

BEAUFTRAGTE FÜR ÖFFENTLICHKEIT UND DATENSCHUTZ

MERKBLATT

Stand: Oktober 2026

DATENSICHERHEITSKONZEPT – WAS IST DAS?!

1. Zielgruppe

Dieses Merkblatt richtet sich an öffentliche Organe des Kantons Aargau gemäss § 3 Abs.1 lit. c IDAG¹, die Personendaten bearbeiten oder bearbeiten lassen. Es soll diese bei der Umsetzung der gesetzlichen Anforderungen an die Datensicherheit unterstützen.

2. Was ist ein Datensicherheitskonzept?

Personendaten müssen durch angemessene technische und organisatorische Massnahmen (TOM) geschützt werden, um die Grund- und Persönlichkeitsrechte der von der Datenbearbeitung betroffenen Personen sowie die Sicherheit ihrer Daten zu gewährleisten.² Im Datensicherheitskonzept dokumentiert das öffentliche Organ welche technischen und organisatorischen Massnahmen umgesetzt wurden und wie deren Wirksamkeit überprüft wird.³

Man kann zwei Arten von Datensicherheitskonzepten unterscheiden. Das Grundsatzkonzept beschreibt das einheitliche Mindest-Sicherheitsniveau, das in der gesamten Organisation für alle Arbeitsplätze, Netzwerke und Datenbearbeitungen gilt. Weitergehende Massnahmen und Ausnahmen, beispielsweise für spezifische Fachanwendungen, werden in einem separaten Datensicherheitskonzept für bestimmte Systeme und Applikationen dokumentiert. Der Vorteil eines Grundsatzkonzeptes liegt darin, dass spätere Konzepte für spezifische Fachanwendungen oder Systeme nicht mehr von Grund auf neu erarbeitet werden müssen, sobald der Grundsatz einmal zentral dokumentiert ist. Sie verweisen auf den Grundsatz und beschreiben nur noch diejenigen Zusatzmassnahmen, die für das konkrete System zusätzlich nötig sind.

Zur Gewährleistung der Datensicherheit muss zwischen Massnahmen und Kontrollen unterschieden werden. Massnahmen stellen aufgrund technischer Konfigurationen und/oder organisatorischer Vorgaben sicher, dass die Daten geschützt sind; sie beschreiben, wie die Massnahmen konkret umgesetzt werden. Ergänzend werden durch die Kontrollen die Wirksamkeit der Massnahmen überprüft. Daher sind sowohl die Massnahmen als auch die Kontrollen im Datensicherheitskonzept zu dokumentieren.

¹ Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006; (SAR 150 700).

² § 12 IDAG i.V.m. § 4 VIDAG.

³ § 5 Abs. 1 VIDAG.

3. Auf welchen Grundlagen basiert ein Datensicherheitskonzept?

3.1. Der Schutzbedarf von Daten

3.1.1. Was sind Schutzziele und wofür sind sie gut?

Der Schutzbedarf beschreibt, wie stark Daten und Systeme geschützt werden müssen, weil die Verletzung der Schutzziele zu einer Beeinträchtigung für die betroffenen Personen (und die Organisation) führen kann. Je grösser die aus der Verletzung resultierende Beeinträchtigung, desto höher ist der Schutzbedarf.

Schutzziele sind grundlegende Ziele der Informations- und Datensicherheit. Sie beschreiben, was bei Informationen und Daten geschützt werden soll. Sie helfen, Risiken zu erkennen und diesen Risiken angepasste Massnahmen festzulegen. Die zentralen Schutzziele sind: Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit.

3.1.2. Welche Schutzziele gibt es und was bedeuten sie?

Schutzziel	Beschreibung / Zweck
Vertraulichkeit	Sie stellt sicher, dass nur berechnigte Personen Zugriff auf Daten erhalten und dass unbefugte Dritte diese nicht einsehen, abfangen oder ableiten können.
Integrität	Sie gewährleistet, dass Daten während ihrer gesamten Lebensdauer unverändert, vollständig und korrekt bleiben – es sei denn, eine berechnigte Person führt eine zulässige Änderung durch.
Verfügbarkeit	Sie garantiert, dass berechnigte Personen jederzeit sowie im erwarteten und benötigten Umfang Zugriff auf die benötigten Daten haben.
Nachvollziehbarkeit (inkl. Zurechenbarkeit)	Sie beschreibt die Fähigkeit, dass sämtliche Zugriffe, Vorgänge, Datenflüsse und Änderungen innerhalb eines Systems zurückverfolgt werden können, so dass erkennbar ist, wer wann was gemacht hat.

3.1.3. Welche Schutzstufen gibt es?

Abhängig vom konkreten Schutzbedarf der Daten werden die erforderlichen Massnahmen festgelegt. Der Schutzbedarf beschreibt, wie stark bestimmte Daten geschützt werden müssen. Er wird mithilfe der folgenden drei Schutzstufen einteilt: normal, hoch und sehr hoch.

Schutzstufen	Beschreibung / Zweck
Grundschutz (normaler Schutzbedarf)	Die Auswirkungen eines Vorfalls auf die Grund- und Persönlichkeitsrechte der betroffenen Personen sind gering oder gut überschaubar.
Hoher Schutzbedarf	Die Datenbearbeitung birgt ein erhöhtes Risiko für die Grund- und Persönlichkeitsrechte der betroffenen Personen. Die Auswirkungen eines Vorfalls können beträchtlich sein und deutlich nachteilige Folgen haben.
Sehr hoher Schutzbedarf	Die Auswirkungen eines Vorfalls können für die betroffenen Personen existentielle Folgen haben und ihre Freiheit oder Lebenssituation schwerwiegend beeinträchtigen.

3.2. Risikoanalyse

Für die Beurteilung des Schutzbedarfs ist das Risiko für die Grund- und Persönlichkeitsrechte der betroffenen Personen zu berücksichtigen, das mit einer Datenbearbeitung einhergeht. Es muss somit stets bedacht werden, welche Risiken eine konkrete Datenbearbeitung mit sich bringt und welche Folgen dies für die betroffenen Personen haben kann.

Im Gegensatz zur klassischen Informationssicherheit, bei der der Schutz der Institution und deren Werte (z.B. Vermeidung von finanziellen Schäden oder Betriebsausfällen) im Vordergrund steht, fokussiert das datenschutzrechtliche Risiko auf die möglichen negativen Auswirkungen für die betroffenen Personen. Eine klare Differenzierung zwischen diesen beiden Risikoschwerpunkten ist aus datenschutzrechtlicher Sicht zwingend erforderlich.

3.3. Welche Massnahmen sieht die VIDAG⁴ vor?

3.3.1. Massnahmen für die einzelnen Schutzziele

Die Einhaltung eines jeden Schutzziels erfordert spezifische Massnahmen. In § 4 Abs. 1 lit. a-j VIDAG ist eine nicht abschliessende Auflistung möglicher Massnahmenkategorien erfasst.

Die Mustervorlage des Datensicherheitskonzeptes verweist bei den einzelnen Kontrollen auf die einschlägigen Schutzziele.

3.3.2. Technische vs. organisatorische Massnahmen

Massnahmen können technischer oder organisatorischer Natur sein. Technische Massnahmen sind technisch implementierte Vorkehrungen und Sicherheitsfunktionen, mit denen Daten, Systeme und Prozesse geschützt oder abgesichert werden. Dahingegen sind organisatorische Massnahmen verbindliche Regeln, Abläufe und Zuständigkeiten innerhalb der Organisation, mit denen der sichere und korrekte Umgang mit Daten, Systemen und Prozessen gewährleistet wird.

Technische Massnahmen sind den organisatorischen in der Regel vorzuziehen, da es sich um automatisierte Massnahmen handelt, die aufgrund ihrer Implementierung weniger einfach umgangen werden können und somit weniger anfällig für Missbrauch sind. Mit organisatorischen Massnahmen können Defizite auf technischer Seite abgefangen werden. Sie erfordern jedoch die Mitwirkung und Sensibilisierung der Mitarbeitenden.

Die Kombination beider Arten von Massnahmen ist wichtig, um die Sicherheit der Bearbeitung personenbezogener Daten zu gewährleisten und die Grund- und Persönlichkeitsrechte der betroffenen Personen zu schützen.

4. Wie erstelle und pflege ich ein Datensicherheitskonzept?

Mit Hilfe der folgenden Checkliste sollen die zentralen Fragen gestellt werden, damit ein Datensicherheitskonzept erstellt werden kann.

4.1. Rollen- und Verantwortlichkeiten

Es ist klar zu bestimmen, wer welche Rolle mit welchen Zuständigkeiten und Verantwortlichkeiten im Zusammenhang mit der Einhaltung der datenschutzrechtlichen Vorgaben übernimmt.

4.2. Geltungsbereich klären

Es muss geklärt werden, wofür das Datensicherheitskonzept gilt. Es besteht die Möglichkeit ein allgemeines Datensicherheitskonzept zu erstellen, ein sogenanntes Grundsatzkonzept, das alle Massnahmen aufzeigt, die in der gesamten Organisation übergeordnet und unabhängig von einem bestimmten System umgesetzt sind.

Alternativ (oder ergänzend zum Grundsatzkonzept) kann sich ein Datensicherheitskonzept auf die umgesetzten Massnahmen eines bestimmten Systems oder eines bestimmten Services beziehen.

4.3. Daten erfassen und klassifizieren

Es muss ermittelt werden, welche Personendaten im Rahmen des festgelegten Geltungsbereichs bearbeitet werden. Zur Erstellung des Datensicherheitskonzeptes müssen nicht die einzelnen Daten

⁴ Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007; (SAR 150 711).

bzw. Datenkategorien klassifiziert werden, sondern die Gesamtheit der Daten innerhalb des relevanten Geltungsbereichs.

Dabei ist einerseits zu beurteilen, ob es sich um "normale" (vgl. § 3 Abs. 1 lit. d IDAG) oder besonders schützenswerte Personendaten (vgl. § 3 Abs. 1 lit. k IDAG) handelt. Andererseits ist zu bestimmen, ob es sich um öffentliche, interne, vertrauliche oder geheime Daten handelt.

4.4. Schutzbedarf bestimmen

Analog zur Klassifizierung muss auch der Schutzbedarf in Bezug auf die einzelnen Schutzziele (vgl. Ziff. 3.1.2 und 3.1.3) der im Rahmen des Geltungsbereichs bearbeiteten Daten bestimmt werden. Dabei ist zu prüfen, welche Folgen ein Verlust, eine Veränderung o.ä. der Daten hätte. Aus datenschutzrechtlicher Sicht sind primär die Folgen für die betroffenen Personen zu beurteilen. Auf dieser Grundlage ist festzulegen, ob ein normaler, hoher oder sehr hoher Schutzbedarf besteht.

4.5. Risiken analysieren

Es ist zu untersuchen, welche Gefahren für die Daten und Systeme bestehen. Dazu zählen beispielsweise Fehlbedienungen, technische Störungen, Cyberangriffe, Verlust von Geräten oder unberechtigte Zugriffe. In der Folge ist zu beurteilen welche Risiken durch diese Gefahren für die Grund- und Persönlichkeitsrechte der betroffenen Personen einhergehen. Für diese Beurteilung muss der Blickwinkel der betroffenen Personen eingenommen werden. Dabei ist beispielsweise an einen Kontrollverlust über die eigenen Daten, Rufschädigung, Diskriminierung oder Stigmatisierung zu denken.

4.6. Massnahmen definieren

Es ist festzulegen, mit welchen Massnahmen die erkannten Risiken reduziert werden sollen. Dazu gehören technische Massnahmen wie Zugriffsschutz, Verschlüsselung oder Datensicherungen sowie organisatorische Massnahmen wie klare Zuständigkeiten, interne Regeln und Schulungen.

4.7. Kontrollen inkl. Zuständigkeiten bestimmen

Die umgesetzten Massnahmen müssen regelmässig auf ihre Wirksamkeit überprüft werden. Eine solche Überprüfung inkl. Intervall muss für jede Massnahme bestimmt und ihre Durchführung dokumentiert werden. Ebenso ist festzulegen, wer für die Umsetzung der Massnahmen sowie deren Kontrolle zuständig ist.

4.8. Dokumentation erstellen

Alle wesentlichen Ergebnisse sind schriftlich festzuhalten. Das Datensicherheitskonzept soll nachvollziehbar darstellen, welche Massnahmen zur Gewährleistung der Datensicherheit umgesetzt sind und wie deren Wirksamkeit überprüft wird.

4.9. Aktualität sicherstellen

Das Datensicherheitskonzept ist in regelmässigen Abständen zu überprüfen und bei Bedarf anzupassen. Änderungen bei Systemen, Prozessen, rechtlichen Vorgaben oder Bedrohungen können dazu führen, dass neue Risiken entstehen oder bestehende Massnahmen angepasst werden müssen.