

150.100

Verordnung über die Informationssicherheit und den Datenschutz

vom 22. April 2025

Kurzbezeichnung:

Informationssicherheitsverordnung

Sachliche Zuständigkeit:

Entwicklung und Ressourcen
Organisationsentwicklung

Stand: 22. April 2025

Verordnung über die Informationssicherheit und den Datenschutz

vom 22. April 2025

Der Stadtrat der Stadt Baden,

gestützt auf § 36 des Gemeindesgesetzes vom 19. Dezember 1978, § 2 und § 12 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 sowie §§ 4 und 5 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007

beschliesst:

I. Allgemeine Bestimmungen

§ 1 Zweck

Diese Verordnung definiert die Zuständigkeiten und Anforderungen in Bezug auf die Informationssicherheit und den Datenschutz der Einwohner- und Ortsbürgergemeinde Baden. Sie bildet die Grundlage für den sicheren Einsatz von Informatikmittel.

§ 2 Geltungsbereich

Diese Verordnung gilt für die Behörden und Kommissionen der Einwohnergemeinde sowie der Ortsbürgergemeinde Baden.

§ 3 Definitionen

1 Die folgenden Begriffe bedeuten:

- Wissen: Gesammelte Informationen über einen Sachverhalt (Tatsachen).
- Informationen: Teilmenge von Wissen, die von einem Absender einem Empfänger über einen Informationskanal vermittelt wird.
- Daten: Elemente (Werte und Inhalte), die eine Information formal darstellen. Sie werden durch verschiedene Symbole und Zeichen definiert, deren Bedeutung sich aus dem Kontext ergibt. Darunter fallen physische oder elektronisch gespeicherte Informationen (insbesondere Daten aus Verwaltungssystemen, Buchhaltung, Adressen, Textdokumente, Bilder, Grafiken, E-Mails).

- Informationssicherheit: Diese ergibt sich aus den technischen und organisatorischen Sicherheitsmassnahmen zum Schutz von Informationen und Daten. Der Begriff "Informationssicherheit" beinhaltet die Datensicherheit als Gesamtheit der integralen Sicherheit aller Daten.
- Datenschutz (im engeren Sinne): Schutz von Personendaten und besonders schützenswerten Personendaten.
- Datensammlung: Strukturierte Sammlung von Daten, die der Erfüllung einer bestimmten öffentlichen Aufgabe dienen.
- Datenklassifizierung: Nach ihrer Vertraulichkeit eingestufte und gekennzeichnete (klassifizierte) Daten. Die Vertraulichkeit ist abhängig vom Schutzbedarf.
- Schutzbedarf: Ein bestimmbares Mass an Schutz, das konkreten Daten aufgrund ihres Zwecks, der Art und dem Umfang der Bearbeitung sowie deren Bedeutung für die Verwaltung und den möglichen Gefahren für die Grundrechte und die Persönlichkeit von Personen zukommt.
- Informationsträger: Gegenständliche Träger von Informationen wie Papierdokumente, Printmedien, Bild- oder Tonträger sowie alle Arten von Datenträgern.
- Datenträger: Physische Speichermedien für digitale Daten als Informationsträger wie USB-Sticks, Speicherkarten, Harddisks.
- ICT: Informations- und Kommunikationstechnologie
- Anwendungen: Informatikgestützte Systeme und Computerprogramme zur Bearbeitung von Daten
- Informatik: Bezeichnet den organisatorischen und operativen Bereich, der für die Bereitstellung, den Betrieb und die Weiterentwicklung von ICT-Dienstleistungen zuständig ist. Diese kann innerhalb einer Organisation durch interne Einheiten umgesetzt oder ganz oder teilweise durch externe Dienstleister erbracht werden.
- Informatikmittel: Alle Geräte, Einrichtungen und Dienste (Hard- und Software) die der elektronischen Bearbeitung von Daten dienen.

2 Die technischen und organisatorischen Massnahmen bei der elektronischen Bearbeitung von Daten dienen folgenden Grundsätzen:

- Vertraulichkeit: Informationen sind nur für befugte Nutzende zugänglich.
- Integrität: Die bearbeitenden Daten sind vollständig und unverändert.
- Verfügbarkeit: Auf einen Service, Dienst, Daten, etc. kann innerhalb nützlicher und vereinbarter Frist zugegriffen werden.
- Zurechenbarkeit: Jede Aktion oder Veränderung an Daten kann eindeutig einer Person oder einem System zugeordnet werden.
- Nachvollziehbarkeit: Personen oder Systeme, die Daten erfassen, verändern oder löschen, sind jederzeit identifizierbar.

3 Die technischen und organisatorischen Massnahmen entsprechen den Ansprüchen gemäss §§ 4 und 5 VIDAG und sind in ISDS-Konzepten zu dokumentieren.

II. Zuständigkeit

§ 4 Der Stadtrat

Der Stadtrat verantwortet die Informationssicherheit und den Datenschutz. Er bezeichnet eine Person und deren Stellvertretung für die folgenden Funktionen, die für die Einhaltung der Informationssicherheit und des Datenschutzes zuständig sind:

- Der/die Chief Information Security Officer
- Der/die Datenschutz-Beauftragte/r

§ 5 Operative Leitung der Verwaltung

1 Die Verwaltungsleitung erlässt ausführende Weisungen und Richtlinien zum Vollzug dieser Verordnung.

2 In dienstlich begründeten Fällen, in welchen dies unumgänglich ist, genehmigt sie Zugriffe auf persönliche Laufwerke und Accounts von Nutzenden. Der Zugriff ist befristet und schriftlich zu dokumentieren sowie den betroffenen Nutzenden sobald als möglich bekannt zu geben.

3 Bei Missbrauchsverdacht lässt sie in begründeten Fällen die Protokollierungsdaten von Nutzenden analysieren. Die Auswertung und allfällige Zugriffe auf persönliche Laufwerke und Accounts sind zu befristen und schriftlich zu dokumentieren. Sie genehmigt die Weitergabe von Analysen an berechtigte Dritte.

§ 6 Chief Information Security Officer (CISO)

1 Der/die Chief Information Security Officer ist für die Informationssicherheit zuständig. Dies beinhaltet die Bewertung der Cyber-Compliance und Cybersicherheitslage sowie die Kommunikation der weiterführenden Weisungen und Richtlinien.

2 Er/Sie überwacht die Informationssicherheit mittels eines Informationssicherheits-Managementsystems und erstattet dem Stadtrat zuhanden des Geschäftsberichts sowie beim Vorliegen besonderer Vorkommnisse einen Bericht.

3 Weitere Zuständigkeiten sind:

- Die Festlegung von Informationssicherheitsverfahren wie die Anordnung von Kontrollmassnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel sowie die Durchführung von entsprechenden Auswertungen.
- Die Antragstellung bei der operativen Leitung der Verwaltung für Zugriffe in Notfällen und Analysen bei Missbrauchverdacht.
- Die Gewährleistung der kantonale Meldepflicht gemäss § 17c IDAG.
- Die Entwicklung einer umfassenden Sicherheitskultur in der Organisation und die Sensibilisierung der Mitarbeitenden für Informationssicherheit.

- Die Vertretung im Bereich Informationssicherheit in externen Gremien und Ausschüssen.
- Die Koordination und Überwachung der Prozesse und Einhaltung der Vorgaben sowie die Abnahme die Informationssicherheit- und der Datenschutzkonzepte (ISDS-Konzept).

§ 7 Datenschutzbeauftragte/r (DSB)

1 Die intern für den Datenschutz beauftragte Person sorgt für die Kontrolle und Einhaltung des Datenschutzes. Sie erstattet dem Stadtrat zuhanden des Geschäftsberichts sowie beim Vorliegen besonderer Vorkommnisse einen Bericht.

2 Im Rahmen ihrer Kontrolltätigkeit besteht das Recht auf Akteneinsicht innerhalb der Verwaltung, Auskünfte einzuholen oder sich Datenbearbeitungen vorführen zu lassen, soweit dies für die Prüfbliedenheit erforderlich ist.

3 Sie unterstützt die Abteilungs- oder Kompetenzbereichsleitungen bei Gesuchen um Zugang zu amtlichen Dokumenten oder bei Einsichts-, Auskunfts- oder Berichtigungersuchen.

§ 8 Abteilungs- und Kompetenzbereichsleitungen

1 Die Abteilungs- und Kompetenzbereichsleitungen sind für die Umsetzung der Informationssicherheit sowie des Datenschutzes in ihren Bereichen zuständig und gewährleisten die rechtmässige Datenbearbeitung.

2 Vor der Erstellung von neuen Datensammlungen haben sie sicherzustellen, dass die Zulässigkeitsvoraussetzungen an die Bearbeitung der Daten erfüllt werden.

3 Verwenden mehrere Organisationseinheiten gemeinsame Datensammlungen, wird in gemeinsamer Absprache bestimmt, wer die Verantwortung für diese trägt. Beim Entscheidung der Zuteilung ist die Sachnähe und das Nutzungspotential der beteiligten Organisationseinheiten zu berücksichtigen. Bei Uneinigkeit entscheidet die Verwaltungsleitung.

§ 9 Dateneigner/innen

Dateneigner/innen sind Personen, die für Daten durch Erstellung oder Zuweisung die Ressourcenverantwortung haben:

- Sie verwalten den gesamten Lebenszyklus der Daten, von der Erstellung über die Nutzung bis zur Archivierung und Löschung gemäss den gesetzlichen Anforderungen. Sie stellen den Schutz der Daten über deren gesamten Lebenszyklus sicher und ergreifen die erforderlichen technischen und organisatorischen Massnahmen.
- Sie klassifizieren die ihnen zugewiesenen Daten, basierend auf deren Sensitivität und Schutzbedarf.
- Sie dienen als Ansprechpersonen im laufenden Betrieb für die Nutzenden und sind die bewilligende Stelle für Zugriffs- und Klassifikationsänderungen. Sie überprüfen regelmässig die Zugriffsrechte auf die Daten.

- Sie führen bei Einführung oder Erweiterung einer informatikgestützten Anwendung zur Datenbearbeitung eine Schutzbedarfsanalyse und erstellen bei Notwendigkeit ein ISDS-Konzept. Ebenso prüfen sie die Erforderlichkeit, ob eine Datenschutzfolgeabschätzung notwendig ist.
- Sie stellen die Datensicherheit bei der Auftragsdatenbearbeitung durch Dienstleister sicher. Sie regeln vertraglich die Pflichten des Auftragnehmers gemäß § 12a VIDAG und kontrollieren die Einhaltung dieser Pflichten.

§ 10 Nutzende

- 1 Als Nutzende werden Personen bezeichnet, die berechtigterweise auf Leistungen von Informatikmittel der Einwohnergemeinde Baden zugreifen.
- 2 Sie dürfen über Daten der Stadt Baden in dem Masse verfügen, sie nutzen oder weitergeben, wie es für die Erfüllung der ihnen zugewiesenen Aufgaben erforderlich und zulässig ist.
- 3 Die Nutzenden halten sich an die vorgegebenen technischen und organisatorischen Massnahmen zum Schutze und zur Sicherung der Daten. Es besteht eine Meldepflicht gegenüber den direkten Vorgesetzten, falls Mängel bei der Bearbeitung von Daten festgestellt werden.

III. Grundsätze bei der Bearbeitung von Personendaten

§ 11 Bearbeitung von Personendaten

- 1 Personendaten dürfen nur in den gesetzlich vorgesehenen Fällen bearbeiten werden, insbesondere wenn sie für die Erfüllung der öffentlichen Aufgaben geeignet und erforderlich sind sowie der Verhältnismässigkeit genügen (Prinzipien der Datenvermeidung und der Datensparsamkeit).
- 2 Bei fehlender kommunaler Rechtsgrundlage für die Bearbeitung von Personendaten, sind Zweck, Umfang und Aufbewahrungsfrist durch Stadtratsbeschluss zu regeln. Handelt es sich um besonders schützenswerte Personendaten, bedarf es zwingend eines einwohnerrätlichen Reglement als gesetzliche Grundlage.

§ 12 Personendatensammlungen

- 1 Jede Datensammlung von Personendaten ist einem konkreten Dateneigner zugeordnet.
- 2 Es wird ein Register der Datensammlungen von Personendaten geführt, das jährlich im Rahmen des IKS auf seine Aktualität zu überprüfen ist.

IV. Schlussbestimmungen

§ 13 Inkrafttreten

Diese Verordnung tritt per 1. Mai 2025 in Kraft

§ 14 Aufhebung bisherigen Rechts

Diese Verordnung ersetzt die Verordnung über die Benutzung von Informatikmitteln und die Überwachung von Informationssicherheit vom 27. März 2017 (KER 150.100) sowie die Verordnung über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 22 Dezember 2008 (KER 150.101)

Baden, 22. April 2025

Stadtrat Baden

Stadtammann:

SCHNEIDER

Stadtschreiber:

KUBLI