

§ 14 GKDZ-StV (Brandenburg) — Personelle, technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit

Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums der Polizeien der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt öffentlichen Rechts

Landesrecht Brandenburg

Stand: 21.08.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Die Anstalt hat alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Bestimmungen dieses Staatsvertrages und den nach § 12 Absatz 2 des Staatsvertrages geltenden Bestimmungen des Datenschutzrechts entsprechende Datenverarbeitung zu gewährleisten. Hierbei ist einheitlich derjenige Schutzbedarf für die Aufbewahrung und Übermittlung von Daten zugrunde zu legen, der gemessen an der Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik im Vergleich der Trägerländer als der höchste anzusehen ist. Die technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik sind entsprechend anzuwenden. Die Maßnahmen richten sich nach den im Einzelfall zu betrachtenden Risiken und dem jeweiligen Stand der Technik.

(2) Die Grundsätze der Datenminimierung, Datenvermeidung und Datensparsamkeit sind zu beachten. Hierzu gehört im Bereich der Kernaufgabe, dass der Umfang der Verarbeitung der im Auftrag erhobenen Daten und das Ausmaß ihrer Zugänglichkeit auf das unabdingbar Erforderliche beschränkt werden. Datenbestände und Kopien von Daten, die im Zuge der Verarbeitung temporär angelegt werden, sind zum frühestmöglichen Zeitpunkt zu löschen. Außerhalb des Bereichs der Kernaufgabe dürfen nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

(3) Die nach dem jeweiligen Stand der Technik zu treffenden personellen, technischen und organisatorischen Maßnahmen zur Datensicherheit sind auf der Grundlage eines Sicherheitskonzepts (Absatz 4) zu ermitteln und haben Folgendes zu bezwecken:

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (Datenträgerkontrolle),

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugangskontrolle),

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind

(Eingabekontrolle),

Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellung),

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

(4) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der Datenverarbeitung sind von der Anstalt die zu treffenden personellen, technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört eine Datenschutz-Folgenabschätzung hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Die datenschutzrechtliche Aufsichtsbehörde ist frühzeitig zu konsultieren. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 3 oder eine Modifizierung der Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden. Die Trägerländer bestimmen die Rahmenbedingungen der Risikoanalyse und des Sicherheitskonzepts in der Satzung der Anstalt näher.

(5) Die Datenverarbeitung muss so organisiert sein, dass bei der Verarbeitung, der Kenntnisaufnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

(6) Die Anstalt bestellt eine behördliche IT-Sicherheitsbeauftragte oder einen behördlichen IT-Sicherheitsbeauftragten.

(7) Zuständige datenschutzrechtliche Aufsichtsbehörde im Sinne des Absatzes 4 ist die oder der Sächsische Datenschutzbeauftragte. Diese oder dieser überwacht die Einhaltung der sich aus diesem Staatsvertrag und aus der Satzung der Anstalt ergebenden Anforderungen zur Informationssicherheit. Sie oder er stellt das Einvernehmen mit den anderen Datenschutzbeauftragten her, sofern die Kernaufgabe berührt ist.

Zitiervorschlag: § 14 GKDZ-StV (Brandenburg)

Quelle: bravors, abgerufen 21.08.2026

Nicht-amtliche Lesefassung — verbindlich ist das Gesetz- und Verordnungsblatt für das Land Brandenburg (landesrecht.brandenburg.de: <https://www.landesrecht.brandenburg.de>)

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/GKDZ-StV/14>