Pflicht für einen Datenschutzberater

Beraten und unterstützen

Die Revision des Bundesgesetzes über den Datenschutz (DSG) verlangt, dass Pensionskassen eine Datenschutzberaterin bzw. einen Datenschutzberater ernennen. Dies gilt auch für betriebliche Pensionskassen, die die Geschäftsführung usw. ausgelagert haben.

Ursula Uttinger
lic. iur./exec MBA,
Inhaberin von Uttinger-Datenschutz

Am 1. September 2023 ist das revidierte Datenschutzgesetz in Kraft getreten.[1] So viel, wie man im Vorfeld aufgrund der vielen Publikationen dazu hätte meinen können, hat sich nicht geändert. Einige Punkte sind aber gerade für Pensionskassen neu: Pensionskassen brauchen eine Datenschutzberaterin oder einen Datenschutzberater, da sie unter die Regelungen für Bundesorgane fallen.

Pensionskasse – ein Bundesorgan

Es gibt zwar kein Bundesgerichtsurteil, doch das Bundesverwaltungsgericht hat im Entscheid A–4467/2011 vom 10. April 2012[2] betreffend Zustellung von Pensionskassenausweisen festgehalten, dass die berufliche Vorsorge eine Bundesaufgabe nach Art. 113 BV und folglich dem öffentlichen Recht zuzuordnen ist (E 4.2). Folglich sind die datenschutzrechtlichen Bestimmungen für Bundesorgane anwendbar. Dies hat zur Folge, dass eine Datenschutzberaterin zu ernennen ist: Im Gegensatz zu privaten Personen müssen Bundesorgane diese Funktion einführen (Art. 10 Abs. 5 DSG i.V.m. Art. 25 DSV).

Dies mag für grössere Bundesorgane sinnvoll und im Alltag hilfreich sein. Diese Vorgaben gelten aber auch für kleinste Einheiten – also auch für betriebliche Pensionskassen, die primär aus einem Stiftungsrat bestehen und alle Aufgaben inklusive Geschäftsführung/Pensionskassenleitung Dritten übertragen. Eine Diskussion über Sinn oder Unsinn erübrigt sich, der Gesetzgeber hat es so vorgesehen.

Unabhängigkeit der Funktion

Da der Stiftungsrat im Sinne von Art. 5 Bst. j verantwortlich ist, muss er einen Datenschutzberater ernennen und darauf achten, dass diese Person über die erforderlichen Fachkenntnisse verfügt und das Amt unabhängig und weisungsungebunden ausüben kann (Art. 26 Abs. 1 DSV). Wird also die Geschäftsführung von einer auf die Vorsorge spezialisierten Organisation übernommen, kann die Funktion Datenschutzberater nicht gleichzeitig von derselben Organisation übernommen werden. Ein Interessenkonflikt wäre vorprogrammiert, die geforderte Unabhängigkeit wäre nicht gegeben. Es liegt also auf der Hand, dass die Funktion Datenschutzberater von einem externen Datenschutzspezialisten übernommen wird. Seine Kontaktdaten müssen im Internet und gegenüber dem EDÖB publiziert werden (Art. 27 Abs. 2 DSV).

Die Funktion Datenschutzberaterin/Datenschutzberater ist, wie der Name bereits zeigt, vor allem beratend und unterstützend tätig und nicht überwachend.[3] Gemäss Verordnung ist die Mitwirkung bei der Anwendung der Datenschutzvorschriften (Art. 26 Abs. 1 Bst. a DSV) und Schulung/Beratung (Art. 26 Abs. 1 Bst. c DSV) gefordert. Zudem soll diese Funktion als Anlaufstelle für betroffene Personen dienen (Art. 26 Abs. 2 Bst. b DSV).

Die Datenschutzberaterin arbeitet im Alltag primär mit den vom Stiftungsrat der Pensionskasse beauftragten Organisationen, die operativ tätig sind. Diese mussten einzelne datenschutzrechtliche Hausaufgaben bereits erfüllen, gelten sie

[1] Mehr dazu siehe Akzentteil in der Februarausgabe 2023.
[2] bit.ly/3RPRp31
[3] Vgl. Ursula Uttinger, Thomas Geiser, Das neue Datenschutzrecht, RZ 2.41, Basel 2013.

doch in der Zusammenarbeit mit der Pensionskasse als Auftragsdatenbearbeiter und müssen gegenüber dem Auftraggeber, also dem Stiftungsrat, nachweisen, dass sie die Datensicherheit gewährleisten können. Dies dürfte mittels einer Auftragsdatenvereinbarung (ADV) vertraglich festgehalten sein.[4]

Wichtigste Aufgaben

Der Datenschutzberater sollte den Stiftungsrat sowie die beauftragte Organisation in folgenden Punkten beraten und begleiten:

- Einhalten der Datenschutzgrundsätze (Art. 6 und 8 DSG) bei der Bearbeitung von Personendaten. Dabei ist vor allem auf die Verhältnismässigkeit und die Aufbewahrungsdauer zu achten.
- Überprüfung und Beratung bezüglich Auftragsnehmer und ADV bzw. Geheimhaltungsvereinbarungen: Bearbeiten Dritte Daten (PK-Administration, PK-Geschäftsführung, IT), braucht es eine ADV. Haben Dritte jedoch einzig potenziell Zugang zu Daten, wie ein Reinigungsunternehmen, genügt eine Geheimhaltungsvereinbarung.
- Erstellen eines Verzeichnisses der Bearbeitungstätigkeiten und Meldung desselben beim EDÖB (Art. 12 DSG). Auch wenn gerade bei solchen betrieblichen Pensionskassen keine 250 Personen angestellt sind, ist doch das Risiko einer Verletzung der Persönlichkeit nicht nur gering (Art. 12 Abs. 5 DSG).
- Information der betroffenen Personen: Dies können sowohl aktive Mitarbeitende als auch bereits Pensionierte sein. Diese müssen über eine Datenbeschaffung informiert werden. Besitzt die Pensionskasse eine eigene Internetseite, kann die Information auch mittels Datenschutzerklärung erfolgen.[5]
- Gibt es eine neue Bearbeitung von Personendaten (Art. 22 DSG) oder wird der Zweck der bestehenden Datenbearbeitung verändert und neue Daten beschafft (Übergangsbestimmung: Art. 69 DSG), ist eine Datenschutz-Folgenabschätzung (DSFA) zu erstellen und die Datenschutzberaterin / der Datenschutzberater soll dabei beraten und deren Ausführung überprüfen (Art. 26 Abs. 2 Bst. a Ziff. 2 DSV).[6]
- Kommt es zu einer Verletzung der Datensicherheit, ist die Datenschutzberaterin / der Datenschutzberater zu informieren (Art. 27 Abs. 2 Bst. b DSV).
- Auch im Zusammenhang mit den Rechten betroffener Personen (Art. 25 ff. DSG) wirkt die Datenschutzberaterin / der Datenschutzberater sinnvollerweise mit – gerade, weil der Stiftungsrat strategisch unterwegs sein sollte.
- Unterstützung bei der Erstellung eines Bearbeitungsreglements (Art. 6 DSV).

Auf den ersten Blick sind dies viele Aufgaben – ein Initialaufwand besteht sicherlich. Doch mittelfristig dürfte der Aufwand abnehmen, sofern es nicht zu einer Datensicherheitsverletzung kommt. Eine solche kann plötzlich viele Ressourcen beanspruchen, wie verschiedene Beispiele von Datenleaks bei Bundesämtern und Kantonen zeigen.[7] Allerdings dürfte der Lead kaum bei der Datenschutzberaterin / beim Datenschutzberater liegen.

Zu den jährlichen Aufgaben gehören ein Jahresbericht zuhanden des Stiftungsrats, (mindestens) ein Meeting mit dem Stiftungsrat und dazwischen Kontakt mit der Geschäftsführung und natürlich die Beantwortung von Anfragen. Diese dürften sich – erfahrungsgemäss – in Grenzen halten.

Zusammengefasst: Die Revision DSG ist eine Weiterentwicklung, stärkt die Rechte der Betroffenen und verlangt von Verantwortlichen einige organisatorische Anpassungen. Mit einer erfahrenen Datenschutzberaterin, wobei Branchenwissen zwingend ist, können die Vorgaben vernünftig erfüllt werden. ▮

TAKE AWAYS

- Pensionskassen brauchen einen Datenschutzberater.
- Abgesehen vom Initialaufwand dürfte sich der Aufwand in Grenzen halten.
- Die beauftragte Geschäftsstelle kann nicht gleichzeitig die Funktion Datenschutzberater übernehmen.
- Das Gesetz und die Verordnung haben die Aufgaben klar umschrieben.

Kurzer Erfahrungsbericht

Im Verlaufe des letzten Jahrs erhielt ich einige Anfragen, ob ich die Funktion Datenschutzberaterin für eine betriebliche Pensionskasse übernehmen würde. Wichtig ist bei der Übernahme eines solchen Mandats ein gutes Vertrauensverhältnis mit der Organisation, die die Geschäftsführung innehat. Wenn man nicht regelmässig in der Organisation ist, besteht eine grosse Abhängigkeit, und man muss darauf vertrauen können, dass man bei einem Vorfall tatsächlich involviert wird.

Gleichzeitig sollte man die Funktion mit Augenmass ausführen: Eine überbordende Bürokratie ist nicht notwendig, um den Datenschutz einzuhalten. Adrian Lobsiger* der EDÖB meinte anlässlich einer Tagung: «Mit der Bereitschaft, sich gedanklich in die Haut der Kundinnen und Kunden zu versetzen, und mit einer Prise gesundem Menschenverstand kann jedes Unternehmen mit dem knapp gehaltenen Text von Gesetz und Verordnung vertretbare Lösungen finden.» Nicht zu vergessen ist, dass Datenschutz ein Menschenrecht** und nicht nur eine Frage von Compliance ist.

* bit.ly/3NUXGZM (6.1.2024)
** bit.ly/3Sa63TW (6.1.2024)

[4] Für ADV gibt es diverse sehr gute Vorlagen, die von verschiedenen Schweizer Fachverbänden erstellt wurden, die auf die eigenen Bedürfnisse anzupassen sind. Man darf sich grundsätzlich auch an Vorlagen, die für die europäische Datenschutz-Grundverordnung (DSGVO) erstellt wurden, orientieren. Die Gesetzesartikel sind unbedingt anzupassen.

[5] BBl 2017 7050.

[6] Auch im Zusammenhang mit der DSFA gibt es inzwischen vor allem von kantonalen Datenschutzbehörden Vorlagen, die leider nicht einheitlich sind. Eine gute Vorlage, die aber noch anzupassen ist, findet man beim Kanton Luzern.

[7] Div. Kantone und Bundesämter XPlain (bit.ly/3tTzaS5; 6.1.2024), Concevis (bit.ly/3S8S4hf; 6.1.2024).

Obligation pour un conseiller à la protection des données

Conseiller et soutenir

La révision de la loi fédérale sur la protection des données (LPD) exige que les caisses de pensions désignent un conseiller à la protection des données. Cette obligation s'applique également aux caisses de pensions d'entreprise qui ont externalisé la gestion, etc.

La loi révisée sur la protection des données est entrée en vigueur le 1er septembre 2023.[1] Contrairement à ce que l'on aurait pu penser au vu des nombreuses publications à ce sujet, elle n'a pas changé grand-chose. Certains points sont toutefois nouveaux, en particulier pour les caisses de pensions qui ont désormais besoin d'un conseiller à la protection des données, car elles sont soumises aux règles applicables aux organes fédéraux.

La caisse de pensions – un organe fédéral

Bien qu'il n'existe pas de décision du Tribunal fédéral en la matière, le Tribunal administratif fédéral a déclaré dans l'arrêt A-4467/2011 du 10 avril 2012[2] concernant la notification de certificats de caisse de pensions que la prévoyance professionnelle est une tâche fédérale selon l'art. 113 Cst. et qu'elle relève par conséquent du droit public (E 4.2). De ce fait, les dispositions relatives à la protection des données édictées pour les organes fédéraux sont applicables. Il en découle qu'un conseiller à la protection des données doit être désigné: contrairement aux personnes privées, les organes fédéraux doivent introduire cette fonction (art. 10 al. 5 LPD en relation avec l'art. 25 OLPD).

Cela peut être judicieux pour les grands organes fédéraux et utile au quotidien. Mais ces directives sont également valables pour les plus petites unités – donc aussi pour les caisses de pensions d'entreprise qui se composent en premier lieu d'un conseil de fondation et qui confient toutes les tâches, y compris la gestion/direction de la caisse de pensions, à des tiers. Inutile de discuter du sens ou du non-sens de cette disposition, le législateur en a décidé ainsi.

Indépendance de la fonction

Comme le conseil de fondation est responsable au sens de l'art. 5 let. j, il doit nommer un conseiller à la protection des données et veiller à ce que cette personne dispose des connaissances spécialisées nécessaires et puisse exercer sa fonction de manière indépendante et sans recevoir d'instructions (art. 26 al. 1 OLPD). Ainsi, si la gestion est assurée par une organisation spécialisée dans la prévoyance, la fonction de conseiller à la protection des données ne peut pas être assumée simultanément par la même organisation. Un conflit d'intérêts serait inévitable et l'indépendance requise ne serait pas garantie. Il est donc évident que la fonction de conseiller à la protection des données doit être assumée par un spécialiste externe de la protection des données. Ses coordonnées doivent être publiées sur Internet et communiquées au PFPDT (art. 27 al. 2 OLPD).

Comme son nom l'indique, la fonction de conseiller à la protection des données a essentiellement un rôle de conseil et d'assistance et non de surveillance.[3] Selon l'ordonnance, la participation à l'application des dispositions relatives à la protection des données (art. 26 al. 1 let. a OLPD) et la formation/le conseil (art. 26 al. 1 let. c OLPD) sont exigés. En outre, cette fonction doit servir de point de contact pour les personnes concernées (art. 26 al. 2 let. b OLPD).

Au quotidien, le conseiller à la protection des données travaille principalement avec les organisations opérationnelles mandatées par le conseil de fondation de la caisse de pensions. Celles-ci ont déjà dû remplir certains devoirs en matière de protection des données, car elles sont considérées comme des responsables du traitement des données dans le cadre de leur collaboration avec la caisse de pensions et doivent prouver au mandant, c'est-à-dire au conseil de fondation, qu'elles peuvent garantir la sécurité des données. Cela devrait être fixé contractuellement au moyen d'un accord sur le traitement des données de commande (ATD).[4]

Principales tâches

Le conseiller à la protection des données devrait conseiller et accompagner le conseil de fondation ainsi que l'organisation mandatée sur les points suivants:

- Respecter les principes de protection des données (art. 6 et 8 LPD) lors du traitement de données personnelles. Il faut surtout veiller à la proportionnalité et à la durée de conservation.
- Vérification et conseil concernant le mandataire et l'ATD ou les accords de confidentialité: si des tiers traitent des données (administration de la CP, direction de la CP, IT), un ATD est né-

[1] Pour en savoir plus, voir la partie «Accent» dans le numéro de février 2023.

[2] bit.ly/3RPRp31

[3] Cf. Ursula Uttinger, Thomas Geiser, Das neue Datenschutzrecht, chif. marg. 2.41, Bâle 2013.

[4] Pour l'ATD, il existe divers très bons modèles créés par différentes associations professionnelles suisses, qu'il convient d'adapter à ses propres besoins. On peut en principe aussi s'inspirer des modèles créés pour le règlement général européen sur la protection des données (RGPD). Les articles de loi doivent impérativement être adaptés.

cessaire. En revanche, si des tiers n'ont qu'un accès potentiel aux données, comme une entreprise de nettoyage, un accord de confidentialité suffit.

- Établissement d'un registre des activités de traitement et déclaration de celui-ci au PFPDT (art. 12 LPD). Même si ces caisses de pensions d'entreprise n'emploient probablement pas 250 personnes, le risque d'atteinte à la personnalité n'est pas négligeable (art. 12 al. 5 LPD).
- Informer les personnes concernées: il peut s'agir aussi bien de collaborateurs actifs que de personnes déjà à la retraite. Ces personnes doivent être informées de la collecte de données. Si la caisse de pensions possède son propre site Internet, l'information peut également se faire au moyen d'une déclaration de protection des données.[5]
- En cas de nouveau traitement de données personnelles (art. 22 LPD) ou si le but du traitement de données existant est modifié et que de nouvelles données sont collectées (disposition transitoire: art. 69 LPD), une analyse d'impact sur la protection des données (AIPD) doit être effectuée et le conseiller à la protection des données doit conseiller et vérifier l'exécution (art. 26 al. 2 let. a ch. 2 OLPD).[6]
- Si une violation de la sécurité des données se produit, le conseiller à la protection des données doit être informé (art. 27 al. 2 let. b OLPD).
- Il est aussi judicieux de faire intervenir le conseiller à la protection des données dans le contexte des droits des personnes concernées (art. 25 et suivants LPD) – précisément parce que le conseil de fondation devrait avoir une orientation stratégique.
- Soutien lors de l'élaboration d'un règlement de traitement (art. 6 OPD).

A première vue, cela représente beaucoup de tâches – il y a certainement un effort initial à faire. Mais à moyen terme, la charge de travail devrait diminuer, pour autant qu'il n'y ait pas de violation de la sécurité des données. Un tel incident peut soudain mobiliser de nombreuses ressources, comme le montrent différents exemples de fuites de données au sein d'offices fédéraux et de cantons.[7] Il est toutefois peu probable que le chef de file soit le conseiller à la protection des données.

Les tâches annuelles comprennent un rapport annuel à l'attention du conseil de fondation, (au minimum) une réunion avec le conseil de fondation et, entretemps, des contacts avec la direction et, bien sûr, des réponses aux demandes. Ces dernières devraient – par expérience – rester limitées.

En résumé, la révision de la LPD constitue une évolution, renforce les droits des personnes concernées et exige quelques adaptations organisationnelles de la part des responsables. Avec une personne expérimentée en matière de protection des données, sachant que la connaissance de la branche est impérative, il est possible de satisfaire raisonnablement aux exigences. ▮

Ursula Uttinger

TAKE AWAYS

- Les caisses de pensions ont besoin d'un conseiller à la protection des données.
- Mis à part l'effort initial, la charge de travail devrait être limitée.
- Le bureau mandaté ne peut pas assumer en même temps la fonction de conseiller à la protection des données.
- La loi et l'ordonnance ont clairement défini les tâches.

Bref rapport d'expérience

Au cours de l'année dernière, j'ai reçu quelques demandes pour assumer la fonction de conseiller à la protection des données pour une caisse de pensions d'entreprise. Lorsqu'on accepte un tel mandat, il est important d'avoir une bonne relation de confiance avec l'organisation qui assume la gestion de la caisse. Si l'on ne se trouve pas régulièrement dans l'organisation, on est très dépendant du bon vouloir de celle-ci et il faut pouvoir se fier au fait d'être effectivement impliqué en cas d'incident.

En même temps, il convient d'exercer cette fonction avec discernement: une bureaucratie débordante n'est pas nécessaire pour respecter la protection des données. Adrian Lobsiger* le PFPDT a déclaré lors d'une conférence: «En étant prêt à se mettre mentalement dans la peau de ses clients et en faisant preuve d'un peu de bon sens, chaque entreprise peut trouver des solutions acceptables avec le texte concis de la loi et de l'ordonnance.» Il ne faut pas oublier que la protection des données est un «droit de l'homme**» et pas seulement une question de conformité.

* bit.ly/3NUXGZM (6.1.2024)
** bit.ly/3Sa63TW (6.1.2024)

[5] FF 2017 7050.

[6] En ce qui concerne l'AIPD également, il existe désormais des modèles, surtout de la part des autorités cantonales de protection des données, qui ne sont malheureusement pas uniformes. Un bon modèle, qui doit toutefois encore être adapté, est celui du canton de Lucerne.

[7] Divers cantons et offices fédéraux XPlain (bit.ly/3tTzaS5; 6.1.2024), Concevis (bit.ly/3S8S4hf; 6.1.2024).