Gesamte Rechtsvorschrift für Informationssicherheitsverordnung, Fassung vom 28.07.2022

Langtitel

Verordnung der Bundesregierung über die Informationssicherheit (Informationssicherheitsverordnung, InfoSiV)
StF: BGBl. II Nr. 548/2003

Änderung

BGBl. II Nr. 67/2012
BGBl. II Nr. 131/2018
BGBl. II Nr. 268/2022

Präambel/Promulgationsklausel

Auf Grund des § 6 des Informationssicherheitsgesetzes, InfoSiG, BGBl. I Nr. 23/2002, wird verordnet:

Inhaltsverzeichnis

Text

Geltungsbereich

§ 1. Diese Verordnung gilt für die Dienststellen des Bundes mit Ausnahme der in § 1 Abs. 2 InfoSiG genannten Organe und Einrichtungen.

Klassifizierte Informationen

§ 2. (1) Klassifizierte Informationen im Sinne dieser Verordnung sind mit einem Klassifizierungsvermerk versehene Informationen und Materialien sowie Nachrichten, unabhängig von Darstellungsform und Datenträger, die aus den in § 2 Abs. 1 und 2 InfoSiG genannten Gründen eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen.

(2) Klassifizierte Informationen können insbesondere sein:

1. Schriftstücke;
2. Zeichnungen, Pläne, Karten, Lichtbildmaterial;

3. elektronisch verarbeitete Daten und deren Datenträger (z. B. E-Mail);
4. Ton- und Bildträger;
5. technische Geräte, technische Systeme und deren Teilkomponenten.

Klassifizierungsstufen

§ 3. (1) Klassifizierte Informationen sind zu qualifizieren als

1. EINGESCHRÄNKT (E), wenn die unbefugte Weitergabe der Informationen den in Art. 20 Abs. 3 B-VG genannten Interessen zuwiderlaufen würde,
2. VERTRAULICH (V), wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist,
3. GEHEIM (G), wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde,
4. STRENG GEHEIM (SG), wenn die Informationen geheim sind und überdies ihr bekannt werden eine schwere Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen wahrscheinlich machen würde.

(2) Die Klassifizierung, Deklassifizierung sowie die Herabstufung einer Information erfolgt durch ihren Urheber. Die Deklassifizierung ist schriftlich festzuhalten. Empfänger einer klassifizierten Information sind von der Deklassifizierung zu informieren.

Informationssicherheitsbeauftragte

§ 4. (1) Als Informationssicherheitsbeauftragte und deren Stellvertreter dürfen ausschließlich Personen bestellt werden, die einer für die höchste im Ressortbereich angewendeten Klassifizierungsstufe erforderlichen Überprüfung gemäß § 3 Abs. 1 InfoSiG unterzogen wurden.

(2) Die Informationssicherheitsbeauftragten haben die Aufgabe, dafür Sorge zu tragen, dass in ihrem Wirkungsbereich

1. die Informationssicherheit durch organisatorische Maßnahmen gewährleistet ist,
2. die Überwachung der Einhaltung des InfoSiG, dieser Verordnung und der sonstigen Informationssicherheitsvorschriften sichergestellt ist,
3. die jährliche Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen gesichert ist,
4. die Unterweisungen gemäß § 6 nachweislich durchgeführt werden,
5. die erforderlichen Aufzeichnungen gemäß § 5 Abs. 1 und § 12 geführt werden,
6. die Regelungen für Zugang, Übermittlung und Verwahrung von klassifizierten Informationen umgesetzt werden,
7. der Verdacht strafbarer Handlungen im Zusammenhang mit der Informationssicherheit an die Ressortleitung gemeldet wird,
8. bei festgestellten Mängeln auf die unverzügliche Behebung des Mangels hingewirkt wird,
9. Verstöße gegen Sicherheitsvorschriften, deren Kenntnis über den eigenen Wirkungsbereich hinaus von Interesse sein kann, der Informationssicherheitskommission berichtet werden und
10. von der Informationssicherheitskommission verlangte Berichte erstattet werden.

Zugang zu klassifizierten Informationen

§ 5. (1) Der Zugang zu klassifizierten Informationen darf nur unter den Voraussetzungen des § 3 InfoSiG gewährt werden, wobei über die Personen, die tatsächlich Zugang zu Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM erhalten haben, über den Zeitpunkt des Zuganges und über die Bezeichnung der Information entsprechende Aufzeichnungen zu führen sind **(**Muster: **Anlage 1).**

(2) Einem Bediensteten des Bundes darf der Zugang nur gewährt werden, wenn

1. dies für die Erfüllung seiner dienstlichen Aufgaben erforderlich ist,
2. der Bedienstete nachweislich gemäß § 6 über den Umgang mit klassifizierten Informationen unterwiesen wurde und
3. bei Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG oder eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG durchgeführt wurde.

(3) Sonstigen Personen darf der Zugang nur gewährt werden, wenn

1. dies für die Ausübung einer im öffentlichen Interesse gelegenen Tätigkeit erforderlich ist,
2. die Voraussetzungen des Abs. 2 Z 2 und 3 vorliegen und der von der zuständigen Dienststelle vorgesehene Schutzstandard gewährleistet wird und
3. sie sich zur Geheimhaltung von klassifizierten Informationen auch nach Beendigung der Tätigkeit verpflichtet haben.

(4) In jedem Ressortbereich ist durch geeignete innerorganisatorische Maßnahmen sicherzustellen, dass der Zugang zu klassifizierten Informationen für Bedienstete nur im Rahmen der Erfüllung ihrer dienstlichen Aufgaben, nach nachweislicher Unterweisung und - soweit vorgesehen - nach Abschluss einer Sicherheitsüberprüfung bzw. Verlässlichkeitsprüfung möglich ist. Dies gilt sinngemäß auch für den Zugang sonstiger Personen.

(5) Ein Bediensteter des Bundes darf den Zugang zu klassifizierten Informationen nur dann suchen, wenn er sich vergewissert hat, dass die Voraussetzungen nach Abs. 2 gegeben sind.

Unterweisung

§ 6. (1) Die Unterweisung nach § 5 Abs. 4 hat jedenfalls über das InfoSiG, diese Verordnung, die jeweils gültigen völkerrechtlichen und unionsrechtlichen Verpflichtungen, allfällige schriftlich erlassene Durchführungsregelungen des Ressorts sowie über die Geheimhaltungspflichten und Sanktionen bei Verstößen gegen diese zu erfolgen.

(2) Die Unterweisung dient der Sensibilisierung für Bedrohungen der Sicherheit von klassifizierten Informationen und soll sicherstellen, dass die vorgesehenen Sicherheitsstandards eingehalten und alle Sicherheitsverletzungen, selbst ein Verdacht auf solche, gemeldet werden. Sie hat vor der Eröffnung des Zugangs zu klassifizierten Informationen zu erfolgen und ist regelmäßig zu wiederholen. Der Nachweis der Unterweisung ist schriftlich festzuhalten (Muster: Anlage 2).

Übermittlung klassifizierter Informationen

§ 7. (1) Vor der Übermittlung von klassifizierten Informationen ist durch Prüfung im Einzelfall oder durch Einhaltung der hiefür vorgesehenen generellen Regelungen sicherzustellen, dass beim Empfänger die Voraussetzungen des InfoSiG und dieser Verordnung gegeben sind.

(2) Im Rahmen der Amtshilfe dürfen klassifizierte Informationen nur übermittelt werden, wenn das ersuchende Organ dies ausdrücklich begehrt und belegt, dass es den erforderlichen Schutzstandard und die vom Gesetz und von der Verordnung verlangten personellen Voraussetzungen zu gewährleisten vermag. Der Informationssicherheitsbeauftragte ist von der beabsichtigten Weitergabe in Kenntnis zu setzen.

(3) Dokumente der Klassifizierungsstufe EINGESCHRÄNKT sind im verschlossenen Kuvert und Dokumente der Klassifizierungsstufe VERTRAULICH oder höher in einem doppelten undurchsichtigen verschlossenen Kuvert zu übermitteln, wobei nur am inneren Kuvert die Klassifizierungsstufe einschließlich der Anschrift des Empfängers anzugeben und eine Empfangsbestätigung beizulegen ist (Muster: **Anlage 3**). Vermerke am äußeren Kuvert dürfen nicht auf den Inhalt schließen lassen.

(4) Für die Übermittlung von klassifizierten Informationen der Stufe STRENG GEHEIM ist die schriftliche Zustimmung des Urhebers erforderlich.

(5) Die Übermittlung von klassifizierten Informationen an Drittstaaten oder internationale Organisationen sowie an einen in einem Drittstaat niedergelassenen Auftragnehmer ist nur mit vorheriger schriftlicher Zustimmung des Urhebers erlaubt, sofern nicht völkerrechtliche oder unionsrechtliche Verpflichtungen die Weitergabe ohne eine solche Zustimmung vorsehen.

(6) Klassifizierte Informationen sind auf folgende Arten zu übermitteln:

1. Mündliche Übermittlung: Bei Besprechungen mit einem Inhalt ab der Klassifizierungsstufe VERTRAULICH hat der Besprechungsleiter dafür Sorge zu tragen, dass die Teilnehmer entsprechend sicherheitsüberprüft oder verlässlichkeitsgeprüft und belehrt sind. Aufzeichnungen sind zu klassifizieren. Bei der mündlichen Darlegung von Informationen, die als GEHEIM oder STRENG GEHEIM klassifiziert sind, sind Maßnahmen gegen Abhören zu treffen.
2. Persönliche Übermittlung: Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH, die persönlich ausgehändigt werden, sind gegen Empfangsbestätigung zu übergeben. Die Übermittlung innerhalb eines Gebäudes hat durch Personen zu erfolgen, die für die betreffende Klassifizierungsstufe ermächtigt sind, und in einem verschlossenen Kuvert, auf dem nur der Name des Empfängers aufscheint; die Entgegennahme ist mit Empfangsbestätigung zu quittieren. Innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe dürfen

Informationen bis zur Stufe STRENG GEHEIM in einem verschlossenen undurchsichtigen Kuvert befördert werden.

3. Übermittlung durch Zustelldienste (Post oder private Kurierdienste), militärische und diplomatische Kuriere und diplomatisches Gepäck:

a) Klassifizierte Informationen der Stufe EINGESCHRÄNKT dürfen durch die Post oder private Kurierdienste, militärische und diplomatische Kuriere, diplomatisches Gepäck oder Handgepäck einer Person, die entsprechend unterwiesen ist, übermittelt werden. Über die Erfüllung der Schutzmaßnahmen entscheidet die Informationssicherheitskommission.

b) Klassifizierte Informationen der Stufe VERTRAULICH dürfen

– durch die Post oder private Kurierdienste innerhalb der EU-Mitgliedsstaaten sowie in Staaten, mit denen ein bilaterales Abkommen gemäß § 14 InfoSiG oder eine sonstige völkerrechtliche Vereinbarung mit Regelungen über die Übermittlung von solchen Informationen auf diesem Wege besteht, übermittelt werden, sofern die Dienste über geeignete Schutzmaßnahmen verfügen, über deren Erfüllung die Informationssicherheitskommission entscheidet;

– mit diplomatischem Gepäck oder durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte Information übermittelt, zumindest bis VERTRAULICH überprüft und hierzu ermächtigt ist (Muster: **Anlage 4**).

c) Klassifizierte Informationen der Stufe GEHEIM dürfen

– im Inland durch die Post oder private Kurierdienste übermittelt werden, sofern sie über geeignete Schutzmaßnahmen verfügen, über deren Erfüllung die Informationssicherheitskommission entscheidet;

– durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte Information übermittelt, zumindest bis GEHEIM überprüft und ermächtigt ist (Muster: **Anlage 4**);

– in Ausnahmefällen durch das diplomatische Gepäck übermittelt werden, wenn keine andere Übermittlungsmöglichkeit zur Verfügung steht.

d) Klassifizierte Informationen der Stufe STRENG GEHEIM dürfen durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte Information übermittelt, bis STRENG GEHEIM überprüft und ermächtigt ist (Muster: **Anlage 4**).

Kennzeichnung

§ 8. (1) Klassifizierte Informationen sind eindeutig und gut erkennbar durch die in § 3 oder in völkerrechtlichen oder unionsrechtlichen Regelungen festgelegten Kennzeichnungen kenntlich zu machen.

(2) Bei Informationen in Papierform sind das Datum, die Geschäftszahl, der Urheber und auf jeder Seite die Kennzeichnung oben und unten und eine Seitennummerierung anzubringen. Falls erforderlich können weiters angebracht werden:

1. eine Urheberidentifikation;
2. weitere Informationen, wie z. B. Verteilungseinschränkungen (auf jeder Seite);
3. ein Zeitpunkt für die Herabstufung der Klassifizierung.

(3) Bei Informationen in elektronischer Form ist der Dateiname mit der betreffenden Klassifizierungsstufe zu versehen.

(4) Auf der ersten Seite von Dokumenten der Klassifizierungsstufe VERTRAULICH oder höher sind alle Anhänge und Anlagen aufzulisten.

Elektronische Verarbeitung und Übermittlung klassifizierter Informationen

§ 9. (1) Die Verarbeitung von klassifizierten Informationen in Informations- und Kommunikationssystemen bedarf besonderer Sicherungsmaßnahmen, die abhängig sind von

1. der Klassifizierungsstufe,
2. dem Grad der Abstrahlsicherheit der Geräte,
3. der Art und dem Ausmaß der Vernetzung,
4. den Speichermöglichkeiten und
5. den örtlichen Gegebenheiten.

(2) Informationen ab der Klassifizierungsstufe VERTRAULICH dürfen auf allen Informations- und Kommunikationssystemen verarbeitet werden, sofern eine Akkreditierung durch die Informationssicherheitskommission vorliegt. Die spezifischen Voraussetzungen (Anforderungen sowie Maßstab und Grad der Detaillierung) sind dabei in Abstimmung mit der Informationssicherheitskommission festzulegen. Für Informations- und Kommunikationssysteme, die Informationen der Klassifizierungsstufe EINGESCHRÄNKT verarbeiten, sind je nach Art und Umfang des Systems (Risikostufe bzw. Komplexität und Vernetzung) die Vorgaben der Informationssicherheitskommission zu beachten. In jedem Fall sind Maßnahmen zur Identifizierung und Protokollierung von Zugriffen vorzusehen. Bei Informations- und Kommunikationssystemen, die der Erfüllung von Aufgaben des Bundesheeres gemäß Art. 79 Abs. 1 B-VG dienen, nimmt diese Aufgaben die vom Bundesminister für Landesverteidigung und Sport für seinen Wirkungsbereich bestimmte Zertifizierungsstelle wahr.

(3) Informationen ab der Klassifizierungsstufe VERTRAULICH, die auf elektronischen Geräten verarbeitet werden, sind so zu schützen, dass von den Informationen über elektromagnetische Abstrahlung nicht unbefugt Kenntnis erlangt werden kann (TEMPEST-Sicherheitsvorkehrungen).

(4) Bei der Übermittlung von klassifizierten Informationen auf elektronischem Wege sind besondere Schutzvorkehrungen, insbesondere die der jeweiligen Klassifizierungsstufe entsprechende Verschlüsselung, sowie die Vorgaben der Informationssicherheitskommission zu beachten. Ungeachtet dieser Anforderung können in Notsituationen spezielle Verfahren oder spezielle technische Konfigurationen nach Maßgabe der Informationssicherheitskommission angewendet werden. Die Übermittlung von klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH ist gemäß den Vorgaben der Informationssicherheitskommission unter Einsatz qualifizierter Signatur bzw. bei automatischer Übermittlung mit technisch gleichwertigen Sicherheitsanforderungen zu protokollieren.

(5) Die Zusammenschaltung eines Informations- und Kommunikationssystems, in dem klassifizierte Informationen verarbeitet werden, mit anderen Systemen bedarf entsprechender Schutzmaßnahmen.

Dienstpflichten

§ 10. (1) Die jeweiligen Dienstvorgesetzten haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche Mitarbeiter Zugang zu klassifizierten Informationen haben. Sie haben weiters dafür Sorge zu tragen, dass dieser Zugang nur unter den Voraussetzungen der bezughabenden Vorschriften erfolgt.

(2) Personen, denen Zugang zu klassifizierten Informationen gewährt wird, sind zur Verschwiegenheit über die ihnen dadurch zur Kenntnis gelangten Informationen und zur Einhaltung der vorgesehenen Schutzstandards verpflichtet. Sie sind insbesondere dazu verpflichtet, jeden Verdacht einer Spionagetätigkeit und ungewöhnliche Umstände im Zusammenhang mit der Sicherheit von Informationen umgehend dem Informationssicherheitsbeauftragten zu melden. Andere gesetzliche Meldepflichten bleiben unberührt.

(3) Der Verlust von klassifizierten Informationen ist unverzüglich dem Dienststellenleiter und dem Informationssicherheitsbeauftragten zu melden. Diese haben alle erforderlichen Maßnahmen zur Auffindung der Informationen, Vermeidung allfälliger weiterer Nachteile und Aufklärung des Vorfalls zu treffen. Diese Maßnahmen sind in geeigneter Weise festzuhalten. Vom Verlust ist auch jene Stelle zu verständigen, von der diese Information stammt.

Administrative Behandlung

§ 11. (1) Klassifizierte Geschäftsstücke der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM sind in einem hiefür vorgesehenen Register (Muster: Anlage 1) zu verbuchen. Dabei ist jedes Geschäftsstück mit einer eigenen Geschäftszahl zu versehen, der Name des Dokuments, die Ausfertigungsnummer, sein Datum und die jeweilige Klassifizierungsstufe anzugeben.

(2) Die auf klassifizierte Systeme bezogenen Verwaltungssysteme sind in geeigneter Weise gegen unbefugten Zugriff und Verlust zu schützen.

Registrierung von klassifizierten Informationen

§ 12. (1) Der Eingang und Ausgang jedes als VERTRAULICH oder höher klassifizierten Dokuments ist zu registrieren, wobei im Register neben den Angaben gemäß § 11 Abs. 1 der Urheber, der Zeitpunkt des Einlangens, der Zeitpunkt der Übermittlung und die Verwaltungseinheit festzuhalten sind (Muster: **Anlage 1**). Jede Phase des Umlaufs der klassifizierten Informationen ist in geeigneter Weise aufzuzeichnen.

(2) Registerbücher für die Klassifizierungsstufen VERTRAULICH und GEHEIM sind zumindest mit der Klassifizierungsstufe EINGESCHRÄNKT, Registerbücher für die Klassifizierungsstufe STRENG GEHEIM mit der Klassifizierungsstufe GEHEIM zu versehen.

(3) Abs. 1 und 2 sind sinngemäß auch bei elektronischer Registrierung zu erfüllen.

Verwahrung von klassifizierten Informationen

§ 13. (1) Informationen sind der jeweiligen Klassifizierungsstufe entsprechend in den Diensträumen gesichert zu verwahren und dürfen nur bei unabdingbaren dienstlichen Notwendigkeiten aus diesen verbracht werden.

(2) Zum physischen Schutz klassifizierter Informationen sind folgende entsprechend abgesicherte Bereiche einzurichten:

1. Verwaltungsbereiche: Bereiche mit sichtbarer äußerer Abgrenzung zur Ermöglichung der Kontrolle von Personen und Fahrzeugen, die nur von Personen betreten werden dürfen, die eine Ermächtigung erhalten haben. Bei allen anderen Personen ist eine ständige Begleitung bzw. gleichwertige Kontrolle sicherzustellen.
2. Besonders geschützte Bereiche: Bereiche mit sichtbarer und geschützter Abgrenzung mit vollständiger Eingangskontrolle (Ausweiskontrolle oder Kontrolle nach Identifikationsklasse 2 gemäß ÖNORM EN 50133-1:2003 „Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen“ vom 1.11.2003) und Ausgangskontrolle (Kontrolle nach Identifikationsklasse 0 gemäß ÖNORM EN 50133-1:2003), die nur von sicherheitsüberprüften, verlässlichkeitsgeprüften oder speziell ermächtigten Personen unbegleitet betreten werden dürfen. Bei allen anderen Personen ist eine ständige Begleitung bzw. gleichwertige Kontrolle sicherzustellen.
3. Besonders geschützte Bereiche mit Abhörschutz: Bereiche, die zusätzlich technisch abgesichert und mit Einbruchsmeldeanlagen ausgestattet sind. Nicht zugelassene Kommunikationsverbindungen oder elektronische Ausrüstung oder Kommunikationsgeräte sind verboten. Im Zuge der Eingangskontrolle sind Personen, die den Bereich betreten, auf die Mitnahme verbotener Geräte zu kontrollieren. Regelmäßige Inspektionen und technische Überprüfungen sind durchzuführen.

(3) Die Auswahl geeigneter Maßnahmen zur physischen Absicherung der Räumlichkeiten erfolgt auf der Grundlage einer Einschätzung der Bedrohungslage durch die zuständigen Behörden, wobei Verwaltungsbereiche und besonders geschützte Bereiche zu unterscheiden sind. Derartige Maßnahmen oder eine Kombination von diesen können sein:

1. Zutrittssperre;
2. Einbruchmeldeanlage;
3. Zugangskontrolle;
4. Sicherheitspersonal;
5. Videoüberwachung;
6. Sicherheitsbeleuchtung;
7. sonstige geeignete physische Maßnahmen.

(4) Informationen gemäß § 2 Abs. 2 Z 1, 2 und 4 aller Klassifizierungsstufen sind in versperrten Behältnissen zu verwahren. Dabei sind für die Klassifizierungsstufe EINGESCHRÄNKT Büromöbel, für VERTRAULICH, GEHEIM bzw. STRENG GEHEIM Wertbehältnisse entsprechend der Zuordnung durch die Informationssicherheitskommission zu verwenden.

(5) Für Verwaltungsbereiche und besonders geschützte Bereiche sind entsprechende Dienstanweisungen festzulegen.

(6) Verfahren über die Verwaltung der Schlüssel und Codes sind vom zuständigen Informationssicherheitsbeauftragten festzulegen. Diese Verfahren müssen Schutz vor unbefugtem Zugang gewähren.

Kopien und Übersetzungen

§ 14. (1) Werden Kopien und/oder Übersetzungen von Dokumenten der Klassifizierungsstufe VERTRAULICH, GEHEIM oder STRENG GEHEIM angefertigt, so ist dies in geeigneter Weise festzuhalten. Jede Kopie ist durch einen geeigneten Zusatz, der auf jeder Seite zu vermerken ist, zu individualisieren. Die Anfertigung von Kopien und Übersetzungen von Informationen der Klassifizierungsstufe STRENG GEHEIM durch Empfänger ist nur mit vorheriger schriftlicher Zustimmung des Urhebers erlaubt. Kopien dürfen ausschließlich unter der unmittelbaren Verantwortung des jeweiligen Leiters der Organisationseinheit und unter Kennzeichnung als Kopie angefertigt werden.

(2) Dokumente der Klassifizierungsstufe VERTRAULICH, GEHEIM oder STRENG GEHEIM dürfen nur von solchen Personen kopiert, abgeschrieben, übersetzt, gescannt, archiviert oder verarbeitet werden, die die Voraussetzungen des § 5 Abs. 2 erfüllen.

Vernichtung von klassifizierten Informationen

§ 15. (1) Der Bestand an klassifizierten Informationen ist möglichst gering zu halten. Werden Informationen nicht mehr benötigt, sind sie mittels geeigneter Verfahren unter Beachtung internationaler und nationaler Vorgaben zu vernichten. Registrierungspflichtige Dokumente werden von der zuständigen Registratur auf Anweisung des Leiters der aufbewahrenden Stelle vernichtet und die Registrierungsinformationen entsprechend aktualisiert. Die Vernichtung von Informationen der Klassifizierungsstufen GEHEIM oder höher hat unter Anwesenheit eines Zeugen zu erfolgen, der über eine Sicherheitsüberprüfung oder Verlässlichkeitsprüfung der entsprechenden Klassifizierungsstufe verfügen muss, und ist im Protokoll durch Unterschrift festzuhalten (Muster: **Anlage 5**). Die Vernichtung von Datenträgern hat nach den von der Informationssicherheitskommission genehmigten Verfahren zu erfolgen.

(2) Der Leiter der aufbewahrenden Stelle einer Information hat festzulegen, wann eine klassifizierte Information zu vernichten ist. Erfolgt keine Festlegung, so ist die Information nach sieben Jahren zu skartieren.

Maßnahmen zum Schutz des Austausches klassifizierter Informationen für Galileo PRS

§ 16. (1) In Österreich nimmt die Agenden der Galileo Public Regulated Service Behörde (PRS Behörde) gemäß Beschluss 1104/2011/EU über die Regelung des Zugangs zum öffentlichen regulierten Dienst, der von dem weltweiten Satellitennavigationssystem bereitgestellt wird, das durch das Programm Galileo eingerichtet wurde, ABl. Nr. L 287 vom 04.11.2011 S. 1, das Bundeskanzleramt wahr.

(2) Die gemäß § 8 InfoSiG beim Bundeskanzleramt eingerichtete Informationssicherheitskommission ist über alle Belange, die die Informationssicherheit in diesem Zusammenhang betreffen, regelmäßig zu informieren und zu hören.

Kontrolle

§ 17. Das System der Informationssicherheit ist durch den jeweiligen Informationssicherheitsbeauftragten einmal jährlich nachweislich zu überprüfen oder überprüfen zu lassen. Dabei ist insbesondere die Vollständigkeit der Aufzeichnungen, die Sicherheit der Behältnisse, das Schlüsselsystem und die Sicherungsmaßnahmen von Kommunikations- und Informationssystemen einer Überprüfung zu unterziehen. Liegen Informationen der Klassifizierungsstufe GEHEIM oder STRENG GEHEIM vor, so ist eine vollständige Überprüfung der Vorgänge des abgelaufenen Jahres vorzunehmen.

Inkrafttreten

§ 18. § 16 in der Fassung BGBl. II Nr. 268/2022, tritt mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft.

Anlage 1

Register

Register haben jedenfalls die nachstehenden Informationen zu enthalten. Sie können zentral oder dezentral, für Entnahmen, Weiterleitungen und Verteilungen gesondert geführt werden.

Evidenzliste	
Dokumentenname	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang	…….. …… Datum Unterschrift
Eigene Geschäftszahl	
Übermittlung an	…….. …… Datum Unterschrift oder Beilage der Empfangsbestätigung

Vernichtung	…….. …… Datum Unterschrift

Anlage 2

Nachweis der Unterweisung

Hiemit wird bestätigt, dass

Herr/Frau .....

gemäß § 6 der Informationssicherheitsverordnung eine Ausgabe des geltenden Textes des InfoSiG, der Informationssicherheitsverordnung und der nachfolgend aufgelisteten Vorschriften erhalten hat, über die sich daraus ergebenden Pflichten und über die Folgen von Verstößen dagegen informiert wurde.

.....	.....	.....
(Datum)	(Unterschrift des Unterweisenden)	(Unterschrift des Unterwiesenen)

Liste:

. . . . .

Anlage 3

Empfangsbestätigung

Innerhalb von zehn Tagen zurück an den Absender!

Empfangsbestätigung

Der Empfänger ..... bestätigt den Empfang von
Dienststempel

Stückzahl	Absender (Dienststempel)	GZ, Ausfertigungsnummer	Beilagen

..... , am .....
Ort Datum

....
Name in Druckschrift Unterschrift

Anlage 4

Kurierbescheinigung

....
(Dienststelle) (Datum)

Kurierbescheinigung

....
(Amtstitel/Dienstgrad) (Vor- und Zuname) (GebDatum)

Ausweis Nr.: .....

ist berechtigt, vom (am) ..... bis .....

Klassifizierte Informationen EINGESCHRÄNKT *)
VERTRAULICH *)
GEHEIM *)
STRENG GEHEIM *)

für .....
(Dienststelle)

anzunehmen bzw. zu übergeben.

Der Leiter:

.....
(Name, Amtstitel/Dienstgrad)

*) Nichtzutreffendes streichen

Anlage 5

Vernichtungsprotokoll

Folgendes klassifiziertes Dokument wurde vernichtet:

Dokumentenname	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang	

Art der Vernichtung:

Name des Zeugen in Druckschrift:

Organisationseinheit:

..... (Datum)

..... (Unterschrift)