



Der Regierende Bürgermeister von Berlin
Senatskanzlei - Jüdenstraße 1, 10178 Berlin (Postanschrift)

Nur per Email

An die Senatsverwaltungen
die Bezirksverwaltungen
die Sonderbehörden

nachrichtlich

An die Berliner Beauftragte für
Informationssicherheit und Datenschutz

Geschäftszeichen (bitte angeben)

V C 13

Frau Laskowski

Tel. +49 30 90 26-1546

Anja.laskowski@senatskanzlei.berlin.de

Jüdenstraße 1, 10178 Berlin

30. Mai 2025

Rundschreiben RBm Skzl Nr. 1/2025

**Festsetzung gemäß § 21 Abs, 2 Nr. 4 EGovG Bln
zur Umsetzung der Richtlinie (EU) 2022/2555 (im Folgenden NIS-2-Richtlinie)**

Zur Umsetzung der NIS-2-Richtlinie für den Sektor öffentliche Verwaltung im Land Berlin werden in Ergänzung zu den Regelungen in § 23 EGovG Bln folgende Festsetzungen auf Grundlage des § 21 Absatz 2 Satz 2 Nr. 4 EGovG Bln getroffen:

**1. Zuständige Behörde nach Art. 8 Abs. 1 der Richtlinie für den Sektor öffentliche
Verwaltung**

1.1 Zuständige Behörde für die Aufsicht über die Umsetzung der Richtlinie für den Sektor öffentliche Verwaltung auf der Ebene der unmittelbaren Landesverwaltung im Land Berlin gemäß Art. 8 Abs. 1 der Richtlinie ist die für Informationssicherheit gemäß § 21 Abs. 2 Nr. 4 EGovG Bln zuständige Senatskanzlei, vertreten durch den oder die Beauftragten für Informationssicherheit des Landes.

1.2 Die zuständige Behörde stellt sicher, dass die Verpflichtungen aus der NIS-2-Richtlinie wirksam beaufsichtigt werden und die erforderlichen Maßnahmen getroffen werden. Sie handelt in dieser Funktion unabhängig.

Der Regierende Bürgermeister
von Berlin - Senatskanzlei -
Jüdenstraße 1, 10178 Berlin

berlin.de/senatskanzlei

@RegBerlin



Sprechzeiten Bürgerberatung:
Mo. und Di. von 9.00 - 15.00 Uhr
Mi. (nur telef.) von 9.00 - 15.00 Uhr
Do. von 9.00 - 18.00 Uhr
Fr. von 9.00 - 14.00 Uhr

Hinweis:

Außerhalb der Sprechzeiten nach
Terminvereinbarung

Verkehrsverbindungen:

U-Bahn Rotes Rathaus, S-Bahn
Alexanderplatz, Regionalbahn, Tram M 2,
M 4, M 5, M 6, Bus 100, 200, 248, 300

Informationen zum Datenschutz
erhalten Sie auf Anforderung oder
unter berlin.de/rbmskzl/datenschutz



1.3 Die zuständige Behörde arbeitet zur Erfüllung ihrer Aufgaben mit den zuständigen Behörden der anderen Länder, dem Bundesamt für Sicherheit in der Informationstechnik als zentrale Anlaufstelle, den Computer-Notfallteams, den Strafverfolgungsbehörden, den Datenschutzbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluffahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72; L 164 vom 23.6.2012, S. 18), geändert durch die Verordnung (EU) Nr. 18/2010 der Kommission vom 8. Januar 2010 (ABl. L 7 vom 12.1.2010, S. 3), und (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluffahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1; L 296 vom 22.11.2018, S. 41), geändert durch die Delegierte Verordnung (EU) 2021/1087 der Kommission vom 7. April 2021 (ABl. L 236 vom 5.7.2021, S. 1), den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44), geändert durch die Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 (ABl. L, 2024/1183, 30.4.2024), den gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1) zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die

elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36; L 334 vom 27.12.2019, S. 164), den gemäß der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164) zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Europäischen Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden zusammen.

1.4 Um die Umsetzung der Anforderungen aus der NIS-2-Richtlinie sicherzustellen, kann die oder der Beauftragte für Informationssicherheit des Landes die erforderlichen Auskünfte und die Überlassung von entsprechenden Unterlagen der staatlichen Stellen nach dem EGovG Bln verlangen.

1.5 Bei der Überprüfung festgestellte Verstöße einer staatlichen Stelle gegen Verpflichtungen, die eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) zur Folge haben können, teilt die oder der Beauftragte für Informationssicherheit des Landes unverzüglich der oder dem Berliner Datenschutzbeauftragten mit.

2. Wichtige Einrichtungen der öffentlichen Verwaltung

2.1 Als wichtige Einrichtung i. S. von Artikel 3 Abs. 2 Satz 1 i. V. m. Nr. 10 Alternative 2 Anhang I NIS-2-Richtlinie gilt gemäß Artikel 2 Abs. 2 Buchst. f Doppelbuchst. ii NIS-2-Richtlinie eine Einrichtung der öffentlichen Verwaltung des Landes Berlin, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte. Zur Ermittlung ist das vom IT-Planungsrat Bund/Länder in seiner 42. Sitzung am 03.11.2023 beschlossene Identifizierungskonzept (Beschluss 2023/39) heranzuziehen. Sofern der IT-Planungsrat Bund/Länder das Identifizierungskonzept aktualisiert, ist die jeweils aktuellste Fassung anzuwenden.

2.2 Wichtige Einrichtungen der öffentlichen Verwaltung können unbeschadet der bestehenden Verpflichtungen aus den Informationssicherheitsrichtlinien des Landes freiwillig Meldung machen über sie betreffende aktuelle wesentliche und wichtige Einrichtungen in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle.

3. Identifizierung wichtiger Einrichtungen

3.1 Die Senatsverwaltungen identifizieren für ihre jeweiligen Geschäftsbereiche auf der Grundlage des Identifizierungskonzeptes des IT-Planungsrates die betroffenen staatlichen Stellen und übermitteln der oder dem Beauftragten für Informationssicherheit des Landes für die von ihnen erstmals oder erneut identifizierten staatlichen Stellen

- a) den Namen der staatlichen Stelle,
- b) die Anschrift und die aktuellen Kontaktdaten der oder des Beauftragten für Informationssicherheit der staatlichen Stelle, einschließlich E-Mail-Adresse und Telefonnummer,
- c) die IP-Adressbereiche der staatlichen Stelle.

3.2 Die Identifizierung ist durch die obersten Senatsverwaltungen alle zwei Jahre zu überprüfen. Erstmalig erfolgt die Überprüfung zum 31.03.2027.

4. Computer-Notfallteam nach Art. 10 Abs. 1 der Richtlinie

4.1 Das Berlin-CERT nach § 23 Abs. 2 EGovG Bln nimmt die Aufgaben als Computer-Notfallteam (Computer Security Incident Response Team - CSIRT) i. S. von Artikel 10 Abs. 1 der NIS-2-Richtlinie auf der Ebene der unmittelbaren Landesverwaltung wahr.

4.2 Aufgaben des Berlin-CERT sind

- a) die Wahrnehmung der Aufgaben des Computer-Notfallteams nach Artikel 10 der Richtlinie (EU) 2022/2555 für die staatlichen Stellen und
- b) die Wahrnehmung der zentralen Meldestelle für Einrichtungen des Sektors öffentliche Verwaltung des Landes Berlin.
- c) Das Computer-Notfallteam sorgt für einen hohen Grad der Verfügbarkeit seiner Kommunikationskanäle, indem es punktuellen Ausfällen vorbeugt und mehrere

Kanäle bereitstellt, damit es jederzeit erreichbar bleibt und selbst mit Anderen Kontakt aufnehmen kann; es legt die Kommunikationskanäle genau fest und macht sie den wichtigen Einrichtungen nach Nummer 3.1 bekannt.

4.3 Durch das Computer-Notfallteam sind folgende Anforderungen zu erfüllen:

- a) Die Räumlichkeiten des Computer-Notfallteams und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet.
- b) Das Computer-Notfallteam muss über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, insbesondere um wirksame und effiziente Übergaben zu erleichtern.
- c) Das Computer-Notfallteam stellt die Vertraulichkeit und Vertrauenswürdigkeit seiner Tätigkeiten sicher.
- d) Das Computer-Notfallteam muss personell so ausgestattet sein, dass es eine ständige Bereitschaft seiner Dienste gewährleisten kann, und es muss sicherstellen, dass sein Personal entsprechend geschult ist.
- e) Das Computer-Notfallteam muss über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die Kontinuität seiner Dienste sicherzustellen.

4.4 Die Identität des Computer-Notfallteams, seine Aufgaben in Bezug auf wichtige Einrichtungen nach Nummer 3.1 sowie etwaige spätere Änderungen dieser Angaben sind der Europäischen Kommission unverzüglich zu notifizieren.

5. Meldung von erheblichen Sicherheitsvorfällen

5.1. Ein erheblicher Sicherheitsvorfall ist ein Sicherheitsvorfall,

- a) der schwerwiegende Betriebsstörungen der Dienste oder materielle Schäden für die betreffende Einrichtung verursacht hat oder verursachen kann oder
- b) Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

5.2 Wichtige Einrichtungen nach Nummer 3 sind verpflichtet, folgende Informationen an das Computer-Notfallteam zu melden:

- a) unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der

angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

- b) unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen Sicherheitsvorfall, in der die unter a) genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie ggf. die Kompromittierungsindikatoren angegeben werden.

5.3 Das Computer-Notfallteam meldet der zentralen Anlaufstelle nach Artikel 8 Abs. 3 NIS-2-Richtlinie unverzüglich grenzübergreifende erhebliche Sicherheitsvorfälle.

5.4 Wichtige Einrichtungen nach Nummer 3.1 können ergänzend zu den Meldungen nach Nummer 5.1 und unbeschadet der bestehenden Verpflichtungen aus den Informationssicherheitsrichtlinien des Landes zu Meldungen freiwillig Meldung machen über sie betreffende aktuelle

- a) sonstige Sicherheitsvorfälle sowie
- b) Beinahe-Vorfälle.

6. Aufgaben der Behördenleitungen

6.1. Behördenleitungen wichtiger Einrichtungen nach Nummer 3.1 sind für die Umsetzung der nach Nummer 4 zu ergreifenden Risikomanagementmaßnahmen verantwortlich.

6.2 Sie veranlassen die erforderlichen Maßnahmen und überwachen deren Umsetzung. Die oder der Beauftragte für Informationssicherheit des Landes meldet dem Bundesamt für Sicherheit in der Informationstechnik die identifizierten staatlichen Stellen erstmals zum 15.06.2025 und danach alle zwei Jahre.

6.3 Leiterinnen oder Leiter der staatlichen Stellen müssen regelmäßig an Schulungen zur Informationssicherheit teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich Informationssicherheit und deren Auswirkungen auf die von ihrer staatlichen Stelle erbrachten Dienste zu erwerben.

7. Cybersicherheitsstrategie des Landes Berlin nach Art. 7 Abs. 1-4 der Richtlinie

7.1 Es ist eine Cybersicherheitsstrategie des Landes Berlin zu erstellen, die die strategischen Ziele, die zur Erreichung der Ziele der NIS-2-Richtlinie erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält.

7.2 Die Cybersicherheitsstrategie ist der Europäischen Kommission innerhalb von drei Monaten nach ihrem Erlass zu notifizieren.

7.3 Die Cybersicherheitsstrategie ist regelmäßig, mindestens aber alle fünf Jahre, auf der Grundlage wesentlicher Leistungsindikatoren zu bewerten und erforderlichenfalls zu aktualisieren.

Mit freundlichen Grüßen



Martina Klement