§ 16 BbgEGovG (Brandenburg) — Informationssicherheit, CERT

Brandenburgisches E-Government-Gesetz
Landesrecht Brandenburg
Stand: 01.08.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit zu gewährleisten. Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen und erstellen die erforderlichen Sicherheitskonzepte unter Einbeziehung der Geschäftsprozesse und Berücksichtigung der datenschutzrechtlichen Vorgaben.

(2) Zur Unterstützung und Beratung der an das Landesverwaltungsnetz Brandenburg angeschlossenen Behörden besteht für sicherheitsrelevante Vorfälle in IT-Systemen ein Computersicherheits-Ereignis- und Reaktionsteam (CERT). Es sammelt und bewertet die zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Landes erforderlichen Daten und analysiert dabei insbesondere Sicherheitslücken, Schadprogramme und Vorgehensweisen bei Angriffen auf die Informationstechnik des Landes. Die an das Landesverwaltungsnetz Brandenburg angeschlossenen Behörden melden dem CERT sicherheitsrelevante Vorfälle und übermitteln die für die Bewertung des Vorfalls notwendigen Informationen zu den von ihnen genutzten IT-Systemen und -Verfahren . Das CERT spricht Warnungen und Empfehlungen gegenüber den Behörden des Landes und der Kommunen aus und informiert die für Informationssicherheit zuständigen Stellen des Bundes und der Länder über ihm bekannt gewordene sicherheitsrelevante Vorfälle. Die Aufgaben des CERT werden durch den Brandenburgischen IT-Dienstleister wahrgenommen.

(3) Für die in Absatz 2 Satz 2 genannten Aufgaben dürfen vom CERT Protokolldaten, die beim Betrieb der Kommunikationstechnik des Landes anfallen, sowie die an den Schnittstellen der Kommunikationstechnik des Landes anfallenden Daten erhoben und ausschließlich automatisiert ausgewertet werden, soweit dies zur Verhinderung und Abwehr von Angriffen auf die Informationstechnik des Landes oder zum Erkennen und Beseitigen technischer Störungen oder Fehler erforderlich ist. Die Daten sind nach der Erhebung zu pseudonymisieren, soweit dies automatisiert möglich ist. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der gespeicherten Daten nur automatisiert erfolgt. Die automatisierte Auswertung erfolgt unverzüglich; danach sind die Daten sofort und spurenlos zu löschen. Abweichend von Satz 4 dürfen die Daten für längstens drei Monate gespeichert werden, wenn die Voraussetzungen nach Absatz 4 Satz 1 vorliegen.

(4) Eine über die automatisierte Auswertung nach Absatz 3 hinausgehende Verwendung von Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

diese ein Schadprogramm enthalten,

diese durch ein Schadprogramm übermittelt wurden oder

sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung zur Bestätigung oder Widerlegung des Verdachts erforderlich ist. Bei Bestätigung des Verdachts ist die weitere Verarbeitung der Daten zulässig, sofern dies

zur Abwehr des Schadprogramms,

zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder

zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung von Daten darf nur durch Bedienstete mit der Befähigung zum Richteramt angeordnet werden. Soweit nach den Sätzen 1, 2 oder Absatz 5 die Wiederherstellung des Personenbezugs von nach Absatz 3 Satz 2 pseudonymisierten Daten erforderlich oder diese aufgrund besonderer bundes- oder landesrechtlicher Rechtsvorschriften zulässig ist, muss sie durch die Leiterin

oder den Leiter des Brandenburgischen IT-Dienstleisters angeordnet werden. Anordnungen nach den Sätzen 4 und 5 sind zu protokollieren; die Protokollierung soll binnen drei Tagen erfolgen.

(5) Von einer Maßnahme nach Absatz 3 oder Absatz 4 betroffene Beteiligte eines Kommunikationsvorgangs sind spätestens nach dem Erkennen oder der Abwehr eines Schadprogramms oder der davon ausgehenden Gefahren zu benachrichtigen, wenn sie bekannt sind und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen.

(6) Die Regelungen zur Datenverarbeitung nach den Absätzen 3 und 4 sowie die Informationspflichten nach Absatz 5 gelten für die Verarbeitung der in Absatz 2 Satz 2 genannten Daten nur, sofern diese personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten beinhalten. Daten nach Satz 1 dürfen nicht weitergehend oder für andere Zwecke als nach den Absätzen 3 und 4 verarbeitet werden. Die Zulässigkeit ihrer Übermittlung an die Strafverfolgungsbehörden und Polizeien sowie andere Behörden oder Stellen des Bundes und der Länder richtet sich nach den für diese geltenden gesetzlichen Ermächtigungen. Von Übermittlungen nach Satz 3 sind Beteiligte eines Kommunikationsvorgangs entsprechend Absatz 5 zu unterrichten.

Einzelnorm