Florian Müller* / Carmela Wyler-Schmelzer**

Das neue Datenschutzgesetz

Inhaltsverzeichnis

I. Einleitung

Das Konzept, dass Personendaten geschützt werden müssen, ist nicht neu. Seine Grundlage liegt im Persönlichkeitsrecht (Art. 28 ff. ZGB). Das erste Datenschutzgesetz (DSG) der Schweiz wurde 1993 publiziert. Der Datenschutz und insbesondere die damit verbundenen Pflichten für Unternehmen gewinnen immer mehr an

* MLaw Rechtsanwalt und Notar, Senior Associate, LEXcellence AG.
** lic.iur. Rechtsanwältin, Senior Legal Consultant, WTW Towers Watson AG.

Bedeutung. Dabei muss der Datenschutz nicht nur innerhalb des Unternehmens selbst, sondern auch bei sämtlichen externen Dienstleistungsanbietern respektive Auftragnehmern gewährleistet werden.

Nach fast dreissig Jahren grosser technologischer Fortschritte und Diskussionen über die Zukunft der entsprechenden Gesetzgebung wurde das revidierte Datenschutzgesetz (revDSG) vom Parlament am 25. September 2020 angenommen. Das totalrevidierte Datenschutzgesetz tritt am 1. September 2023 ohne Übergangsfrist in Kraft.[1]

In diesem Beitrag soll die Revision des Datenschutzgesetzes näher beleuchtet und die Bedeutung dieses Themas für die berufliche Vorsorge hervorgehoben werden. Zunächst wird auf die relevantesten Änderungen und die praktischen Ziele der abgeschlossenen Totalrevision eingegangen sowie die spezifischen Rechtsgrundlagen für Pensionskassen dargelegt und danach werden ausgewählte Themen tiefer beleuchtet.

II. Grundzüge des neuen Datenschutzgesetzes

Durch die Revision wird das Regelungskonzept des Datenschutzgesetzes nicht angetastet.[2] Wie bereits im geltenden DSG sind auch im revDSG für die Datenbearbeitung gewisse Grundsätze vorgesehen. Neben diesen Bearbeitungsgrundsätzen sind im modernen Datenschutzrecht auch die datenschutzrechtlichen sogenannten flankierenden Massnahmen (insbesondere Prozesse und Dokumentation) von grosser Bedeutung.[3] Zu ihnen gehören die Führung eines Bearbeitungsverzeichnisses, die Durchführung von Datenschutz-Folgeabschätzungen sowie verschiedene Meldepflichten.

1 Bundesamt für Justiz BJ, Neues Datenschutzrecht ab 1. September 2023, <https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-90134.html>, zuletzt besucht am 16.11.2022.

2 ROSENTHAL DAVID, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 7.

3 VASELLA DAVID, Das neue Datenschutzgesetz und seine Umsetzung, Schweizerischer Treuhänder-Verband STV, S. 272, 273.

A. Praktische Ziele der Revision

Ziel der Revision ist die Stärkung der Rechte der Betroffenen einer Datenbearbeitung. Mit dem Aufkommen zahlreicher Technologien in der digitalen Welt ist die Wahrscheinlichkeit einer Persönlichkeitsverletzung durch eine unrechtmässige Bearbeitung von Personendaten stark gestiegen und wirkt sich eine Persönlichkeitsverletzung stärker aus. Die neuen Möglichkeiten bedürfen entsprechend neuer Regulierungen. Sodann soll das revDSG das Angemessenheitsniveau gegenüber der EU erhalten.[4]

Zu den praktischen Zielen der abgeschlossenen Revision gehören insbesondere:

- Erweiterung des Anwendungsbereichs des DSG
- Stärkung der Betroffenenrechte
- Klarere Unterscheidung zwischen Verantwortlichen und Auftragsbearbeitern
- Definition von Informationspflichten
- Implementierung einer Pflicht zur Erstellung von Datenschutz-Folgeabschätzungen
- Einführung von Meldepflichten
- Einführung strengerer Sanktionen, um die Einhaltung des Gesetzes zu forcieren.

B. Die wichtigsten Neuerungen

Der Geltungsbereich des revDSG wurde erweitert, damit sämtliche Akteure erfasst werden können, welche durch ihre Datenbearbeitungen einen Einfluss auf die Schweiz nehmen können. So hält Art. 3 revDSG fest, dass sämtliche Sachverhalte erfasst werden, welche sich in der Schweiz auswirken.

4 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 6943.

Weiter werden Datenbearbeiter gezwungen, ihre Datenbearbeitungen besser zu dokumentieren und die betroffenen Personen darüber detaillierter aufzuklären.

Ausserdem wurden die datenschutzrechtlichen Sanktionsmöglichkeiten im Fall einer Verletzung angepasst bzw. erweitert. Es kann festgestellt werden, dass die strafrechtlichen Regelungen strenger geworden sind.

Vorliegend wird nur auf die wichtigsten Änderungen eingegangen. Daneben hat der Gesetzgeber zahlreiche andere Änderungen vorgenommen.

1. Erweiterung von Dokumentationspflichten als Corporate-Governance-Massnahme

Zur Erweiterung der Dokumentationspflicht gehören Massnahmen wie die Pflicht zur Erstellung eines Verzeichnisses der Bearbeitungstätigkeiten (nachfolgend Bearbeitungsverzeichnis) und Datenschutz-Folgenabschätzung sowie die Meldung von Datensicherheitsverletzungen seitens der Bearbeiter. Diese eingeführten Instrumente werden in der Praxis als neue Corporate-Governance-Massnahmen qualifiziert, indem mögliche datenschutzrechtliche Verletzungen und unrechtmässige Bearbeitungen vermieden werden sollen. Gleichzeitig soll die nachträgliche Überprüfung und Sanktionierung effektiver und effizienter durchgeführt werden können.

2. Neue Konzepte für Profiling und Profiling mit hohem Risiko

Auf der Grundlage der während des Konsultationsverfahrens eingegangenen Stellungnahmen wurde der Inhalt des Begriffs «Profiling» an die europäische Terminologie angepasst und umfasst nun nur noch die automatisierte Bearbeitung von Personendaten.[5] Dieser Begriff ist in Art. 5 lit. f des revDSG verankert und definiert. Laut Gesetz kann «Profiling» dadurch gekennzeichnet werden, dass Personendaten

5 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 7021.

automatisiert ausgewertet werden, um auf der Grundlage dieser Auswertung, ebenfalls in automatisierter Weise, die Merkmale einer Person zu bewerten.[6]

Bei einem «Profiling mit hohem Risiko» handelt es sich um ein Profiling, dass ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt und zur Verknüpfung von Daten führt, die eine Bewertung der wesentlichen Aspekte der Persönlichkeit einer natürlichen Person ermöglichen.[7] An ein solches Profiling werden in verschiedenen Bereichen Rechtsfolgen geknüpft, beispielsweise Protokollierungspflicht gemäss Art. 4 DSV oder ausdrückliche Einwilligung gemäss Art. 6 Abs. 7 revDSG.

3. Neue Kompetenzen des EDÖB

Aufgrund der in der Praxis festgestellten Defizite betreffend die Rolle und Kompetenzen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) werden durch das Inkrafttreten des neuen Gesetzes dessen Möglichkeiten ausgebaut und gestärkt. Er kann zukünftig Untersuchungen von Verstössen gegen Datenschutzvorschriften von Amtes wegen eröffnen und mittels Verfügungskompetenzen nach Art. 51 Abs. 1 revDSG Verpflichtungen aussprechen. Darüber hinaus werden missachtete Verfügungen des EDÖB gemäss Art. 63 revDSG von Amtes wegen verfolgt und mit Busse bestraft.[8] Damit erhält der EDÖB umfassende Aufsichtsbefugnisse, um die Einhaltung des Datenschutzes sicherzustellen.

III. Spezifische Rechtsgrundlagen für Pensionskassen

Das revDSG sieht gewisse Unterschiede vor, je nachdem, ob Bundesorgane oder Private tangiert sind. Gemäss dem Datenschutzgesetz werden Pensionskassen im Bereich der obligatorischen beruflichen Vorsorge als Bundesorgane eingestuft[9].

6 Art. 5 Bst. f revDSG.
7 Art. 5 Bst. g revDSG.
8 Art. 63 revDSG.
9 EMMEL SIMONE, Art. 85*a* BVG N 2, in: Hürzeler Marc/Hans-Ulrich Stauffer (Hrsg.), Basler Kommentar Berufliche Vorsorge, Basel 2021.

Deshalb erfordert deren Bearbeitung von Personendaten laut revDSG eine gesetzliche Grundlage.[10] Im Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) sind datenschutzrechtliche Bestimmungen in den Art. Art. 85*a* ff. BVG zu finden. Trotz der Revision des DSG bleiben diese Bestimmungen im BVG unverändert.

Neben dieser allgemein einzuhaltenden Regel bezüglich einer gesetzlichen Grundlage sind die Bestimmungen des revDSG in Bezug auf das BVG ergänzend anwendbar, insbesondere die Bearbeitungsgrundsätze[11]. Wo die Pensionskassen im überobligatorischen Bereich Personendaten bearbeiten, unterstehen sie den allgemeinen Regelungen für Private im Datenschutzrecht[12]. Bei umhüllenden Pensionskassen besteht neben dem obligatorischen Vorsorgeverhältnis auch ein Vorsorgeverhältnis im Überobligatorium. Die Daten und Anforderungen an den Datenschutz lassen sich in der Praxis in der Regel allerdings nicht trennen. Umhüllende Pensionskassen haben daher sicherzustellen, dass sie sowohl die Anforderungen nach BVG als auch jene nach revDSG einhalten.

Wenn es um rein ausser- oder rein überobligatorische Vorsorgeeinrichtungen geht, sind diese Pensionskassen gemäss revDSG als Privatpersonen zu qualifizieren und nicht als Bundesorgane[13]. Diesfalls gelten die Bestimmungen des revDSG.

10 Art. 34 revDSG.

11 PÄRLI KURT, Art. 85*a* BVG N 5, in: Schneider Jacques-André/Geiser Thomas/Gächter Thomas (Hrsg.), Kommentar zum schweizerischen Sozialversicherungsrecht, BVG und FZG, 2. Aufl., Bern 2019.

12 Die Art. 85a ff. BVG sind in Art. 49 Abs. 2 BVG nicht aufgezählt (Ausnahmen vgl. Art. 49 Abs. 2 Ziff. 25*a*, 25*b* und 26 BVG); PÄRLI KURT, Art. 85*a* BVG N 15, in: Schneider Jacques-André/Geiser Thomas/Gächter Thomas (Hrsg.), Kommentar zum schweizerischen Sozialversicherungsrecht, BVG und FZG, 2. Aufl., Bern 2019.

13 Vorsorgeeinrichtungen, die an der Durchführung der obligatorischen Versicherung teilnehmen wollen, müssen sich bei der Aufsichtsbehörde in das Register für die berufliche Vorsorge eintragen lassen. Registrierte Vorsorgeeinrichtungen müssen die Rechtsform einer Stiftung haben oder eine Einrichtung des öffentlichen Rechts mit eigener Rechtspersönlichkeit sein. In der obligatorischen beruflichen Vorsorge war bis 31. Dezember 2013 auch die Gründung einer registrierten Vorsorgeeinrichtung in der Rechtsform einer Genossenschaft zulässig. In der ausserobligatorischen beruflichen Vorsorge ist neben der Stiftung und Einrichtung des öffentlichen Rechts auch die Genossenschaft zugelassen (Art. 48 BVG, Art. 331 Abs. 1 OR). Die öffentlich-rechtlichen Vorsorgeeinrichtungen müssen seit 1. Januar 2014 eine Einrichtung des öffentlichen Rechts mit eigener Rechtspersönlichkeit sein. Das umfasst einerseits die selbständige öffentlich-rechtliche Anstalt, anderseits die Stiftung des öffentlichen Rechts. Eine mögliche Rechtsform für die Vorsorgeeinrichtung einer öffentlich-rechtlichen Körperschaft ist auch die privatrechtliche Stiftung. Siehe zum Ganzen KONRAD HANSPETER/LAUENER

Demzufolge wird für die Bearbeitung von Personendaten keine bestimmte gesetzliche Grundlage verlangt, wenn die Persönlichkeit der Betroffenen nicht verletzt wird (dies wäre der Fall, wenn die Bearbeitungsgrundsätze nicht eingehalten werden, die Bearbeitung entgegen dem ausdrücklichen Willen der Betroffenen erfolgten oder es sich um besonders schützenswerte Personendaten handelt[14]). Falls eine Persönlichkeitsverletzung eingetreten ist, werden Rechtfertigungsgründe verlangt.

IV. Umsetzung der Revision des Datenschutzgesetzes

Im Vordergrund steht vor allem die konkrete Umsetzung der Betroffenenrechte und damit das Wissen, in welchen Systemen Personendaten bearbeitet werden, wie sie herauszugeben sind und welche Schutzmassnahmen ergriffen werden. Die Komplexität und Struktur der Unternehmen bzw. Pensionskassen und der Umfang der bearbeiteten Daten sind unterschiedlich, was sich bei der konkreten Umsetzung auswirkt. Ungeachtet dessen, empfiehlt es sich, nach einem allgemeinen Ansatz vorzugehen.

Es gilt, die einzelnen Compliance-Schritte von Beginn an konsequent durchzusetzen und zu implementieren. Dies ermöglicht eine effiziente und gleichzeitig auch korrekte Implementierung der neuen Anforderungen:

1. Evaluation Status quo: Status quo der aktuellen Bearbeitungen von Personendaten ermitteln.
2. Analyse: Durchführung einer GAP-Analyse (Status quo vs. neue Anforderungen des revDSG) zur Identifikation von Lücken.
3. Umsetzungsentscheide: Entscheid zur Umsetzung eines Datenschutzprojektes.

MICHAEL, Art. 48 BVG N 21 ff., in: Hürzeler Marc/Hans-Ulrich Stauffer (Hrsg.), Basler Kommentar Berufliche Vorsorge, Basel 2021. Im Rahmen dieses Aufsatzes nicht weiter behandelt wird die ausserobligatorische beruflichen Vorsorge in Form der Einrichtung des öffentlichen Rechts.

14 Art. 30 revDSG.

4. Umsetzungsplan: Erstellung eines Plans mit Handlungsbedarf, Zeitplan und Verantwortlichkeiten.
5. Umsetzung: Massnahmen zur Einhaltung des revDSG formalisieren (z.B. Datenschutzerklärungen, DSG-Richtlinien, Anpassung der Vereinbarungen mit Dritten, Prozesse) und technische & organisatorische Massnahmen erstellen, anpassen und implementieren.
6. Dokumentation: Angemessene Dokumentation erstellen (Bearbeitungsverzeichnis usw.)
7. Schulung: Schulung der involvierten Personen, insbesondere Stiftungsräte, Geschäftsführung und Versichertenverwaltung, HR-Mitarbeiter des Arbeitgebers usw.
8. Überwachung: Periodische Überprüfung und Aktualisierung der Dokumentation und der Prozesse.

V. Strafbestimmungen

Laut Botschaft zum Bundesgesetz über die Totalrevision des DSG, die im Jahr 2017 publiziert wurde, müssen die strafrechtlichen Bestimmungen im Vergleich zum geltenden Recht verstärkt werden.[15] Die verschärften Sanktionen des revDSG sind in den Art. 60 ff. revDSG verankert. Mit Bussen bis zu CHF 250'000 werden sowohl die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten als auch die Verletzung von Sorgfaltspflichten und beruflicher Schweigepflicht bestraft.[16] Die Tatbestände sind jedoch nur in Fällen (eventual)vorsätzlicher Handlungen erfüllt.

Aus privater Sicht brachte das revidierte Gesetz eine Neuigkeit. Im Unterschied zur DSGVO werden grundsätzlich die handelnden Personen (Private) und nicht die Unternehmen bestraft. Mit der handelnden Person bezieht sich der Gesetzgeber im Fall

15 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 7099.

16 Art. 60 und Art. 61 DSG.

der Datenbearbeitung bei Unternehmen auf die Leitungspersonen.[17] Diese sind gesetzlich verpflichtet, die Einhaltung dieser Pflichten im Unternehmen sicherzustellen.[18] Wie sich in der Praxis die Sanktionierung der Leitungspersonen ausgestalten wird, darf mit Spannung verfolgt werden. Es muss gehofft werden, dass nicht die ausführenden Personen verfolgt werden, sondern tatsächlich die Entscheidungsgremien.

Der Bussenrahmen wurde mit der Totalrevision von CHF 10'000 auf CHF 250'000 erhöht, wobei dieser Betrag den gesetzlich festgelegten Höchstbetrag darstellt.[19] Weiter wird eine neue Strafandrohung eingeführt bei Missachtung von Verfügungen des Eidgenössischen Datenschutzbeauftragten (EDÖB).[20]

VI. Ausgewählte Beispiele

A. Verzeichnis der Bearbeitungstätigkeit

Gemäss Art. 12 revDSG müssen der Verantwortliche und der Auftragsbearbeiter je ein sogenanntes Verzeichnis der Bearbeitungstätigkeiten führen.[21] Beim Bearbeitungsverzeichnis handelt es sich grundsätzlich um ein Inventar aller Bearbeitungstätigkeiten einer Person, die Personendaten verarbeitet. Dieses Verzeichnis wird in der Folge Informationen zu Software, Datenbanken, Verantwortlichen, Datenempfängern enthalten und dem Verantwortlichen sowie dem EDÖB als Orientierungspunkt für datenschutzrechtliche Fragen dienen.

Das revidierte Gesetz nennt zur Orientierung den Minimalinhalt für Bearbeitungsverzeichnisse (Art. 12 Abs. 2 revDSG). Der Mindestumfang umfasst insbesondere den Zweck der Bearbeitung, die betroffenen Personen sowie die Kategorien der

17 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 7100.
18 BGE 142 IV 315.
19 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 6974.
20 Art. 63 DSG.
21 Art. 12 revDSG.

bearbeiteten Personendaten (bspw. Kontaktinformationen, Identifikationsdokumente, Altersguthaben, Gesundheitsvorbehalt). Die einzelnen Bearbeiter sind jedoch frei, weitere Informationen zu erfassen. Dies kann sich für interne Zwecke anbieten, falls das Bearbeitungsverzeichnis als umfassende Dokumentation dienen soll. Die Bundesorgane haben ihre Verzeichnisse dem EDÖB zu melden[22].

Obwohl das Gesetz keine Anforderungen an die Form des Bearbeitungsverzeichnisses stellt, empfehlen wir ab einer gewissen Unternehmensgrösse (ab ca. 50 bis 100 Mitarbeitern) oder einer grossen Menge von Personendaten das Bearbeitungsverzeichnis in einem spezifischen Datenschutztool[23] zu erfassen. Die entsprechenden Hilfsmittel stellen bereits vorgefertigte Verzeichnisse zur Verfügung und leiten den Nutzer bei der korrekten Erstellung des Bearbeitungsverzeichnisses an. Weiter lassen sich die Daten meist intern verknüpfen, was Fehler durch Kopiervorgänge vermeiden und stets aktuelle Daten sicherstellen soll. Für die meisten Vorsorgeeinrichtungen wird allerdings die Nutzung einer einfachen Excel-Tabelle ausreichend sein.

B. Datenschutzberater

Anders als Private müssen Bundesorgane gemäss Art. 25 DSV immer einen Datenschutzberater ernennen. Somit hat der Bundesrat von seiner Kompetenz, das Thema Datenschutzberater von Bundesorganen zu regeln (Art. 10 Abs. 4 revDSG), umfassend Gebrauch gemacht. Für kleinere Pensionskassen dürfte dabei insbesondere der in Art. 25 DSV enthaltene Passus, nachdem mehrere Bundesorgane eine/n gemeinsame/n Datenschutzberater/in ernennen können, von grossem Interesse sein. Hier könnten entsprechende Branchenverbände allenfalls eine zentrale Rolle einnehmen, um die Einhaltung des Datenschutzes ihrer Mitglieder zu erleichtern und Synergien nutzbar zu machen.

22 Art. 12 Abs. 4 revDSG.

23 Beispiele wären: ZOA, Swiss GRC, OneTrust.

C. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) wurde bereits 2018 im europäischen Datenschutzrecht verankert. Sie soll präventiv die Datenschutzkonformität einzelner Datenbearbeitungen sicherstellen, indem die geplante Bearbeitung beschrieben, analysiert und falls notwendig die gebotenen Schutzmassnahmen definiert werden. Sie erfreut sich in den letzten Jahren als Compliance-Instrument zunehmender Beliebtheit und wird teilweise auf freiwilliger Basis bereits in der Schweiz angewendet. In der Schweiz wird die Durchführung notwendig sein, wenn eine geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann[24]. Das hohe Risiko wird sogleich selbst im Gesetz umschrieben, wobei ein solches insbesondere bei Verwendung neuer Technologien vorliegen soll. Weiter kann sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ein hohes Risiko ergeben.

Eine Datenschutz-Folgenabschätzung ist das Instrument, um eine Bearbeitung von Personendaten unter dem Gesichtspunkt der Einhaltung der Datenschutznormen zu validieren und zu rechtfertigen.[25] Eine DSFA nach Art. 22 revDSG soll deshalb zeigen, wo Risiken für die Persönlichkeit oder die Grundrechte von betroffenen Personen bestehen und deshalb Massnahmen zu deren Schutz benötigt werden sowie die entsprechenden Massnahmen aufzeigen.[26]

Aufgrund der grossen Verbreitung der DSFA haben verschiedene europäische Aufsichtsbehörden, Interessensverbände sowie Datenschutztools-Hersteller Muster[27] erstellt. Da für öffentliche Institutionen und Behörden DSFAs bereits seit 2020 vorgeschrieben sind, wurden auch Muster in der Schweiz publiziert[28]. Private können sich an diesen orientieren.

24 Art. 22 Abs. 1 revDSG.

25 DAVID ROSENTHAL, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, Rz. 148.

26 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, S. 7059.

27 Information Commissioner's Office (Aufsichtsbehörde des Vereinigten Königreichs) <https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf>, zuletzt besucht am 28.11.2022.

28 Datenschutzbeauftragte des Kantons Zürich, <https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung>, zuletzt besucht am 28.11.2022.

Bei der Durchführung ist zwingend notwendig, dass eine interdisziplinäre Arbeitsgruppe zusammengestellt wird, um sämtliche Aspekte der Bearbeitung zu erfassen. So sind üblicherweise die Rechtsabteilung, die für die Bearbeitung Verantwortlichen (bspw. die Personalabteilung) sowie die zuständige Informatikabteilung und wo notwendig auch der Hersteller/Betreiber einer Software involviert. Die Dokumentation zur DSFA sind für mindestens zwei Jahre über die eigentliche Bearbeitung hinaus aufzubewahren (Art. 14 DSV), weshalb bereits während der Durchführung das Thema Archivierung geplant werden muss. Eine DSFA ist beispielsweise erforderlich, wenn intern eine neue Cloud-Lösung eingeführt wird, wenn mit einem neuen Outsourcing-Partner zusammengearbeitet wird oder wenn neue Self-Service-Portale zur Verfügung gestellt werden (beispielsweise zur Simulation von Leistungen der Pensionskasse).

D. Internationaler Datentransfer

Ein internationaler Datentransfer liegt vor, wenn Personendaten von Personen in der Schweiz in ein Drittland oder an eine internationale Organisation übermittelt werden. Ein solcher Transfer von Personendaten, unabhängig ob an einen Verantwortlichen oder Auftragsbearbeiter, darf nur erfolgen, wenn die Empfänger einen angemessenen Schutz gewährleisten können. Dies kann durch die lokale Gesetzgebung geschehen[29] oder durch die Ergreifung von zusätzlichen Absicherungsmassnahmen[30].

Anders als heute wird zukünftig nicht mehr der EDÖB über die Staatenliste betreffend angemessenem Datenschutzniveau[31] bzw. über die Angemessenheit von lokalen Datenschutzgesetzgebungen entscheiden, sondern diese Kompetenz wird dem Bundesrat zufallen. Die Staaten, welche einen angemessenen Schutz gewährleisten können, werden im Anhang der DSV aufgeführt werden (Art. 16 revDSG i.V.m. Art. 8 DSV).

29 Art. 16 Abs. 1 revDSG.

30 Art. 16 Abs. 2 revDSG.

31 Staatenliste abrufbar unter <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html>, zuletzt besucht am 28.11.2022.

Sind die entsprechenden Länder nicht im Anhang der DSV aufgeführt, so müssen zusätzliche Absicherungsmassnahmen vorliegen (Art. 16 Abs. 2 revDSG). In der Praxis sind die vom EDÖB genehmigten Standarddatenschutzklauseln das meistverwendete Instrument, um ein entsprechendes Schutzniveau sicherzustellen. Selbst grosse Internetdienstleister sehen die Verwendung der entsprechenden Klauseln teilweise bereits vor.

Der internationale Datentransfer hat insbesondere aufgrund der Thematiken rund um US-Cloud Anbieter in den letzten Jahren an Brisanz gewonnen. Bereits zweimal wurden bestehende Schutzmechanismen (Safe Harbour und Privacy Shield) durch europäische Gerichtsurteile ausser Kraft gesetzt (Schrems I und II). Grund für die in der Praxis hart geführten Diskussionen sind insbesondere die extensiven Überwachungs- und Zugriffsmöglichkeiten (insb. Cloud-Act und FISA) der amerikanischen Strafverfolgungs- und Geheimdienstbehörden und der mögliche Rechtschutz von betroffenen Personen. So hat sich der EDÖB bereits kritisch über die Rechtmässigkeit des Einsatzes von US-Cloud-Anbietern in der Schweiz geäussert, selbst wenn die Daten in Rechenzentren in der Schweiz gespeichert werden.[32] Grund sind die extensiven Möglichkeiten der US-Behörden die Herausgabe der Personendaten auch aus Schweizer Rechenzentren zu verlangen, ohne den internationalen Rechtshilfeweg zu beschreiten. Inwiefern diese Möglichkeiten bestehen, ob entsprechende Weigerungsgründe möglich wären und ob eine Cloud-Nutzung nun unrechtmässig ist, wird in Datenschutzkreisen intensiv diskutiert.[33]

Unserer Ansicht nach ist ein Einsatz aktuell und unter dem zukünftigen Datenschutzrecht möglich, wenn die notwendigen Rahmenbedingungen geschaffen werden (zusätzliche Absicherungsmassnahmen, Vereinbarung Geheimnisschutz und Standardvertragsklauseln, etc.). Wichtig ist jedoch eine zielgerichtete Abklärung,

32 Stellungnahme des EDÖB Risikobeurteilung Suva Projekt Digital Workplace M365 <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1587794875>, zuletzt besucht am 28.11.2022.

33 Vgl. CHRISTIAN LAUX, ALEXANDER HOFMANN, Rechtmässigkeit von Public Cloud Services "Cloud-Gutachten"; DAVID ROSENTHAL, GENIE OUT OF THE BOTTLE?, in: Alps Forum 2021, Tagungsband; DAVID VASELLA, auf datenrecht.ch, <https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/>, zuletzt besucht am 28.11.2022; ADRIAN LOBSIGER, Edöb: "Vertrauen Behörden nur auf private Gutachten, können sie sich eine blutige Nase holen", <https://www.inside-it.ch/edoeb-vertrauen-behoerden-nur-auf-private-gutachten%2C-koennen-sie-sich-eine-blutige-nase-holen-20220928>, zuletzt besucht am 28.11.2022.

Dokumentation und ein intern getragener Risikoentscheid betreffend Umsetzung. Weiter ist es unabdingbar, diese Thematik weiter zu beobachten.

VII. Fazit

Das revidierte Datenschutzgesetz wird am 1. September 2023 ohne Übergangsfrist in Kraft treten, womit sämtliche Anforderungen umgehend einzuhalten sind. Wie vorgehend aufgezeigt, müssen Pensionskassen nun ihre vorhandenen Datenschutzmassnahmen evaluieren, um den Bedarf an weiteren Massnahmen zu klären. Ein entsprechendes Projekt kann in Einzeletappen organisiert und durchgeführt werden, benötigt jedoch entsprechende interne und evtl. externe Ressourcen für eine praxisorientierte, pragmatische und gleichzeitig rechtmässige Umsetzung. Gleichzeitig bietet die Umsetzung der Massnahmen eine gute Gelegenheit, allfällige Altlasten aufzuräumen und mögliche Synergien zu erkennen und nutzbar zu machen. Aufgrund der drastisch erhöhten Sanktionsmöglichkeiten sollte nicht mit der Umsetzung zugewartet werden.

Da in der Praxis verschiedene Normen des revDSG bzw. der DSV in ihrer konkreten Ausgestaltung noch unklar sind, werden sich in den nächsten Monaten und Jahren wohl verschiedene Behörden und Gerichte mit dem Thema Datenschutz befassen. Entsprechend sollte eine regelmässige Konsultation mit Experten oder interne Überwachung der laufenden Diskussionen eingeplant werden.

Obwohl die Pflichten unter dem revDSG extensiv erscheinen, so verhindert weder das bestehende noch das neue Datenschutzgesetz den Einsatz und Entwicklung innovativer Ideen und Technologien. Eine gut geplante Einführung entsprechender Produkte, unter Berücksichtigung des Datenschutzes, kann folglich weiterhin ein Gewinn für sämtliche Beteiligte sein.