

# Rundschreiben des Senators für Finanzen Nr. 10/2026 – Private Nutzung des Internets an dienstlichen Infrastrukturen

Inkrafttreten: 22.04.2026

**Verteiler:** Alle Dienststellen

**Über Verteilerlisten:**

organisation@dienststelle.bremen.de

personal@dienststelle.bremen.de

dienststellenleitung@dienststelle.bremen.de

it-stelle@dienststelle.bremen.de

haushalt@dienststelle.bremen.de

**Adressatenkreis:**

alle Beschäftigten

**Bezug (Rechtsnorm):**

**EU:** NIS 2-Richtlinie, Cyber Resilience Act (CRA), Cybersecurity Act (CSA), Critical Entities Resilience (CER) Directive), etc.

**D:** BSI-Gesetz (BSIG), IT-Sicherheitsgesetz, NIS2-Umsetzungsgesetz (NIS2UmsuCG), KRITIS-Dachgesetz, etc.

**FHB:** Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen vom 1. Februar 2004, Rundschreiben der Senatorin für Finanzen Nr. 04/2019 - Addendum zur Internet-Richtlinie der Freien Hansestadt Bremen, Leitlinie für Informationssicherheit, Verwaltungsvorschrift zur Umsetzung der EU-NIS-2-Richtlinie („VV NIS2Ums FHB“)

Im Zuge der fortlaufenden Anpassung der Informations- und Cybersicherheitsmaßnahmen an die geltenden gesetzlichen und regulatorischen Vorgaben wird die Nutzung der dienstlichen IT-Infrastruktur der Freien Hansestadt Bremen neu geregelt.

Aufgrund der gestiegenen rechtlichen Anforderungen an die Informationssicherheit sowie der Verpflichtungen aus der Regulierung im Bereich der Cybersicherheit ist die entgeltliche und unentgeltliche private Nutzung der dienstlichen Zugänge zum Internet über dienstliche Endgeräte und Netzwerke ab dem 01.06.2026 nicht mehr zulässig.

Dies gilt, soweit für bestimmte Gerätegruppen keine anderweitigen Regelungen des zentralen IT-Managements der Freien Hansestadt Bremen beim Senator für Finanzen bestehen.

In diesem Zusammenhang besteht im Rahmen der gesetzlichen Vorgaben die Verpflichtung zur Einrichtung und zum Betrieb von Systemen zur Angriffserkennung sowie zur Aufzeichnung und Auswertung sicherheitsrelevanter Protokolldaten. Die Protokollierung erfolgt unter Beachtung der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie der einschlägigen datenschutzrechtlichen Bestimmungen.

Die Verarbeitung von Protokolldaten aufgrund der gesetzlichen Vorgaben dient ausschließlich der Gewährleistung der Informationssicherheit, der Erkennung und Abwehr von IT-Sicherheitsvorfällen sowie der Einhaltung gesetzlicher Anforderungen. Eine Leistungs- oder Verhaltenskontrolle der Beschäftigten ist hiermit nicht intendiert. Die Nutzung des Internets im dienstlichen Kontext ist weit gefasst und regelmäßig auch dann gegeben, wenn Recherchen im erweiterten beruflichen Kontext stattfinden. Dies können bspw. Aufrufe von Webseiten des Wetters, News, Restaurants, Krankenkassen, Informationen zu Ehrenämtern, Gewerkschaften, Mobilitäts- und Verkehrsangeboten etc. umfassen. Diese Aufzählung ist beispielhaft und nicht abschließend.

Die Auswertung der gewonnenen Protokolldaten erfolgt zweckgebunden im Rahmen der Cybersicherheit, verhältnismäßig und unter Wahrung der geltenden Datenschutzvorschriften. Eine Weitergabe der gewonnenen Informationen an Dritte erfolgt grundsätzlich nicht; eine Herausgabe kann ausschließlich auf Grundlage einer gesetzlichen Verpflichtung, insbesondere aufgrund eines richterlichen Beschlusses, erfolgen.

Mit Inkrafttreten der Neuregelung zum 01.06.2026 entfällt zugleich die bislang praktizierte entgeltliche Möglichkeit der privaten Internetnutzung. In der bisherigen Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen sollte die Nutzung der Internet-Dienste unter anderem die Medienkompetenz der Mitarbeiterinnen und Mitarbeiter erhöhen (Prinzip: „Internet für Alle“). Im Zuge der vergangen 20 Jahre wird davon ausgegangen, dass ein erforderliches Maß an Medienkompetenz nunmehr erlangt wurde.

Der derzeit über Performa Nord erhobene monatliche Betrag in Höhe von 2,00 € wird ab diesem Zeitpunkt nicht mehr über die Gehaltsabrechnungen eingezogen.

Die Maßnahme dient dem Schutz sensibler Daten, der Sicherstellung der Integrität und Verfügbarkeit der IT-Systeme sowie der rechtskonformen Ausgestaltung der IT-Nutzung.

Wir bitten alle Mitarbeitenden, sich ab dem genannten Stichtag entsprechend zu verhalten. Führungskräfte werden gebeten, die Umsetzung in ihren Organisationseinheiten sicherzustellen.

Für Rückfragen steht Ihnen das zentrale Informationssicherheitsmanagement bzw. der Landesbeauftragte für Informationssicherheit zur Verfügung.

## **Kontakt**

Der Senator für Finanzen

Referat 45

Rudolf-Hilferding-Platz 1

28195 Bremen

E-Mail: [informationssicherheit-fhb@finanzen.bremen.de](mailto:informationssicherheit-fhb@finanzen.bremen.de)