

Checkliste Datenschutz-Compliance Pensionskasse

Allgemeines

	Ja	Nein
Sofern die Einwilligung der betroffenen Personen für die Bearbeitung von Personendaten erforderlich ist, werden diese Einwilligungen eingeholt und dokumentiert?	☐	☐
Sofern die Einwilligung der betroffenen Personen für die Bearbeitung von Personendaten erforderlich ist, werden diese für bestimmte Bearbeitungen, mit angemessener Information und ggf. ausdrücklich für die Bearbeitung von besonders schützenswerten Personendaten von den Betroffenen eingeholt?	☐	☐
Führt die Pensionskasse ein Bearbeitungsverzeichnis mit allen erforderlichen Angaben?	☐	☐
Hat die Pensionskasse das Bearbeitungsverzeichnis dem EDÖB mitgeteilt?	☐	☐
Führt die Pensionskasse Datenbearbeitungen aus, die ein hohes Risiko für die Persönlichkeit oder Grundrechte der Betroffenen bedeutet und hat sie für solche Datenbearbeitungen vorgängig eine Datenschutz-Folgenabschätzung ausgeführt?	☐	☐
Bewahrt die Pensionskasse erstellte Datenschutz-Folgenabschätzungen nach Beendigung der Datenbearbeitung für mindestens zwei Jahre auf?	☐	☐
Erfüllt die Pensionskasse etwaige weitergehende kantonale Anforderungen zum Datenschutz?	☐	☐

Datenschutzberater

Umhüllende (registrierte) Pensionskassen, die sowohl im obligatorischen als auch im überobligatorischen Bereich tätig sind, unterliegen den Datenschutzbestimmungen für Bundesorgane und müssen nach Art. 25 DSV einen Datenschutzberater benennen.

	Ja	Nein
Hat die Pensionskasse einen Datenschutzberater benannt?	☐	☐
Gehört es zu den Aufgaben des Datenschutzberaters, die Pensionskasse in Fragen des Datenschutzes zu schulen und zu beraten?	☐	☐
Werden dem Datenschutzberater die notwendigen Ressourcen und Zugang zu allen Auskünften, Unterlagen, Bearbeitungsverzeichnissen und Personendaten zur Verfügung gestellt, die er zur Erfüllung seiner Aufgaben benötigt und hat er das	☐	☐

Recht, in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan der Pensionskasse zu informieren?		
Wurden die Kontaktdaten des Datenschutzberaters auf der Webseite der Pensionskasse veröffentlicht?	☐	☐
Wurden die Kontaktdaten des Datenschutzberaters dem EDÖB mitgeteilt?	☐	☐
Wurden die Kontaktdaten des Datenschutzberaters den Beschäftigten mitgeteilt und steht der Datenschutzberater als Ansprechpartner in Datenschutzfragen allen Beschäftigten zur Verfügung?	☐	☐

Prozesse

	Ja	Nein
Wurden angemessene Massnahmen getroffen, um bei einer Auskunftsanfrage die betroffene Person zu identifizieren?	☐	☐
Wurden Prozesse implementiert, wonach Auskunftsanfragen Betroffener innerhalb der vorgegebenen Frist von 30 Tagen beantwortet werden?	☐	☐
Wurden Prozesse implementiert, wonach Personendaten auf Anfrage der Betroffenen in einem elektronischen Format herausgegeben werden?	☐	☐
Wurden Prozesse implementiert, wonach Anfragen Betroffener auf Berichtigung, Löschung oder Vernichtung von Personendaten fristgerecht bearbeitet werden?	☐	☐
Wurden Prozesse implementiert, wonach Datenschutzverletzungen mit hohem Risiko für die Persönlichkeit und Grundrechte für Betroffene baldmöglichst an den EDÖB gemeldet werden?	☐	☐
Wurden Prozesse implementiert, wonach Datenschutzverletzungen dokumentiert und die Dokumentationen mindestens zwei Jahre aufbewahrt werden?	☐	☐

Informationspflichten

Nach Art. 19 DSGVO müssen Betroffene umfassend über die Datenbearbeitungen der Pensionskasse aufgeklärt werden.

	Ja	Nein
Werden die Betroffenen (Versicherte, Mitarbeitende, ...) zum Zeitpunkt der Beschaffung von Personendaten über Umfang und Zwecke der	☐	☐

Checkliste Datenschutz-Compliance Pensionskasse

Datenbearbeitungen in präziser, transparenter, verständlicher und leicht zugänglicher Form informiert und sind diese Informationen vollständig?	☐	☐
Werden Betroffene über automatisierte Einzelentscheidungen informiert und haben sie die Möglichkeit, ihren Standpunkt darzulegen?	☐	☐

Datenlöschung

Das Datenschutzrecht fordert, dass Personendaten nur so lange bearbeitet werden, wie es für die festgelegten Zwecke und etwaige gesetzliche Aufbewahrungsfristen erforderlich ist.

	Ja	Nein
Wird das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten von Personendaten protokolliert, wenn besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder ein Profiling mit hohem Risiko durchgeführt wird und präventiven Massnahmen den Datenschutz nicht gewährleisten können?	☐	☐

Auftragsbearbeitung und Bekanntgabe ins Ausland

Die weisungsgebundene Bearbeitung von Personendaten durch Dienstleister soll auf Grundlage eines Vertrages durchgeführt werden. Wenn Dienstleister Personendaten im Auftrag bearbeiten, ist nach Art. 9 DSGVO die Einhaltung bestimmter Sicherheitsstandards zu fixieren. Personendaten dürfen ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet ist.

	Ja	Nein
Sind alle Auftragsbearbeiter identifiziert?	☐	☐
Wurden mit allen Auftragsbearbeitern vertragliche Regelungen zur Auftragsbearbeitung getroffen?	☐	☐
Hat sich die Pensionskasse bei jedem Auftragsbearbeiter vergewissert, dass dieser in der Lage ist, die Datensicherheit zu gewährleisten?	☐	☐
Dürfen Auftragsbearbeiter Personendaten nur mit vorgängiger spezifischer oder allgemeiner Genehmigung der Pensionskasse einem Dritten übertragen?	☐	☐
Ist bei einer Bekanntgabe von Personendaten ins Ausland ein geeigneter Datenschutz gewährleistet und erfolgt die Bekanntgabe nur in ein Land mit angemessenem Datenschutzniveau, unter Anwendung von Standardvertragsklauseln oder gemäss Ausnahmen nach Art. 17 DSGVO?	☐	☐

Verwendet die Pensionskasse bei einer Datenbekanntgabe ins Ausland auf Grundlage von Standardvertragsklauseln die genehmigten Vertragsklauseln des EDÖB mit den vorgeschriebenen Anpassungen?	☐	☐
Hat die Pensionskasse angemessene Massnahmen getroffen, um sicherzustellen, dass die Empfänger bei einer Datenbekanntgabe ins Ausland mittels Standardvertragsklauseln diese auch beachten?	☐	☐

Technische Sicherheit

	Ja	Nein
Hat die Pensionskasse die Risiken für Persönlichkeit und Grundrechte der Betroffenen sowie Schutzbedarfe der Personendaten bestimmt und geeignete technische und organisatorische Massnahmen gemäss dem Risiko festgelegt?	☐	☐
Wurden geeignete Massnahmen getroffen, damit für die bearbeiteten Daten ihren Schutzbedarfen entsprechend die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Datenbearbeitung gewährleistet ist?	☐	☐
Werden Personendaten vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind?	☐	☐
Wurden bei der Datenbearbeitung datenschutzfreundliche Voreinstellungen getroffen?	☐	☐

Organisatorische Sicherheit

	Ja	Nein
Hat die Pensionskasse eine Datenschutzrichtlinie und ein Datenschutzkonzept erstellt?	☐	☐
Soweit erforderlich, hat die Pensionskasse ein Bearbeitungsreglement erstellt, in dem Angaben zur internen Organisation, Datenbearbeitungs- und Kontrollverfahren, Verantwortlichkeiten der beteiligten Personen sowie den Massnahmen zur Gewährleistung der Datensicherheit enthalten sind und wurde das Reglement dem Verwaltungsrat zur Kenntnis gebracht?	☐	☐
Soweit erforderlich, wurde das Datenschutzreglement nach dem BVG der kantonalen Revisionsstelle zur Prüfung vorgelegt?	☐	☐
Werden interne und externe Personen mit Zugang zu Personendaten zur datenschutzrechtlichen Verschwiegenheit verpflichtet?	☐	☐