



Reglement über den Umgang mit Informationen (Informationsreglement)

Gültig ab 01.09.2023

Vom 30.08.2023 (Stand 30.08.2023)

Inhaltsverzeichnis

Kapitel A	Allgemeine Bestimmungen	3
Art. 1	Zweck und Unterstellung	3
Art. 2	Ziele und Grundsätze	3
Art. 3	Umsetzung	4
Art. 4	Berichterstattung	4
Kapitel B	Schlussbestimmungen	5
Art. 5	Inkrafttreten	5

Der Verwaltungsrat erlässt gestützt auf das Organisationsreglement der PKBS, Art. 85a Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG), das Gesetz des Kantons Basel-Stadt über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG, SG 153.260) und seiner zugehörigen Verordnung des Kantons Basel-Stadt über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV, SG 153.270) folgendes Reglement:

Kapitel A Allgemeine Bestimmungen

Art. 1 Zweck und Unterstellung

- ¹ Das vorliegende Reglement definiert die Ziele, Grundsätze und Massnahmen im Umgang mit Informationen und der für ihre Bearbeitung erforderlichen Infrastruktur innerhalb der PKBS.
- ² Das vorliegende Reglement gilt für alle Fachbereiche und Mitarbeitenden der PKBS.
- ³ Die für externe Personen relevanten Bestimmungen werden in vertraglichen Vereinbarungen verbindlich festgelegt.

Art. 2 Ziele und Grundsätze

- ¹ **Rechtmässigkeit:** Die PKBS hält im Umgang mit Informationen ihre gesetzlichen Grundlagen und Vorgaben ein und ergreift geeignete Massnahmen zur Wahrung der Informationssicherheit, ihrer betrieblichen Resilienz und des Datenschutzes.
- ² **Vertrauen:** Die PKBS tut dies jedoch nicht nur, weil sie gesetzlich dazu verpflichtet ist. Vielmehr geht es darum, den berechtigten Erwartungen ihrer Destinatäre, Kunden und Mitarbeitenden, aber auch der Politik und der Öffentlichkeit gerecht zu werden. Das Vertrauen in die PKBS soll gestärkt werden.
- ³ **Ethik:** Der Umgang mit Informationen bei der PKBS genügt zu jeder Zeit den ethischen Grundsätzen der Transparenz, Kontrolle und Vermeidung von Diskriminierung. Diese Grundsätze werden bereits bei der Planung neuer Projekte, wie der Einführung neuer Systeme oder Bearbeitungstätigkeiten, berücksichtigt.
- ⁴ **Digitalisierung:** Die PKBS verzichtet soweit wie möglich auf die Bearbeitung von Informationen auf Papier. Sie stellt ihren Destinatären und Kunden Möglichkeiten zur Verfügung, um elektronisch mit ihr kommunizieren zu können.
- ⁵ **Governance:** Die PKBS definiert, plant, steuert und kontrolliert die Informationssicherheit und den Datenschutz mithilfe eines Information Security Management Systems (ISMS).
- ⁶ **Resilienz:** Die PKBS trifft geeignete Massnahmen, um die Belastbarkeit ihrer IT-Systeme sicherzustellen. Im Falle einer Störung sind Informationen innerhalb einer angemessenen Frist wiederherzustellen oder wieder verfügbar zu machen.
- ⁷ **Auswertung:** Die Massnahmen zur Umsetzung der Informationssicherheit und des Datenschutzes werden periodisch überprüft und bei Bedarf angepasst; dafür werden diese Massnahmen im ISMS geführt. Ein Bericht über die aktuellen Massnahmen und geplanten Anpassungen erfolgt jährlich.
- ⁸ **Risikoorientierung:** Die Umsetzung der Informationssicherheit und des Datenschutzes erfolgt risikobasiert. Für jede Informationsbearbeitung gibt es intern eine/n Risikoeigner/in aus dem betroffenen Fachbereich, der/die Risiken abnehmen und tragen muss. Risiken sind stufengerecht zu tragen.
- ⁹ **Aktive Informationsbewirtschaftung:** Die PKBS verwaltet und bewirtschaftet Informationen über ihren ganzen Lebenszyklus hinweg aktiv. Datenfriedhöfe werden vermieden. Der Lebenszyklus umfasst dabei die Erstellung bzw. Sammlung, die Bearbeitung, die Archivierung gemäss den relevanten gesetzlichen Anforderungen sowie die Löschung und Vernichtung.
- ¹⁰ **Verantwortung:** Die Aufgaben, Kompetenzen und Verantwortlichkeiten werden innerhalb der PKBS eindeutig festgelegt und dokumentiert. Den Mitarbeitenden ist bewusst, dass sie in ihrem jeweiligen Bereich für die Einhaltung der Informationssicherheit und des Datenschutzes verantwortlich sind.
- ¹¹ **Sensibilisierung:** Die Mitarbeitenden werden regelmässig zu den Themen Informationssicherheit und Datenschutz geschult. Die PKBS fördert dabei eine positive Haltung zur Informationssicherheit und zum Datenschutz.

Art. 3 Umsetzung

¹ Der Verwaltungsrat delegiert die Kompetenz zum Erlass von Weisungen zur Umsetzung des vorliegenden Reglements, insbesondere im Bereich Informationsbewirtschaftung, Informationssicherheit, Geschäftsfortführungsmanagement und Datenschutz, an die Geschäftsleitung.

² Die Geschäftsleitung ist dafür verantwortlich, die notwendigen organisatorischen und prozeduralen Rahmenbedingungen zur Umsetzung des vorliegenden Reglements sowie der darauf basierenden Weisungen zu schaffen und deren Einhaltung sicherzustellen. Dazu gehört die Ernennung eines Chief Information Security Officers (CISO).

Art. 4 Berichterstattung

¹ Der CISO erstattet der Geschäftsleitung und dem Prüfungsausschuss jährlich Bericht.

² In diesem Zusammenhang informiert der CISO über die generelle Entwicklung der Informationssicherheit bei der PKBS, die Umsetzung des ISMS sowie über sicherheitsrelevante Vorkommnisse, Projekte und deren Auswirkungen. Er gibt bei Bedarf Empfehlungen ab. Diese stimmt er mit der Geschäftsleitung ab, handelt aber von dieser unabhängig.

Kapitel B Schlussbestimmungen

Art. 5 Inkrafttreten

¹ Das Reglement wurde am 30.08.2023 vom Verwaltungsrat verabschiedet und tritt am 01.09.2023 in Kraft.