings mit hohem Risiko (Art. 5 revDSV).
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).
DATENSCHUTZBERATER CONSEILLER À LA PROTECTION DES DONNÉES	
Wer ist dafür zuständig, zu kontrollieren, dass bei den Pensionskassen alles richtig umgesetzt wird, der EDÖB?	Nein, die Datenschutzberaterin bzw. der Datenschutzberater (Art. 10 revDSG/Art. 25ff. revDSV). Diese/dieser wirkt u.a. bei der Anwendung der Datenschutzvorschriften mit: sie/er prüft die Bearbeitung von Personendaten, empfiehlt Korrekturmassnahmen nach Feststellung einer Verletzung der Datenschutzvorschriften, berät die Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung und überprüft deren Ausführung. Dabei hat die Vorsorgeeinrichtung der Datenschutzberaterin/dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten zu gewähren, die sie/er zur Erfüllung ihrer/seiner Aufgaben benötigt (Art. 27 Abs. 1 lit. a revDSV). Der EDÖB kann jedoch eine Untersuchung eröffnen, wenn er Kenntnis von einem Datenschutzvorfall erhält (Art. 49 revDSG).
Qui est chargé de contrôler que tout est correctement mis en œuvre dans les caisses de pension, le PFPDT?	Non, le conseiller à la protection des données (art. 10 nLPD/art. 25 ss. nOPDo). Celui-ci/celle-ci participe entre autres à l'application des prescriptions en matière de protection des données: il/elle contrôle le traitement des données personnelles, recommande des mesures correctives après avoir constaté une violation des prescriptions en matière de protection des données, conseille les responsables lors de l'élaboration de l'analyse d'impact relative à la protection des données et contrôle son exécution. Dans ce cadre, l'institution de prévoyance doit permettre au conseiller à la protection des données d'accéder à tous les renseignements, documents, listes des activités de traitement et données personnelles dont il a besoin pour accomplir ses tâches (art. 27, al. 1, let. a, nOPDo). Le PFPDT peut toutefois ouvrir une enquête s'il a connaissance d'un incident en matière de protection des données (art. 49 nLPD).
Ist die Ernennung der	Die Ernennung der Datenschutzberaterin bzw. des Datenschutzberaters liegt beim obersten Organ der Vorsorgeeinrich-

Datenschutzberaterin bzw. des Datenschutzberaters (Art. 25 revDSV) zwingend Sache des obersten Organes, oder kann dies auch durch die Geschäftsführung geschehen? 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?	tung. Erstens gehört nämlich der Datenschutz (Umsetzung des revDSG) zur Organisation der Vorsorgeeinrichtung, ist somit Teil einer unentziehbaren und undelegierbaren Aufgabe des obersten Organs (Art. 51a Abs. 1 i.V.m. Art. 49 Abs. 2 Ziff. 7 BVG), und zweitens ergibt sich dieses Erfordernis auch aus den Aufgaben der Datenschutzberaterin bzw. des Datenschutzberaters (Art. 10 Abs. 2 revDSG und Art. 26 Abs. 2 revDSV): a. Schulung und Beratung des obersten Organs im Bereich des Datenschutzes, b. Mitwirkung bei der Anwendung der Datenschutzvorschriften (Prüfung der Bearbeitung von Personendaten, Empfehlung von Korrekturmassnahmen nach Feststellung einer Verletzung der Datenschutzvorschriften), c. Beratung der Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung und Überprüfung von deren Ausführung und d. Ansprechpartner für die versicherten Personen und die Datenschutzbehörden. *Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.* 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.*
Ist es mit Blick auf die fachliche Unabhängigkeit und Weisungsungebundenheit des Datenschutzberaters gemäss Art. 10 Abs. 3 lit. a revDSG denkbar, dass die Pensionskasse den Datenschutzberater des Arbeitgebers ernennt, oder sind da Interessens-	1. Es ist für eine Vorsorgeeinrichtung möglich, den Datenschutzberater des Arbeitgebers als eigenen Datenschutzberater zu ernennen. Auch können mehrere Bundesorgane (registrierte Vorsorgeeinrichtungen) gemeinsam einen Datenschutzberater ernennen (Art. 25 revDSV). Nicht registrierten Vorsorgeeinrichtungen ist die Ernennung eines Datenschutzberaters freigestellt. 2. Die fachliche Unabhängigkeit und Weisungsungebundenheit sind vertraglich sicherzustellen. Dabei ist zu beachten, dass Personen, welche pensionskassenintern als für den Datenschutz zuständig erklärt werden, nicht automatisch als Datenschutzberater im Sinne von Art. 10 revDSG gelten. Die Datenschutzberater müssen als solche bezeichnet werden. *Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.*

konflikte zu befürchten, die einer solchen Ernennung entgegenstehen? Est-il concevable que la caisse de pension nomme le conseiller à la protection des données de l'employeur, compte tenu de l'indépendance professionnelle du conseiller et du fait qu'il n'est pas lié par des instructions selon l'art. 10, al. 3, let. a, nLPD, ou faut-il craindre des conflits d'inté-rêts qui s'opposeraient à une telle nomination?	1. Une institution de prévoyance a la possibilité de désigner le conseiller à la protection des données de l'employeur comme le sien. De même, plusieurs organes fédéraux (institutions de prévoyance enregistrées) peuvent désigner conjointement un conseiller à la protection des données (art. 25 nOPDo). Les institutions de prévoyance non enregistrées sont libres de désigner un conseiller à la protection des données. 2. L'indépendance professionnelle et le fait de ne pas être lié par des instructions doivent être garanties par contrat. Il convient de noter que les personnes qui sont déclarées responsables de la protection des données au sein de la caisse de pension ne sont pas automatiquement considérées comme des conseillers à la protection des données au sens de l'art. 10 nLPD. Ceux-ci doivent être désignés comme tels. *Voir le webinaire de l'ASIP sur la protection des données des 10/14/15 novembre 2022, diapositive 26.*
Sind mit der in der ASIP-Fachmitteilung Nr. 131, S. 8 unten, angekündigten IT-basierten Plattform die Anforderungen des neuen DSG an ein Bundesorgan abgedeckt, oder muss man parallel zur IT-basierten Plattform noch andere Aufgaben	Durch die vom ASIP für seine Mitglieder zur Verfügung gestellte IT-basierte Plattform (verbunden mit regelmässiger Begleitung und entsprechenden Schulungsangeboten) soll den Vorsorgeeinrichtungen die Suche eines Datenschutzberaters teilweise erleichtert werden. Die Ernennung desselben muss jedoch durch die jeweilige Vorsorgeeinrichtung selbst vorgenommen werden (zwingende Weisungsungebundenheit des Datenschutzberaters). Allerdings besteht für die registrierten Vorsorgeeinrichtungen die Möglichkeit, dass mehrere Bundesorgane gemeinsam einen Datenschutzberater bzw. eine Datenschutzberaterin ernennen können (Art. 25 revDSV). Mit dessen Ernennung ist das Erfordernis des revDSG erfüllt. Die Aufgaben des Datenschutzberaters (Art. 10 Abs. 2 revDSG und Art. 26 Abs. 2 revDSV) sind: a. Schulung und Beratung des obersten Organs im Bereich des Datenschutzes, b. Mitwirkung bei der Anwendung der Datenschutzvorschriften (Prüfung der Bearbeitung von Personendaten, Empfehlung von Korrekturmassnahmen nach Feststellung einer Verletzung der Datenschutzvorschriften, c. Beratung der Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung und Überprüfung von deren Ausführung und d. Ansprechpartner für die versicherten Personen und die Datenschutzbehörden.

beachten? La plate-forme informatique annoncée dans la circulaire de l'ASIP n° 131, p. 8 ci-dessous, couvre-t-elle les exigences de la nouvelle LPD à l'égard d'un organe fédéral ou faut-il tenir compte d'autres tâches parallèlement à la plate-forme informatique?	*Siehe ASIP-Webinare Datenschutz vom 10./14./15. November 2022, Folie 26.* La plate-forme informatique mise à la disposition de ses membres (associée à un suivi régulier et à des offres de formation pertinentes) par l'ASIP doit aider en partie les institutions de prévoyance à rechercher un conseiller à la protection des données. La nomination de cette personne doit toutefois être effectuée par l'institution de prévoyance elle-même (cette personne ne doit pas être liée par des instructions). Néanmoins, plusieurs organes fédéraux ont la possibilité de nommer conjointement un conseiller ou une conseillère à la protection des données (art. 25 nOPDo). La nomination de cette personne satisfait à l'exigence de la nLPD. Les tâches du conseiller à la protection des données (art. 10, al. 2, nLPD et art. 26, al. 2, nOPDo) sont les suivantes: a) former et conseiller l'organe suprême dans le domaine de la protection des données, b) participer à l'application des dispositions relatives à la protection des données (vérification du traitement des données personnelles, recommandation de mesures correctives après constatation d'une violation des dispositions relatives à la protection des données), c) conseiller les responsables lors de l'élaboration de l'analyse d'impact relative à la protection des données et vérifier la mise en œuvre de celle-ci) et, d) être l'interlocuteur des personnes assurées et des autorités de protection des données. *Voir le webinaire de l'ASIP sur la protection des données des 10/14/15 novembre 2022, diapositive 26.*
Nach Art. 27 Abs. 2 DSV muss der/die Datenschutzberater/in auf dem Internet publiziert werden. Als firmeneigene Pensionskasse betreiben wir keine öffentlich-zugängliche Website. Muss extra für diese Information eine solche erstellt werden? Selon l'art. 27, al. 2, nOPDo, le nom du conseiller ou de la	Ja, grundsätzlich schon. Allenfalls besteht die Möglichkeit einer Veröffentlichung auf der Website des Arbeitgebers (Firma). En principe, oui. Il existe éventuellement la possibilité d'une publication sur le site web de l'employeur (entreprise).

conseillère à la protection des données doit être publié sur internet. En tant que caisse de pension de l'entreprise, nous ne disposons pas d'un site Internet accessible au public. Faut-il en créer un spécialement pour publier cette information?	
Benötigt es einen formellen Stiftungsratsbeschluss für die Ernenung des Datenschutzberaters? Une décision formelle du conseil de fondation est-elle nécessaire pour la nomination du conseiller à la protection des données?	Die Ernnenung des Datenschutzberaters verlangt einen Beschluss des obersten Organs, wobei nicht registrierten Vorsorgeeinrichtungen die Ernennung eines Datenschutzberaters freigestellt ist. Erstens gehört nämlich der Datenschutz (Umsetzung des revDSG) zur Organisation der Vorsorgeeinrichtung, ist somit Teil einer unentziehbaren und undelegierbaren Aufgabe des obersten Organs (Art. 51a Abs. 1 und 2 lit. f BVG/Art. 49 Abs. 2 Ziff. 7 BVG), und zweitens ergibt sich dieses Erfordernis auch aus den Aufgaben des Datenschutzberaters (Art. 10 Abs. 2 revDSG und Art. 26 Abs. 2 revDSV). Dabei ist der Datenschutzberater gegenüber dem Verantwortlichen, d.h. dem obersten Organ der Vorsorgeeinrichtung, nicht weisungsgebunden. La nomination du conseiller à la protection des données requiert une décision de l'organe suprême, bien que les institutions de prévoyance non enregistrées soient libres de nommer un conseiller à la protection des données. Premièrement, la protection des données (mise en œuvre de la nLPD) fait partie de l'organisation de l'institution de prévoyance et constitue donc une tâche inaliénable et intransmissible de l'organe suprême (art. 51a, al. 1 et 2, let. f, LPP/art. 49, al. 2, ch. 7, LPP), et deuxièmement, cette exigence découle également des tâches du conseiller à la protection des données (art. 10, al. 2, nLPD et art. 26, al. 2, nOPDo). Dans ce contexte, le conseiller à la protection des données n'est pas tenu de suivre les instructions du responsable, c'est-à-dire de l'organe suprême de l'institution de prévoyance.
DATENSCHUTZ-FOLGENABSCHÄTZUNG **ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES**	
Muss eine Datenschutz-	Die Datenschutz-Folgenabschätzung muss nicht per 1. September 2023 durchgeführt werden, sondern erst wenn ein zu beurteilendes Risiko entsteht. Dieses ergibt sich, insbesondere bei Verwendung neuer Technologien, im Zusammenhang

Folgenabschätzung zum Zeitpunkt des Inkrafttretens durchgeführt werden oder nur, wenn es eine Änderung des Bearbeitungskonzepts gibt? Une analyse d'impact relative à la protection des données doit-elle être effectuée au moment de l'entrée en vigueur ou seulement s'il y a une modification du concept de traitement?	mit umfangreichen Bearbeitungen besonders schützenswerter Personendaten, mit einer wesentlichen Änderung der Bearbeitung von Personendaten, einer Änderung des Bearbeitungszwecks oder der Beschaffung neuer Daten (Art. 22 Abs. 2 revDSG), beispielsweise bei der Auslagerung der technischen Verwaltung an einen Dritten, der Einführung eines Versichertenportals oder der Nutzung einer Cloudlösung. L'analyse d'impact relative à la protection des données ne doit pas être effectuée pour le 1er septembre 2023, mais seulement lorsqu'un risque à évaluer apparaît. Celui-ci apparaît, notamment en cas d'utilisation de nouvelles technologies, en relation avec des traitements à grande échelle de données personnelles sensibles, avec une modification importante du traitement de données personnelles, un changement de finalité du traitement ou la collecte de nouvelles données (art. 22, al. 2 nLPD), par exemple en cas d'externalisation de la gestion technique à un tiers, d'introduction d'un portail des assurés ou d'utilisation d'une solution en nuage.
Wie lange müssen Datenschutz-Folgenabschätzungen aufbewahrt werden? Combien de temps les analyses d'impact sur la protection des données doivent-elles être conservées?	Der Verantwortliche, d.h. die Vorsorgeeinrichtung, muss die Datenschutz-Folgenabschätzung nach Beendigung der Datenbearbeitung mindestens zwei Jahren aufbewahren (Art. 14 revDSV). Le responsable, c'est-à-dire l'institution de prévoyance, doit conserver l'analyse d'impact relative à la protection des données pendant au moins deux ans après la fin du traitement des données (art. 14 nOPDo).

OUTSOURCING-VERHÄLTNISSE **RELATIONS D'OUTSOURCING**	
Vereinbarungen zur Datenverarbeitung sind mit Dienstleistern und IT-Providern abzuschliessen:	
1. Was bedeutet dies im Outsourcing-Verhältnis (Auslagerung der Verwaltung)? Reicht die Bestätigung des Outsourcing-Partners für ihre IT-Provider (Cloud, PK-Software)?	1. Hat die Vorsorgeeinrichtung ihre Verwaltung (Geschäftsführung, technische Verwaltung, Administration Aktive und Rentner, Rechnungswesen) an einen Dritten ausgelagert, so erfolgt die Datenbearbeitung durch die Verwaltung (als Auftragsbearbeiter) im Auftrag der Vorsorgeeinrichtung (Art. 9 revDSG). Letztere muss dann insbesondere sicherstellen, dass die Verwaltung in der Lage ist, die Datensicherheit zu gewährleisten, da die Vorsorgeeinrichtung weiterhin verantwortlich ist. Ein weiteres Beispiel eines Auftragsbearbeiters ist der Cloud-Provider (Cloud-Software). In diesem Fall muss die ganze Kette von der Vorsorgeeinrichtung über den/die Software-Anbieter und Cloud-Provider vertraglich abgesichert sein. Des Weiteren darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung der Vorsorgeeinrichtung einem Dritten übertragen. In allen Fällen ist ein entsprechender Vertrag abzuschliessen (Auftragsbearbeitungsvertrag oder «Data Processing Agreement»). Dabei gilt der Cloud-Provider (bei der Speicherung von Daten auf der vom IT-Provider betriebenen Cloud) lediglich als Auftragsbearbeiter gemäss revDSG, die Vorsorgeeinrichtung jedoch ist Verantwortliche. Sie hat sämtliche verwaltungs- und IT-technischen Abläufe vertraglich zu regeln. *Bestimmt jedoch eine Servicegesellschaft selbst über den Zweck und die Mittel der im Rahmen des Auftrags vorzunehmenden Datenbearbeitungen, so gilt sie datenschutzrechtlich – neben der Vorsorgeeinrichtung – als eigenständige Verantwortliche (Co-Controller) und nicht als Auftragsbearbeiterin (Processor). Diese Differenzierung muss in der Auftragsdatenvereinbarung (ADV) zwischen der Vorsorgeeinrichtung und der Servicegesellschaft geregelt werden («Data Processing Agreement» bzw. «Controller to Processor Agreement» vs. «Controller to Controller Agreement»), weshalb das reine Auftragsrecht nicht genügt. Mit dem IT-Unternehmen zu regeln ist beispielsweise die technische Frage, wie die Protokolle getrennt vom System, in welchem die Personendaten bearbeitet werden, während mindestens einem Jahr aufbewahrt (Art. 4 Abs. 5 DSV) werden können.*[3]
2. Subdelegation vom Processor an Sub-Processor ist nur mit	2. Ja. Die Vorsorgeeinrichtung hat als Verantwortliche gemäss revDSG auch das Verhältnis vom Processor zum Sub-Processor vertraglich mit dem Outsourcing-Partner zu regeln. Dabei sind namentliche Nennungen nicht notwendig (Ausnahme: Bearbeitungsverzeichnis; *siehe oben*).

[3] Ergänzung vom 26.02.2025: Der EDÖB hat sich auf seiner Website unter FAQ → Versicherungen zur Frage geäussert, ob eine Dienstleistungsgesellschaft, an welche eine Vorsorgeeinrichtung einen Teil oder die Gesamtheit des operativen Geschäftsbetriebs übertragen hat, eine Auftragsbearbeiterin oder eine Verantwortliche ist: https://www.edoeb.admin.ch/de/faq (zuletzt besucht am 26.02.2025).

vorgängiger Genehmigung des Verantwortlichen zulässig. Wie sehen Sie das in der Praxis? Sind namentliche Nennungen notwendig?	
3. Gilt die Post als Verantwortliche oder als Datenbearbeiterin gemäss revDSG?	3. Für die Datenbearbeitung auf der Transportebene – wozu auch die Adressen auf den Postsendungen gehören – ist die Post verantwortlich (= Verantwortliche nach revDSG); die Datenbearbeitung auf der Inhaltsebene – was die Kunden in ihren Briefen oder auf ihren Postkarten schreiben – ist Sache der Postkunden, hier also der Vorsorgeeinrichtung (Vorsorgeeinrichtung = Verantwortliche nach revDSG). Es liegt keine gemeinsame Verantwortlichkeit der Vorsorgeeinrichtung und der Post vor, sondern diese sind je auf ihrer Tätigkeitsebene Verantwortliche gemäss revDSG. Deshalb tangiert ein von der Post fehlzugestellter Brief nicht die datenschutzrechtliche Verantwortlichkeit der Vorsorgeeinrichtung, während ein falschadressierter Brief einzig in der datenschutzrechtlichen Verantwortlichkeit der Vorsorgeeinrichtung liegt, mit entsprechenden Folgen etwa für die Meldepflichten bei Datenschutzverstössen. *Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 87.*
Des accords portant sur le traitement des données doivent être conclus avec des prestataires de services et des fournisseurs informatiques :	
1. Quelles conséquence cela aura-t-il dans le cadre de la relation d'outsourcing (externalisation de la gestion)? La confirmation du partenaire d'outsourcing est-elle	1. Si l'institution de prévoyance a externalisé sa gestion (gestion technique, administration des actifs et des retrai-tés, comptabilité) auprès d'un tiers, le traitement des données est alors effectué par l'administration – en tant que sous-traitante – sur mandat de l'institution de prévoyance (art. 9 nLPD). Cette dernière doit alors s'assurer en particulier que l'administration est en mesure de garantir la sécurité des données, car l'institution de prévoyance reste responsable. Le fournisseur de cloud (lo-giciel en nuage) est un autre exemple de sous-traitant. Dans ce cas, toute la chaîne allant de l'institution de prévoyance au(x) fournisseur(s) de logiciels et au(x) fournisseur(s) de cloud doit être sécurisée par contrat. Par ailleurs, le sous-traitant ne peut confier le traitement à un tiers qu'avec l'autorisation préalable de l'institution de prévoyance. Dans tous les cas, un contrat ad hoc doit être conclu (contrat de traitement des données ou «Data Pro-

suffisante pour leurs fournisseurs informatiques (cloud, logiciel CP)?	cessing Agreement»). Dans ce contexte, le fournisseur de cloud (en cas de stockage de données sur le cloud exploité par le fournisseur informatique) n'est considéré que comme un sous-traitant au sens de la nLPD, mais l'institution de prévoyance est néanmoins responsable. Elle doit régler par contrat tous les processus administratifs et informatiques. Toutefois, si une société de services décide elle-même de la finalité et des moyens des traitements de données à effectuer dans le cadre du mandat, elle est considérée, du point de vue de la protection des données, comme un responsable indépendant (co-contrôleur) - aux côtés de l'institution de prévoyance – et non comme un sous-traitant (processor). *Cette différenciation doit être réglée dans l'accord sur les données du mandat entre l'institution de prévoyance et la société de services («Data Processing Agreement» ou «Controller to Processor Agreement» vs «Controller to Controller Agreement»), raison pour laquelle le simple droit du mandat ne suffit pas. Il faut par exemple régler avec l'entreprise informatique la question technique de savoir comment les journaux peuvent être conservés pendant au moins un an, séparément du système dans lequel les données personnelles sont traitées (art. 4, al. 5, nOPDo).*[4]
2. La subdélégation du processeur au sous-processeur n'est autorisée qu'avec l'accord préalable du responsable. Comment voyez-vous cela dans la pratique ? Des désignations nominatives sont-elles nécessaires ?	2. Oui. En tant que responsable selon la nLPD, l'institution de prévoyance doit également régler par contrat avec le partenaire d'outsourcing la relation entre le processeur et le sous-processeur. Il n'est pas nécessaire de men-tionner les désignations (à l'exception du registre des activités de traitement; voir plus haut).
3. La Poste est-elle considérée comme responsable ou chargée du traitement des données au sens de la nLPD?	3. La Poste est responsable du traitement des données au niveau du transport – dont font partie les adresses fi-gurant sur les envois postaux – (= responsable selon la nLPD); le traitement des données au niveau du contenu – ce que les clients écrivent dans leurs lettres ou sur leurs cartes postales – est l'affaire des clients de la Poste, donc ici de l'institution de prévoyance (= responsable selon la nLPD). Il n'existe pas de responsabilité commune entre l'institution de prévoyance et la Poste, chacune d'elles étant responsable à son niveau d'activité selon la nLPD. Une lettre envoyée par erreur par la Poste à un mauvais destinataire n'affecte donc pas la responsabilité de l'institution de prévoyance en matière de protection des données, en l'occurrence l'institution de prévoyance, alors qu'une lettre portant une adresse er-

[4] Complément du 26.02.2025: Le PFPDT s'est exprimé sur son site Internet sous FAQ → Assurances sur la question de savoir si une société de services à laquelle une institution de prévoyance a confié une partie ou l'ensemble de ses activités opérationnelles est un sous-traitant ou un responsable du traitement: https://www.edoeb.admin.ch/fr/questions-frequemment-posees (dernière visite le 26.02.2025).

	ronée relève uniquement de la responsabilité de l'institution de prévoyance, avec les conséquences qui en découlent, p. ex. en ce qui concerne les obligations d'annoncer les violations de la protection des données. *Voir David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17 juin 2019, cm 87.*
Wie gestaltet sich das Verhältnis der Vorsorgeeinrichtung als Verantwortliche zu anderen Verantwortllichen gemäss revDSG? Comment se présente la relation entre l'institution de prévoyance en tant que responsable et les autres responsables selon la nLPD?	Wenn eine Vorsorgeeinrichtung im Bereich ihrer Tätigkeit als Bundesorgan Dienstleistungen an einen Datenschutzverantwortlichen (wie PK-Experte, Anwalt, etc.) outsourced, muss dieser wie die VE selbst alle gesetzlichen Anforderungen erfüllen, dies im Unterschied zum Auftragsbearbeiter. Im Verhältnis der Vorsorgeeinrichtung (Verantwortliche) zu einem Dritten, der ebenfalls Verantwortlicher ist (insbesondere zu Organen gemäss Art. 52 BVG), empfiehlt sich eine vertragliche Regelung für den Datentransfer von der Vorsorgeeinrichtung zu diesem Dritten (Abgrenzung der Verantwortlichkeiten gemäss revDSG und Art. 52 BVG) (ASIP-Fachmitteilung Nr. 131, S. 8). Lorsqu'une institution de prévoyance externalise ses activités, en tant qu'organe fédéral, auprès d'un responsable de la protection des données (comme un expert CP, un avocat, etc.), le prestataire externe doit, tout comme l'institution de prévoyance elle-même, satisfaire à toutes les exigences légales, ceci à la différence du sous-traitant. Dans les relations entre l'institution de prévoyance (responsable) et un tiers qui est également responsable (en particulier des organes selon l'art. 52 LPP), il est recommandé de prévoir une réglementation contractuelle pour le transfert de données de l'institution de prévoyance à ce tiers (délimitation des responsabilités selon la nLPD et l'art. 52 LPP). Voir circulaire de l'ASIP n° 131, p. 8.
Was passiert, wenn kein Vertrag mit einem Auftragsbearbeiter unterzeichnet wird?	Gemäss Art. 9 Abs. 1 revDSG kann die Bearbeitung von Personendaten vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn: a. die Daten so bearbeitet werden, wie der Verantwortliche, d.h. die VE, selbst es tun dürfte; und b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. Der Auftragsbearbeiter handelt auf Weisung und für die Zwecke des Verantwortlichen, d.h. der VE. Wenn kein Vertrag mit einem Auftragsbearbeiter unterzeichnet wird (und auch keine gesetzliche Bestimmung zur Auftragsbearbeitung zwingt), kommt das Auftragsrecht (Art. 394ff. OR) zur Anwendung. Dieses bestimmt, dass, Verträge über Arbeitsleistung, die keiner besonderen Vertragsart des Obligationenrechts (OR) unterstellt sind, unter den Vorschriften über den Auftrag stehen (Art. 394 Abs. 2 OR). Das Zustandekommen des Auftrags bedarf keiner besonderen Form, also auch nicht der Schriftlichkeit (https://digilaw.ch/im-internet-praktisch-alle-vetraege-formlos/). Dabei gilt es jedoch zu beachten, dass nicht jeder Auftragnehmer automatisch als Auftragsbearbeiter qualifiziert.

Que se passe-t-il si aucun contrat n'est signé avec un sous-traitant?	Selon l'art. 9, al. 1, de la nLPD, le traitement de données personnelles peut être confié à un sous-traitant par contrat ou par la législation si: a. les données sont traitées comme le responsable, c'est-à-dire l'IP, devrait le faire lui-même; et b. aucune obligation légale ou contractuelle de garder le secret n'interdit la délégation. Le sous-traitant agit sur instruction et pour les besoins du responsable, c'est-à-dire l'IP. Si aucun contrat n'est signé avec un sous-traitant (et si aucune disposition légale n'impose le traitement d'un mandat), le droit du mandat (art. 394 ss. CO) s'applique. Celui-ci stipule que les contrats portant sur des prestations de travail qui ne sont pas soumis à un type de contrat particulier du Code des obligations (CO) sont régis par les dispositions relatives au mandat (art. 394, al. 2, CO). La conclusion du mandat ne requiert pas de forme particulière, donc pas non plus d'écrit (https://digilaw.ch/im-internet-praktisch-alle-vetraege-formlos/). Il convient toutefois de noter que tout mandataire n'est pas automatiquement qualifié de mandataire.
Die Pensionskasse befindet sich an einem der Standorte des Unternehmens. Sie nutzt bestimmte IT-Dienste des Arbeitgebers, wie z. B. das E-Mail-Programm Outlook, um mit unseren Versicherten zu kommunizieren, oder den Online-Speicher OneDrive (auch wenn der Zugang gesichert und speziell für die Pensionskasse ist), der auf den Servern des Arbeitgebers gehostet wird, sowie verschiedene Tools (Buchhaltungssoftware, Zahlungssoftware). Könnte dies ein Prob-	Der Arbeitgeber und seine Pensionskasse sind völlig getrennte Einheiten. In seinem Urteil vom 10. April 2012 (A-4467/2011) stellte das Bundesverwaltungsgericht klar, dass die Bearbeitung und Veröffentlichung von Personendaten unter das Bundesgesetz über den Datenschutz (DSG, ergänzt durch die gesetzlichen Spezialnormen des BVG und des OR) fällt und dass die Vorsorgeeinrichtung dem Arbeitgeber nur diejenigen Personendaten übermitteln darf, die für die Erfüllung der im Arbeitsvertrag und im Rahmen der beruflichen Vorsorge vorgesehenen Aufgaben objektiv notwendig sind. Gemäss dem Bundesverwaltungsgericht verstösst es gegen den Grundsatz der Datensicherheit (Art. 7 DSG), wenn Vorsorgeausweise in unverschlossenen Umschlägen an die Arbeitgeber zur Weiterleitung an die bei ihnen versicherten Arbeitnehmenden abgegeben werden. Dies wird natürlich auch unter dem neuen Datenschutzgesetz gelten. Aus diesem Grund muss die Pensionskasse, die nach dem geltenden Datenschutzgesetz und dem neuen Datenschutzgesetz Verantwortliche ist, sicherstellen, dass der Arbeitgeber keinen Zugriff auf die persönlichen Daten der Versicherten und Rentnerinnen und Rentner hat. In Bezug auf das revDSG sollte die Pensionskasse mit dem Cloud-Anbieter des Arbeitgebers einen Vertrag zur Auftragsdatenverarbeitung («Data Processing Agreement») aushandeln, der sicherstellt, dass die IT-Dienste des Arbeitgebers für den Arbeitgeber in Bezug auf die persönlichen Daten der Versicherten und Rentnerinnen und Rentner absolut undurchlässig sind. Da der Zugang sicher und spezifisch für die Pensionskasse ist, scheint das (geltende und neue) Datenschutzgesetz eingehalten zu werden. Wichtig ist, dass die Buchhaltungssoftware und die Zahlungssoftware auch für den Arbeitgeber undurchlässig sind. Dies alles sollte jedoch im Vertrag (zumindest in einer Vertragsklausel) vorgesehen werden.

lem darstellen? Was müsste unternommen werden, um das revDSG gegebenenfalls einzuhalten? La Caisse de pension se trouve sur l'un des sites de l'entreprise. Elle utilise certains services informatiques de l'employeur, comme par exemple la messagerie Outlook pour communiquer avec nos assurés, ou le stockage en ligne OneDrive (même si les accès sont sécurisés et spécifiques à la Caisse de Pensions) qui est hébergé sur les serveurs de l'employeur, ainsi que différents outils (logiciel comptable, logiciel de paiement). Est-ce que cela pourrait poser problème? Que faudrait-il entreprendre pour respecter la nLPD le cas échéant?	L'employeur et sa caisse de pension sont des entités tout à fait separées. Dans son jugement prononcé le 10 avril 2012 (A-4467/2011), le Tribunal administratif fédéral a précisé que le traitement et la publication de données personnelles relevait de la loi fédérale sur la protection des données (LPD, complétée par les normes légales spéciales de la LPP et du CO), et que l'IP ne pouvait transmettre à l'employeur que les données personnelles objectivement nécessaires pour remplir les tâches prévues dans le contrat de travail et dans le cadre de la prévoyance professionnelle. Selon le Tribunal administratif fédéral, la remise des certificats de prévoyance aux employeurs dans des enveloppes non fermées afin que ces derniers les transmettent aux salariés assurés chez eux viole le principe de la sécurité des données (art. 7 LPD). Ceci sera bien sûr aussi valable sous la nouvelle loi sur la protection des données. A cause de cela la Caisse de Pension, qui est responsable selon la loi sur la protection des données en vigueur et la nouvelle loi sur la protection des données, doit veiller à ce que l'employeur n'ait pas accès aux données personnelles des assurés et des retraités. Concernant la nLPD la caisse de pension devrait négocier un contrat de traitement des commandes («Data Processing Agreement») avec le fournisseur de cloud de l'employeur qui garantit que les services informatiques de l'employeur sont totalement imperméables pour l'employeur en ce qui concerne les données personnelles des assurés et des retraités. Parce que les accès sont sécurisés et spécifiques à la Caisse de Pensions, la loi sur la protection des données (en vigueur et nouvelle) semble respectée. Ce qui est important est que le logiciel comptable et le logiciel de paiement sont aussi imperméables pour l'employeur. Mais tout cela devrait être prévu dans le contrat (au moins dans une clause contractuelle).

Können externe Partner grundsätzlich als Datenverarbeiter von der Unterstellung unter das revDSG ausgeschlossen werden, wenn diese ausschliesslich nur noch mit anonymen Daten arbeiten? (IT-Provider, Experten, Revisoren, ...)	Ja, wobei die Experten und Revisoren – im Unterschied zu den IT-Providern – als Verantwortliche gelten. Eine Anonymisierung von Personendaten hat datenschutzrechtlich dieselbe Wirkung wie eine Löschung derselben; denn wenn das Datenschutzrecht für anonyme Daten nicht gilt, kann auch nicht ihre Löschung verlangt werden. Somit fallen anonymisierte Personendaten als anonyme Daten nicht unter das «Recht auf Vergessen».
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».
Sind für den PK-experten und die Revisionsstelle ein Auftragsbearbeitungsverträge zu erstellen?	Die Vorsorgeeinrichtung hat für den PK-Experten und die Revisionsstelle keine Auftragsbearbeitungsverträge («Data Processing Agreement» bzw. «Controller to Processor Agreement») abzuschliessen, da es sich bei beiden um Verantwortliche (d.h. nicht Auftragsbearbeiter) gemäss revDSG handelt. Die Vorsorgeeinrichtung hat mit diesen vielmehr sog. «Controller to Controller Agreements» zur Abgrenzung der Verantwortlichkeiten gemäss revDSG zu vereinbaren. Dies schliesst jedoch nicht aus, dass der PK-Experte für die Vorsorgeeinrichtung bestimmte Tätigkeiten ausübt, bei welchen sie bzw. er aus datenschutzrechtlicher Sicht die Rolle des Auftragsbearbeitenden einnimmt. An diese Rolle ist z.B. zu denken, wenn die Vorsorgeeinrichtung hinsichtlich der Datenverwendung eine Weisungsbefugnis innehat und darüber entscheidet, welche Personendaten der PK-Experte zu welchem Zweck zur Verfügung gestellt werden.

Faut-il établir un contrat de mandat pour l'expert de la CP et l'organe de révision?	L'institution de prévoyance ne doit pas conclure de contrat de traitement des données («Data Processing Agreement» ou «Controller to Processor Agreement») pour l'expert CP et l'organe de révision, étant donné qu'ils sont tous deux responsables (c.-à-d. qu'ils ne traitent pas les données sur mandat) selon la nLPD. L'institution de prévoyance doit plutôt convenir avec eux de ce que l'on appelle des «Controller to Controller Agreements» pour délimiter les responsabilités selon la nLPD. Cela n'exclut toutefois pas que l'expert de la CP exerce pour l'institution de prévoyance certaines activités pour lesquelles elle ou il joue le rôle de sous-traitant du point de vue de la protection des données. On peut penser à ce rôle par exemple lorsque l'institution de prévoyance dispose d'un pouvoir d'instruction concernant l'utilisation des données et décide quelles données personnelles sont mises à la disposition de l'expert de la CP et dans quel but.
UNTERSTELLUNG DER KANTONALEN ÖFFENTL.-RECHTL. VORSORGEEINRICHTUNGEN UNTER DAS REVDSG? ASSUJETTISSEMENT DES INSTITUTIONS DE PRÉVOYANCE CANTONALES DE DROIT PUBLIC À LA nLPD?	
1. Was muss eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung betreffend revDSG unternehmen? 2. Untersteht eine öffentlich-rechtliche Vorsorgeeinrichtung nach der Verselbständigung dem kantonalen DSG?	1./2. Es kann in verschiedenen Rechtsbereichen zu Abgrenzungsschwierigkeiten zwischen Datenschutzvorschriften des Bundes und der Kantone kommen. Insbesondere stellen sich diese Fragen z.B. dann, wenn kantonale Behörden Bundesrecht vollziehen. Für die kantonalen öffentlich-rechtlichen Vorsorgeeinrichtungen besteht im Hinblick auf das Inkrafttreten des totalrevidierten Datenschutzgesetzes des Bundes kein zwingender Handlungsbedarf; insbesondere sind sie nicht verpflichtet, einen Datenschutzberater zu ernennen.
3. Muss eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung einen Datenschutzberater gemäss revDSG ernennen? 4. Würden Sie öffentlich-rechtlichen Vorsorgeeinrichtungen trotzdem anraten – im	3./4. Allerdings können Konstellationen vorkommen, in denen Datenschutzvorschriften aus der Gesetzgebung des Bundes z.B. im Bereich der beruflichen Vorsorge oder aus weiteren Sozialversicherungszweigen auf Datenbearbeitungen Anwendung finden, welche eine kantonale öffentlich-rechtliche Vorsorgeeinrichtung vornimmt. Es ist im Grundsatz aber so, dass eine öffentlich-rechtliche Vorsorgeeinrichtung als öffentliches Organ des Kantons dem kantonalen DSG untersteht. Es handelt sich bei einer kantonalen öffentlich-rechtlichen Vorsorgeeinrichtung weder um ein Bundesorgan noch um eine private Person gemäss revDSG, weshalb sie prinzipiell nicht in den Geltungsbereich der Datenschutzgesetzgebung des Bundes fällt. Punktuell kann es jedoch Ausnahmen geben. Angesichts ihrer Aufgaben, die regelmässig das Bearbeiten von besonders schützenswerten Personendaten beinhalten, ist es trotzdem geboten, dass die kantonalen öffentlich-rechtlichen Vorsorgeeinrichtungen die Compliance im Bereich Datenschutz sicherstellen.

Sinne des Vorsichtsprinzips – die grundsätzlichen Bestimmungen und Vorgaben (z.B. Erstellung Bearbeitungsverzeichnis) des revDSG für registrierte Pensionskassen zu implementieren? Oder war wäre Ihre Empfehlung für das weitere Vorgehen für öffentlich-rechtliche Pensionskassen?	
1. Que doit faire une institution de prévoyance cantonale de droit public concernant la nLPD? 2. Une institution de prévoyance de droit public est-elle soumise à la LPD cantonale après son autonomisation?	1./2. Dans différents domaines juridiques, des problèmes de délimitation entre les dispositions de protection des données de la Confédération et celles des cantons peuvent se produire. Ces questions se posent notamment lorsque des autorités cantonales appliquent le droit fédéral. Les institutions de prévoyance cantonales de droit public ne sont pas tenues de prendre des mesures urgentes et contraignantes en vue de l'entrée en vigueur de la loi fédérale sur la protection des données totalement révisée; elles ne sont notamment pas obligées de désigner un conseiller à la protection des données.
3. Une institution de prévoyance cantonale de droit public doit-elle désigner un conseiller à la protection	3./4. Mais il peut arriver que des prescriptions de protection des données issues de la législation fédérale, p. ex. dans le domaine de la prévoyance professionnelle ou d'autres branches des assurances sociales, s'appliquent à des traitements de données effectués par une institution de prévoyance cantonale de droit public. En principe, une institution de prévoyance de droit public est soumise à la LPD cantonale en tant qu'organe public du canton. Une institution de prévoyance cantonale de droit public n'est ni un organe fédéral ni une personne privée au sens de la nLPD, raison pour la-

des données conformément à la nLPD? 4. Conseilleriez-vous malgré tout aux institutions de prévoyance de droit public – en vertu du principe de précaution – de mettre en œuvre les dispositions et prescriptions fondamentales de la nLPD pour les caisses de pension enregistrées (p. ex. création d'un registre des activités de traitement)? Ou quelle serait votre recommandation concernant la suite de la procédure pour les caisses de pension de droit public?	quelle elle ne tombe en principe pas dans le champ d'application de la législation fédérale sur la protection des données. Il peut toutefois y avoir des exceptions ponctuelles. Compte tenu de leurs tâches, qui impliquent régulièrement le traitement de données personnelles sensibles, il est néanmoins nécessaire qu'elles soient en conformité avec la législation sur la protection des données.
BEKANNTGABE VON PERSONENDATEN INS AUSLAND COMMUNICATION DE DONNÉES PERSONNELLES À L'ÉTRANGER	
Was ist unter der «Gewährleistung eines angemessenen Schutzes durch die Gesetzgebung des betreffenden Staates oder das	Es bedeutet, dass Personendaten ins Ausland nur dann bekannt gegeben werden dürfen, wenn der betreffende Staat einen angemessenen Datenschutz gewährleistet. Falls sich der Staat nicht auf der Liste befindet, muss ein geeigneter Datenschutz anders gewährleistet werden, beispielsweise mittels der Verwendung von Standardvertragsklauseln (Art. 9-12 revDSV). Siehe zu dieser Thematik die Ausführungen des EDÖB zu Datenübermittlungen ins Ausland: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-741117193: «Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf an-

internationale Organ» (Art. 16 Abs. 1 revDSG/Art. 8 revDSV) zu verstehen?	erkannte Standardvertragsklauseln und Musterverträge» vom 27. August 2021. Sowohl registrierte als auch nicht-registrierte Pensionskassen müssen überprüfen, ob Datentransfers ins Ausland stattfinden und – falls dies der Fall ist – ob die Grundsätze von Art. 16 revDSG eingehalten werden oder die Datenbekanntgabe ins Ausland allenfalls gestützt auf eine Ausnahme nach Art. 17 revDSG erfolgen darf. Dabei dürfen Personendaten ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 revDSG). Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch: a. einen völkerrechtlichen Vertrag; b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden; c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat; d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden (Art. 16 Abs. 2 revDSG). Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen (Art. 16 Abs. 3 revDSG). Ausnahmen in Art. 17 revDSG.
Que faut-il entendre par «que l'État concerné dis-pose d'une législation as-surant un niveau de protection adéquat ou que l'organisme international garantisse un niveau de protection adéquat» (art. 16, al. 1, nLPD / art. 8 nOPDo)?	Cela signifie que les données personnelles ne peuvent être communiquées à l'étranger que si l'État concerné garantit une protection adéquate de ces données. Si l'État ne figure pas sur la liste, une protection des données appropriée doit être garantie d'une autre manière, p. ex. par l'utilisation de clauses contractuelles standard (art. 9-12 nOPDo). Voir à ce sujet les explications du PFPDT sur les transmissions de données à l'étranger: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html «Transfert de données personnelles vers un pays ne présentant pas un niveau de protection des données adéquat en application de clauses contractuelles types et de contrats types reconnus» du 27 août 2021. Les caisses de pension, qu'elles soient enregistrées ou non, doivent vérifier si des transferts de données ont lieu à l'étranger et – dans l'affirmatif – si les principes de l'art. 16 nLPD sont respectés ou si la communication de données à l'étranger peut éventuellement avoir lieu sur la base d'une exception selon l'art. 17 nLPD. Dans ce contexte, des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que la législation de l'État concerné ou un organisme international garantit une protection adéquate (art. 16, al. 1, nLPD). En l'absence d'une décision du Conseil fédéral selon l'al. 1, des données personnelles peuvent être communiquées à l'étranger si une protection appropriée est garantie par: a) un traité international; b) les clauses d'un contrat conclu avec le responsable ou le sous-traitant et son cocontractant, clauses qui auront été préalablement communiquées au PFPDT; c) des garanties spécifiques élaborées par l'organe fédéral compétent et communiquées préalablement au PFPDT; d) des clauses standard de protection des données que le PFPDT a préalablement approuvées, délivrées ou reconnues; ou e) des prescriptions con-

	traignantes internes à l'entreprise en matière de protection des données ayant été préalablement approuvées par le PFPDT ou par l'instance d'un État chargée de la protection des données et assurant un niveau de protection adéquat (art. 16, al. 2, nLPD). Le Conseil fédéral peut prévoir d'autres garanties appropriées au sens de l'al. 2 (art. 16, al. 3, nLPD). Exceptions à l'art. 17 nLPD.
Wenn Daten in der Cloud gespeichert werden, ist nicht klar, wo diese Daten genau liegen. Ist das dann ein Datentransfer ins Ausland?	Der Cloud-Provider (bei der Speicherung von Daten auf der vom IT-Provider betriebenen Cloud) gilt lediglich als Auftragsbearbeiter gemäss revDSG, die Vorsorgeeinrichtung jedoch ist Verantwortliche. Sie hat sämtliche verwaltungs- und IT-technischen Abläufe vertraglich zu regeln (Auftragsbearbeitungsvertrag oder « Data Processing Agreement»). Es muss die ganze Kette von der Vorsorgeeinrichtung über den/die Software-Anbieter und Cloud-Provider vertraglich abgesichert sein. Im Weiteren darf der Auftragsbearbeiter die Bearbeitung nur mit vorgängiger Genehmigung der Vorsorgeeinrichtung einem Dritten übertragen. Wer beispielsweise Personendaten aus der Schweiz seiner eigenen Zweigniederlassung im Ausland zugänglich macht, muss sich an Art. 16f. revDSG und Art. 8-12 revDSV halten. Dies analog auch, wenn eine Vorsorgeeinrichtung Personendaten ihrem sich im Ausland befindenden Cloud-Provider zukommen lässt. Die Vorsorgeeinrichtung hat den betroffenen Personen, d.h. den Versicherten und Rentnern/Rentnerinnen den Staat, in welchem sich der Cloud-Provider befindet, in der Datenschutzerklärung mitzuteilen (Art. 19 Abs. 4 revDSG). *Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 66.*
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. 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)
a) Handelt es sich beim Versand eines Versicherungsausweises an eine im Ausland wohnhafte versicherte Person um einen Datentransfer ins Ausland gemäss Definition revDSG?	a) Nein. Unter «Bekanntgeben» ist das «Übermitteln oder Zugänglichmachen von Personendaten» (Art. 5 lit. e revDSG) zu verstehen. Das «Bekanntgeben» erfordert begriffslogisch, dass der Kreis der Personen, die über die betreffende Information verfügen, erweitert wird. *Siehe David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 66.*
b) Handelt es sich bei der Benützung eines Mitgliederportals durch eine im Ausland wohnhafte versicherte Person um einen Datentransfer ins Ausland gemäss Definition revDSG?	b) Nein. Es gilt Antwort unter a). Anders verhält es sich, wenn eine Vorsorgeeinrichtung Personendaten ihrem sich im Ausland befindenden Cloud-Provider zukommen lässt (Art. 16f. revDSG; Art. 8-12 revDSV). Die Vorsorgeeinrichtung hat den betroffenen Personen, d.h. den Versicherten und Rentnern/Rentnerinnen den Staat, in welchem sich der Cloud-Provider befindet, in der Datenschutzerklärung mitzuteilen (Art. 19 Abs. 4 revDSG). *Siehe David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019, Rz. 66.*
a) L'envoi d'un certificat d'assurance à une personne assurée domiciliée à l'étranger constitue-t-il un transfert de données à l'étranger selon la définition de la nLPD?	a) Non. Par «communiquer», il faut entendre «transmettre ou rendre accessibles des données personnelles» (art. 5, let. e, LPD révisée). D'un point de vue conceptuel, la «communication» exige que le cercle des personnes disposant de l'information en question soit élargi. *Voir David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16 novembre 2020, n. 66.*
b) L'utilisation d'un portail de membres par une personne assurée domiciliée à	b) Non. La réponse sous a) s'applique. Il en va différemment lorsqu'une institution de prévoyance transmet des données personnelles à son fournisseur de services informatiques en nuage situé à l'étranger (art. 16 s. nLPD; art. 8 à 12 nOPDo). L'institution de prévoyance doit indiquer aux personnes concernées, c'est-à-dire aux assurés et aux rentiers/rentières, l'Etat dans lequel se trouve le fournisseur de services informatiques en nuage dans la déclaration de pro-

l'étranger constitue-t-elle un transfert de données vers l'étranger selon la définition de la nLPD?	tection des données (art. 19, al. 4, nLPD). *Voir David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, dans: Jusletter 17 juin 2019, n. 66.*
Kommunikation im Ausland, wie sieht es in England aus?	Bei der Übermittlung der Daten ins Ausland hat die VE einen angemessenen Schutz dieser Daten sicherzustellen. Dabei bedeutet die «Gewährleistung eines angemessenen Schutzes durch die Gesetzgebung des betreffenden Staates oder das internationale Organ» (Art. 16 Abs. 1 revDSG/Art. 8 revDSV), dass Personendaten ins Ausland nur dann bekannt gegeben werden dürfen, wenn der betreffende Staat einen angemessenen Datenschutz gewährleistet. Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz werden in Anhang 1 der revDSV aufgeführt (Art. 8 Abs. 1 revDSV). Die Angemessenheit des Datenschutzes wird periodisch neu beurteilt (Art. 8 Abs. 4 revDSV). Die Beurteilungen werden veröffentlicht (Art. 8 Abs. 5 revDSV). Wenn die Beurteilung nach Art. 8 Abs. 4 revDSV oder andere Informationen zeigen, dass kein angemessener Datenschutz mehr gewährleistet ist, wird Anhang 1 geändert; dies hat keine Auswirkungen auf die bereits erfolgten Datenbekanntgaben (Art. 8 Abs. 6 revDSV). Bei Drittländern ohne gleichwertiges Datenschutzniveau hat die VE zusätzliche Abklärungen/Absicherungen vorzunehmen. Falls sich der Staat nicht auf der Länderliste gemäss Anhang 1 revDSV befindet, muss ein geeigneter Datenschutz anders gewährleistet werden, beispielsweise mittels der Verwendung von Standardvertragsklauseln (Art. 9-12 revDSV). England befindet sich im Anhang 1 der revDSV unter den «Staaten, Gebieten, spezifischen Sektoren in einem Staat und internationalen Organen mit einem angemessenen Datenschutz» (39 Vereinigtes Königreich**; 15 Gibraltar**; 17 Guernsey**; 19 Isle of Man**; 25 Jersey***). Bei der Beurteilung, ob ein Staat, ein Gebiet, ein spezifischer Sektor in einem Staat oder ein internationales Organ einen angemessenen Datenschutz gewährleistet, werden u.a. die internationalen Verpflichtungen des Staates oder internationalen Organs, hier also des Vereinigten Königreichs und seiner weiteren Gebiete (Gibraltar, Guernsey, Isle of Man, Jersey), insbesondere im Bereich des Datenschutzes berücksichtigt (Art. 8 Abs. 2 lit. a revDSV). Da das Vereinigte Königreich nicht mehr Mitglied der Europäischen Union (EU) ist, stützt sich der Bundesrat betreffend das Datenschutzniveau des Vereinigten Königreichs in der revDSV auf den Angemessenheitsbeschluss der Europäischen Kommission («EU-Kommission») gemäss Art. 45 Abs. 3 DSGVO vom 28. Juni 2021 (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de) ab. Der Angemessenheitsbeschluss hat eine Verfallsklausel, durch die seine Geltungsdauer auf vier Jahre beschränkt ist, in denen die EU-Kommission die Rechtslage und mögliche Abweichungen hinsichtlich des Datenschutzniveaus beobachten will (https://www.taylorwessing.com/de/insights-and-events/insights/2021/12/datenschutz-im-vereinigten-koenigreich).

	Mit Ausnahme von Jersey wird der Datenschutz des Vereinigten Königreichs durch die EU-Kommission als mit der EU-DSGVO gleichwertig und somit angemessen anerkannt (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de). Auf diese Anerkennung baut der Bundesrat auf: Der Datenschutz des Vereinigten Königreichs inkl. Gibraltar, Guernsey, Isle of Man und Jersey wird als mit dem revDSG gleichwertig und somit angemessen anerkannt.
Communication à l'étranger, qu'en est-il en Angleterre?	Lors de la transmission des données à l'étranger, l'IP doit garantir une protection adéquate de ces données. A cet égard, la «garantie d'une protection adéquate par la législation de l'Etat concerné ou par l'organe international» (art. 16, al. 1, nLPD/art. 8 nOPDo) signifie que les données personnelles ne peuvent être communiquées à l'étranger que si l'Etat concerné garantit une protection adéquate des données. Les Etats, territoires, secteurs spécifiques dans un Etat et organes internationaux offrant une protection adéquate des données sont énumérés à l'annexe 1 de l'OCRPD (art. 8, al. 1, nOPDo). Le caractère adéquat de la protection des données est réévalué périodiquement (art. 8, al. 4, nOPDo). Les évaluations sont publiées (art. 8, al. 5, nOPDo). Si l'évaluation selon l'art. 8, al. 4, nOPDo ou d'autres informations montrent que la protection adéquate des données n'est plus garantie, l'annexe 1 est modifiée; cela n'a aucune incidence sur les communications de données déjà effectuées (art. 8, al. 6, nOPDo). Pour les pays tiers ne disposant pas d'un niveau de protection des données équivalent, l'IP doit procéder à des clarifications/assurances supplémentaires. Si l'Etat ne figure pas sur la liste des pays selon l'annexe 1 de la nOPDo, une protection des données appropriée doit être garantie d'une autre manière, par exemple par l'utilisation de clauses contractuelles standard (art. 9-12 nOPDo). L'Angleterre figure à l'annexe 1 de la la nOPDo parmi les «États, territoires, secteurs spécifiques dans un État et organes internationaux assurant une protection adéquate des données» (39 Royaume-Uni**; 15 Gibraltar**; 17 Guernesey**; 19 Île de Man**; 25 Jersey***). Pour déterminer si un État, un territoire, un secteur spécifique d'un État ou une institution internationale assure une protection adéquate des données, il est tenu compte, entre autres, des obligations internationales de l'État ou de l'institution internationale, en l'occurrence le Royaume-Uni et ses autres territoires (Gibraltar, Guernesey, l'Île de Man, Jersey), notamment en matière de protection des données (art. 8, al. 2, let. a, nOPDo). Etant donné que le Royaume-Uni n'est plus membre de l'Union européenne (UE), le Conseil fédéral se base, en ce qui concerne le niveau de protection des données du Royaume-Uni dans la la nOPDo, sur la décision d'adéquation de la Commission européenne («Commission UE») selon l'art. 45, al. 3 RGPD du 28 juin 2021 (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fr). La décision d'adéquation est assortie d'une clause de caducité qui limite sa durée de validité à quatre ans, période pendant laquelle la Commission européenne entend surveiller la situation juridique et les éventuelles divergences concernant le niveau de protection des données (https://www.taylorwessing.com/de/insights-and-events/insights/2021/12/datenschutz-im-vereinigten-koenigreich).

	L'exception de Jersey, la protection des données du Royaume-Uni est reconnue par la Commission européenne comme équivalente au RGPD et donc adéquate (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fr). Le Conseil fédéral se base sur cette reconnaissance: La protection des données du Royaume-Uni, y compris Gibraltar, Guernesey, l'île de Man et Jersey, est reconnue comme équivalente à la loi révisée sur la protection des données et donc adéquate.
ABGRENZUNG REVDSG/INFORMATIONSSICHERHEITSGESETZ (ISG) DÉLIMITATION ENTRE LA nLPD ET LA LOI SUR LA SÉCURITÉ DE L'INFORMATION (LSI)	
Neu werden die Vorsorgeeinrichtungen als Bundesorgan eingestuft. Hat dies neben den höheren Anforderungen im DSG auch noch weitere Auswirkungen (z.B. Unterstellung ISG) falls ja, welche?	Die ISG-Revision hat keine direkten Auswirkungen auf das geltende DSG und das revDSG. Der ASIP befürwortete – angesichts der Tatsache, dass Cyberrisiken schon seit etlichen Jahren auch für Pensionskassen und deren Versicherte bzw. Rentnerinnen und Rentner ein grosses Risiko darstellen – in seiner Vernehmlassung vom 14.04.2022 grundsätzlich das neue ISG. Wir begrüssten dabei die im Erläuterungsbericht, S. 18f., erwähnte Möglichkeit der Einschränkung der Meldepflicht aller registrierten und nicht registrierten Vorsorge- und Freizügigkeitseinrichtungen gemäss Art. 74a i.V.m. Art. 74b lit. j E-ISG.[5]
Les institutions de prévoyance sont désormais considérées comme des organes fédéraux. Outre les exigences plus élevées stipulées dans la LPD, cela aura-t-il d'autres conséquences (p. ex. assujettissement à la	La révision de la LSI n'a pas de conséquences directes sur la LPD en vigueur et la nLPD. Dans sa consultation du 14 avril 2022, l'ASIP s'est en principe prononcée en faveur de la nouvelle LSI, étant donné que les cyber-risques représentent depuis plusieurs années déjà un danger important pour les caisses de pension et leurs as-surés ou retraités. Nous avons salué à cet égard la possibilité, mentionnée dans le rapport explicatif, p. 18s., de limiter l'obligation d'annonce pour toutes les institutions de prévoyance, enregistrées ou non, et des institutions de libre passage conformément à l'art. 74a en relation avec l'art. 74b let. j pLSI.[3]

[5] https://www.inter-pension.ch/uploads/1/1/8/3/118397790/informationssicherheitsgesetz.pdf; https://www.inter-pension.ch/uploads/1/1/8/3/118397790/erlaeuternder_bericht.pdf.

[5] https://www.fedlex.admin.ch/fr/consultation-procedures/ended/2022: DFF, Obligation de signaler les cyberattaques contre les infrastructures critiques.

LSI)? Si oui, lesquelles?	