

Cyber Security & Data Privacy Policy

Inhaltsverzeichnis

1	Unser Bekenntnis	2
2	Unsere Verantwortung.....	2
3	Unsere Cyber Security Grundsätze.....	2
4	Unsere Data Privacy Grundsätze.....	2
5	Unsere Management Systeme	3
6	Beschwerdemechanismus	3
7	Gültigkeit.....	3

1 Unser Bekenntnis

Der Schutz vor Cyber Bedrohungen und der Schutz von Sach-, Geschäfts- und Personendaten (Daten) ist für die BKW ein zentrales Anliegen. Diese Policy legt für die BKW und ihre Konzerngesellschaften die Bedeutung und den Stellenwert des Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie der Achtung der Privatsphäre und informationellen Selbstbestimmung fest. Sie ist für die Verarbeitung von Daten verbindlich und vermittelt die Grundsätze zur Verhinderung, Erkennung und Abwehr von Cyberangriffen.

2 Unsere Verantwortung

Die BKW verpflichtet sämtliche Organe und Mitarbeitenden im Umgang mit Daten, diese Policy zu respektieren und einzuhalten. Es werden die nötigen Voraussetzungen geschaffen und angemessenen Massnahmen getroffen, um die für die BKW geltenden rechtlichen Vorschriften und deren Einhaltung zu gewährleisten. Auch von Geschäftspartnern, Lieferanten und externen Mitarbeitenden erwartet die BKW, dass sie im Rahmen ihrer Zusammenarbeit mit der BKW im Sinne dieser Policy handeln.

Die BKW verfolgt das Ziel, dass sämtliche Daten, die sich in ihrem Einflussbereich befinden oder in ihrem Auftrag verarbeitet werden, mit technischen und organisatorischen Massnahmen und entsprechend ihrem Schutzbedarf geschützt werden und eine unrechtmässige oder unverhältnismässige Verarbeitung verhindert wird.

3 Unsere Cyber Security Grundsätze

Die BKW bekennt sich zu den folgenden Cyber Security Grundsätzen:

- **Wir betrachten die Cyber Security als grundlegenden Pfeiler für unseren Geschäftserfolg** und als integralen Bestandteil unserer Unternehmenskultur.
- **Wir verfolgen einen ganzheitlichen Ansatz für Cyber Security**, der die organisatorische, menschliche, physische und technische Dimension umfasst. Unsere Sicherheitsstrategie berücksichtigt alle Aspekte, von der Infrastruktur bis zu individuellem Verhalten, um eine umfassende und robuste Verteidigung gegen Cyberbedrohungen zu gewährleisten.
- **Unsere Cyber Security-Massnahmen basieren auf einer sorgfältigen Risikobewertung**. Wir identifizieren, bewerten und priorisieren kontinuierlich potenzielle Bedrohungen und Schwachstellen, um Ressourcen effizient einzusetzen und die grössten Risiken zu minimieren.
- **Unsere Sicherheitsprozesse und Vorgaben werden regelmässig überprüft und aktualisiert**, um sicherzustellen, dass sie den neuesten rechtlichen Anforderungen entsprechen.
- **Wir investieren in Schulungen und Massnahmen zur Bewusstseinsförderung**, um sicherzustellen, dass alle Mitarbeitenden die Bedeutung der Cyber Security verstehen und aktiv dazu beitragen, Sicherheitsrisiken zu minimieren.
- Cyber Security und damit zusammenhängende Aktivitäten befinden sich in einem sich ständig wandelnden Umfeld. Entsprechend verpflichten wir uns zur **kontinuierlichen Überprüfung und Verbesserung unserer Sicherheitsmassnahmen**, um den sich entwickelnden Bedrohungen einen Schritt voraus zu sein.

4 Unsere Data Privacy Grundsätze

Im Umgang mit Personendaten sowie die Nutzung von KI gelten die folgenden Data Privacy Grundsätze:

- **Wir verarbeiten Personendaten auf rechtmässige Weise**. Unsere Verarbeitungen sind transparent und für betroffenen Personen nachvollziehbar (Treu und Glauben).
- **Wir erheben Personendaten nur für festgelegte, eindeutige und legitime Zwecke**. Eine Weiterverarbeitung für andere Zwecke erfolgt nicht (Zweckbindung).
- **Wir erheben nur Personendaten, die für den jeweiligen Zweck notwendig sind**. Unrichtige

Daten werden gelöscht oder berichtigt (Datenminimierung).

- **Wir stellen sicher, dass Personendaten sachlich richtig und aktuell sind.** Eine längere Speicherung erfolgt nur unter bestimmten Bedingungen und Wahrung der Rechte der betroffenen Personen (Richtigkeit).
- **Wir speichern Personendaten nur so lange, wie es für den angestrebten Zweck notwendig ist.** In unseren Geschäftsbereichen definieren wir, wie lange wir Personendaten aufbewahren (Speicherbegrenzung).
- **Wir schützen Personendaten vor unbefugter oder unrechtmässiger Verarbeitung sowie vor unbeabsichtigtem Verlust.** Dies stellen wir durch angemessene Sicherheitsmassnahmen sicher (Integrität und Vertraulichkeit).
- **Wir sind uns unserer Rechenschaftspflicht bewusst und können die Datenschutzgrundsätze nachweisen.** Dies erfordert dokumentierte Verfahren und regelmässige Überprüfungen (Rechenschaftspflicht).

5 Unsere Management Systeme

Zur Sicherstellung einer konzernweiten Umsetzung und Einhaltung unserer Grundsätze betreibt die BKW im Bereich Cyber Security ein Information Security Management System (ISMS) und im Bereich Data Privacy ein Privacy Information Management System (PIMS). Die KI Governance der BKW sowie die Nutzung von KI-Anwendungen sind integraler Bestandteil des PIMS. Der Betrieb der Management Systeme erfolgt zentral jeweils durch Group Security oder Group Compliance und basiert auf etablierten, international anerkannten Best-Practice-Ansätzen sowie dem anwendbaren Datenschutzrecht.

Unsere Management Systeme beinhalten ineinandergreifende Prozesse zur Ermittlung des Sicherheitsniveaus, zur Umsetzung notwendiger Anforderungen sowie zur Prüfung, Optimierung und Berichterstattung der implementierten Massnahmen. Ziel unserer Management Systeme ist es, Risiken zu identifizieren und zu minimieren, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen und den Schutz der Privatsphäre sowie der informationellen Selbstbestimmung unserer Mitarbeitenden, Kundinnen und Kunden und Geschäftspartner zu gewährleisten.

Durch klare Vorgaben, regelmässige Überprüfungen und kontinuierliche Anpassungen streben wir eine robuste Cyber Security und Data Privacy Kultur an, die fest in allen Aspekten unserer Geschäftstätigkeit verankert ist. Dabei binden unsere Management Systeme unsere Mitarbeitenden, Werte, Vorschriften und Prozesse umfassend ein.

6 Beschwerdemechanismus

Die BKW stellt ein öffentlich zugängliches Hinweisgebersystem, die Integrity Line, zur Verfügung, über das Mitarbeitende, Geschäftspartner sowie externe Stakeholder vertraulich und anonym Hinweise auf potenzielle Verstösse gegen die Cyber Security & Data Privacy Policy einreichen können. Eingegangene Meldungen werden sorgfältig geprüft und gemäss den geltenden Reglementen bearbeitet. Der Schutz der Hinweisgebenden ist garantiert, sodass keine negativen Konsequenzen für diejenigen entstehen, die Verstösse melden. Die BKW arbeitet zudem eng mit Behörden, Lieferanten, Geschäftspartnern, Kundinnen und Kunden sowie weiteren externen Stakeholdern zusammen und übernimmt eine aktive Rolle zur Sicherstellung der Cyber Security und Data Privacy.

7 Gültigkeit

Diese Policy wurde vom Verwaltungsrat der BKW Gruppe verabschiedet und tritt am 11.11.2025 in Kraft.