

## Anwendung auf Bundesverwaltung

Die Anwendung des Teil 3, Kapitel 1 § 29 und Kapitel 3 wird auf weitere Bundesbehörden ausgedehnt

### § 29

#### Einrichtungen der Bundesverwaltung

[...]

(2) Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. ~~Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden.~~

[...]

### § 44

#### Vorgaben des Bundesamts

(1) Die Einrichtungen der Bundesverwaltung müssen Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindestanforderungen ergeben sich aus den BSI-Standards und dem IT-Grundschutz-Kompendium (IT-Grundschutz) sowie aus den die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) ~~als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen in den jeweils geltenden Fassungen. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht.~~ Die Mindeststandards ~~werden vom~~ legt das Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden ~~fest festgelegt und auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz und die Mindeststandards werden durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 3 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter.~~ Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.

~~(2) Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz wird durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 4 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.~~

(2) ~~(3)~~ Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 und Satz 2 Absatz 2 Satz 1 ist die Erfüllung der Vorgaben nach § 30 gewährleistet, soweit nicht die Europäische

Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen über die Mindestanforderungen aus Absatz 1 Satz 1 und ~~Satz 2 Absatz 2 Satz 1~~ hinausgehen. Falls eine Einrichtung des Bundes gleichzeitig ein Betreiber kritischer Anlagen ist und die Anforderungen des IT-Grundschutzes und der Mindeststandards den Anforderungen nach § 30 Absatz 9 und § 31 widersprechen, genießen letztere Vorrang.

(3) ~~(4)~~ Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 Satz 1 und ~~Satz 2 Absatz 2 Satz 1~~, stellt Hilfsmittel zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus

**Absätze 5 und 6 werden Absätze 4 und 5, im Übrigen unverändert**

#### **Begründung:**

**Zu § 29:** Alle Einrichtungen der Bundesverwaltung sind seit dem Kabinettsbeschluss „Umsetzungsplan Bund“ (UP Bund) 2017 sind zur Umsetzung des IT-Grundschutzes verpflichtet. Im Gesetzentwurf werden bislang nur die Bundesministerien und das Bundeskanzleramt zur Umsetzung verpflichtet, weil die NIS2-Richtlinie nur die Zentralregierung adressiert. Rückmeldungen zum Gesetzentwurf zeigen jedoch, dass hierdurch das Missverständnis entstehen kann, dass der IT-Grundschutz für den nachgeordneten Bereich weniger verbindlich ist. Um dieses Missverständnis zu vermeiden, sollten alle Einrichtungen der Bundesverwaltung gesetzlich zur Umsetzung des IT-Grundschutzes verpflichtet werden.

Auch der Bundesrechnungshof weist in seinem Bericht zum NIS2UmsuCG (Gz.: VII 4 – 0002698) darauf hin, dass gerade vor dem Hintergrund, dass die untergesetzliche Regelung bisher nicht ausgereicht hat, um den Defiziten bei der Umsetzung von Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit entgegenzuwirken, eine bundesweite gesetzliche Regelung notwendig ist, um Verbundrisiken für alle miteinander vernetzten Einrichtungen der Bundesverwaltung zu reduzieren. Es sollte ein gemeinsames, kohärentes und handhabbares Regelungsregime für die Informationssicherheit auf Bundesebene erreicht werden, um – insbesondere mit Blick auf die aktuelle Bedrohungslage – das Sicherheitsniveau in der Bundesverwaltung flächendeckend zu steigern.

Insbesondere auch sicherheitsrelevante Behörden wie das BSI oder das BKA sollten laut Gesetz den IT-Grundschutz einhalten müssen. Es sind laut Bundesrechnungshof vielfach gerade die Fachbehörden in den Geschäftsbereichen, deren unbedingte Handlungsfähigkeit durch den Ausfall von IT-Diensten im Krisen- und Katastrophenfall gefährdet wäre.

**Zu § 44:** Die Änderungen in § 44 ergeben sich aus der Änderung des § 29 Absatz 2, s. Begründung dort.