# Erläuterungen

## Allgemeiner Teil

**Hauptgesichtspunkte des Entwurfs:**

Internationale Entwicklungen sowie Lücken im nationalen Geheimschutzsystem erfordern die Anpassung der gesetzlichen Regelung zum Schutz klassifizierter Informationen und Umsetzung völkerrechtlicher Vereinbarungen zur sicheren Verwendung von Informationen. Diese können wie folgt zusammengefasst werden:

**1. Internationale Entwicklungen**

In einer Phase des digitalen Wettrüstens, erhöhter Terroralarmbereitschaft in Europa, neuer militärischer Konflikte und veränderter geopolitischer Bedingungen spielt der Schutz klassifizierter Informationen eine entscheidende Rolle. Besonders betroffen sind Inhalte mit sicherheitspolitischer Relevanz, jene der Krisenprävention und Krisenbewältigung, aber auch Informationen, die die strategische Unabhängigkeit der heimischen Wirtschaft garantieren sollen. Die merkbare Zunahme von Cyber- und Hackerangriffen auf staatliche Einrichtungen und Unternehmen verdeutlicht das wachsende Interesse feindlich gesinnter Akteure und damit auch die Notwendigkeit, diese Informationen angemessen zu schützen. All diese Entwicklungen führen zu einem signifikanten Anstieg klassifizierter Informationen sowohl auf nationaler als auch auf internationaler Ebene. Ebenso kommt es zu vermehrten Abschlüssen von Abkommen zum gegenseitigen Austausch und Schutz klassifizierter Informationen zwischen Österreich und anderen Staaten oder auch Internationalen Organisationen, welche das Vorhandensein einer einheitlichen Rechtsgrundlage bedingen, um das gegenseitige Vertrauen in das Geheimschutzsystem zu sichern.

**2. Lücken im nationalen Geheimschutzsystem**

In Österreich wurden national und international klassifizierte Informationen in unterschiedlichen Rechtsregimen mit unterschiedlicher Rechtsqualität (InfoSiG, Informationssicherheitsverordnung, Geheimschutzordnung, etc.) geschützt. Zudem waren Vorgaben des Geheimschutzes nicht direkt auf Dritte, wie Unternehmen und Forschungseinrichtungen, anwendbar.

Die vorliegende Novelle des Informationssicherheitsgesetzes konsolidiert den internationalen und nationalen Geheimschutz und erweitert den Anwendungsbereich auf Dritte, an die klassifizierte Informationen weitergegeben werden. Dadurch wird ein einheitlicher und lückenloser Schutzstandard im Geheimschutz geschaffen, das bestehende System vereinfacht und der Standard der Informationssicherheit erhöht. Dies schafft Rechtssicherheit, stärkt den Wirtschaftsstandort Österreich und fördert das Vertrauen der Öffentlichkeit in die Bundesverwaltung.

Die Stärkung des nationalen Geheimschutzes unterstützt darüber hinaus die im Bundes-Krisensicherheitsgesetz normierte Stärkung der staatlichen Resilienz in Österreich.

**Kompetenzgrundlage:**

Die Zuständigkeit des Bundes zu dieser Gesetzesnovelle ergibt sich aus Art. 10 Abs. 1 Z 2 B-VG („äußere Angelegenheiten“), Art. 10 Abs. 1 Z 6 („Strafrechtswesen“), Art. 10 Abs. 1 Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit einschließlich der ersten allgemeinen Hilfeleistung, jedoch mit Ausnahme der örtlichen Sicherheitspolizei“), Art. 10 Abs. 1 Z 8 („Angelegenheiten des Gewerbes und Industrie“) und Art. 10 Abs. 1 Z 16 („Einrichtung der Bundesbehörden und Dienstrecht“).

**Kosten:**

Es sind keine Kosten für Bund, Länder und Gemeinden zu erwarten.

## Besonderer Teil

**Zu Z 1 (Langtitel):**

Die Änderung des Langtitels dieses Bundesgesetzes erfolgt in Hinblick auf das nunmehr geänderte Ziel des § 1, wonach neben international auch national klassifizierte Informationen umfasst sind.

**Zu Z 4 (§ 1):**

Ziel dieses Bundesgesetzes gemäß Abs. 1 ist der einheitliche Schutz sowohl national als auch international klassifizierter Informationen sowie die Umsetzung völkerrechtlicher Vereinbarungen zum Schutz dieser Informationen. Dadurch wird ein lückenloser Schutzstandard im österreichischen

Geheimschutzsystem geschaffen. Zudem wird der Anwendungsbereich des Gesetzes konkretisiert und umfasst nunmehr auch Dritte, an die klassifizierte Informationen im Rahmen dieses Gesetzes weitergegeben werden. Unter dem Begriff „Dritte“ im Sinne dieses Bundesgesetzes sind sowohl jene juristischen Personen, die im Kompetenzbereich des Bundes liegen und in den Anwendungsbereich der industriellen Sicherheit im Sinne der §§ 11ff fallen, als auch jene natürlichen Personen, an die innerhalb dieser juristischen Personen klassifizierte Informationen weitergegeben werden, zu verstehen. Durch die Ausweitung des Anwendungsbereiches wird Rechtssicherheit für die Betroffenen geschaffen und der Grundstein für die Vorbereitung österreichischer Unternehmen zur Teilnahme an national und international klassifizierten Aufträgen gelegt. Diese werden durch die gesetzlichen Vorgaben direkt gebunden, sodass keine Notwendigkeit zum Abschluss anderweitiger vertraglicher Vereinbarungen zur Einhaltung der gesetzlichen Bestimmungen besteht.

Der Terminus des „Zugangs“ wird in Hinblick auf die Richtung des Informationsflusses durch „Weitergabe“ ersetzt. Dadurch wird klargestellt, dass der Übergeber der Information die Verantwortung für die Erfüllung der Voraussetzungen des § 3 durch den Empfänger trägt. Es besteht somit auch nach Erfüllung der Voraussetzungen des § 3 durch den Empfänger kein Recht auf die klassifizierte Information. Insbesondere wird die dienstliche Notwendigkeit im Sinne des § 3 Abs. 1 Z 1 und das Kriterium der Erfüllung beruflicher Pflichten im Sinne des § 12 Abs. 3 („Need-To-Know“) immer vom Übergeber der Information und nicht vom Empfänger bestimmt. Bei der Bestimmung des Need-To-Know sind geltende kompetenzrechtliche Vorgaben heranzuziehen.

Darüber hinaus wird mit der Änderung der Begrifflichkeit eine deutliche Abgrenzung zum Informationsfreiheitsgesetz – IFG, BGBl. I Nr. 5/2024, geschaffen, das den „Zugang zu Informationen“ regelt. Die Terminologie wurde im gesamten Gesetz dahingehend angepasst.

Der Ausnahmetatbestand des Abs. 2 betreffend die Voraussetzungen der Weitergabe klassifizierter Informationen an bestimmte Organe und Einrichtungen wird gemäß internationaler Praxis konkretisiert. Nunmehr sollen nicht mehr die Institutionen als solche erfasst sein, sondern lediglich jene Personen, die das entsprechende Amt bekleiden und klassifizierte Informationen für die Erfüllung der ihnen übertragenen verfassungsgemäßen Aufgaben benötigen. Personen, die vertraglich für diese Institutionen tätig werden, sind somit von der Ausnahmeregelung nicht erfasst. Diese Konkretisierung hat somit nicht die Zugangsbeschränkung der Institution selbst zu den klassifizierten Informationen zum Gegenstand. Vielmehr soll dadurch sichergestellt werden, dass innerhalb der Organisation nur jene Personen, die die Voraussetzungen für die Weitergabe klassifizierter Informationen erfüllen, mit der Bearbeitung der entsprechenden klassifizierten Sachverhalte betraut werden. Die Entscheidung der Erfüllung der Voraussetzungen des § 3 Abs. 1 Z 2 und 3 InfoSiG hat daher stets im eigenen Wirkungsbereich der Organisation zu erfolgen. Was die Erweiterung der Voraussetzung des § 3 Abs. 1 Z 1 InfoSiG auf den Hilfsapparat der jeweiligen Institution betrifft, ist dies auf keinen Fall als Einschränkung der Weitergabe von klassifizierten Informationen an diese zu verstehen. Die Rechte staatlicher Organe bleiben somit davon unberührt. Dies gilt insbesondere für Institutionen wie den Rechnungshof und die Volksanwaltschaft, deren Aufgabenerfüllung einfach- oder verfassungsgesetzlich begründet ist.

Der Verweis auf den Bereich des Nationalrates und des Bundesrates wurde gestrichen und in Abs. 3 klargestellt, dass sich die Weitergabe klassifizierter Informationen gemäß § 3 sowie der entsprechende Umgang in diesem Bereich nach dem Informationsordnungsgesetz richten. Derartige Voraussetzungen zur Weitergabe klassifizierter Informationen an Amtsträger können sich jedoch aus völkerrechtlichen Vereinbarungen ergeben. Die Begriffe Richter und Staatsanwälte umfassen alle Richter und Staatsanwälte im Sinne der Artikel II beziehungsweise IIa des RStDG.

Die Möglichkeit der Weitergabe klassifizierter Informationen an die genannten Personen ohne die Erfüllung der entsprechenden gesetzlichen Voraussetzungen gemäß § 3 enthebt diese jedoch nicht von der Einhaltung der national sowie international vorgesehenen Schutzstandards. Diese sind neben § 4 insbesondere der Informationssicherheitsverordnung zu entnehmen. Klassifizierte Informationen müssen dabei über ihren gesamten Lebenszyklus, insbesondere bei deren Entstehung, Bearbeitung, Aufbewahrung, Besprechung, Vervielfältigung bis hin zu deren Vernichtung, entsprechend den Vorgaben, abhängig von der jeweiligen Klassifizierungsstufe, geschützt werden.

Die Streichung des Abs. 3 dient der Rechtsbereinigung.

**Zu Z 4 (§ 2):**

Die Zuordnung schutzbedürftiger Informationen zu Klassifizierungsstufen bedarf klarer Kriterien, da an jede Klassifizierung sowohl Beschränkungen der Weitergabe als auch Handlungsanweisungen zur Sicherstellung des Schutzes der Informationen geknüpft sind. Dafür ist das Ausmaß des Schadens bei Preisgabe der Information zu berücksichtigen. Hilfestellung und Orientierung soll dabei eine Klassifizierungsrichtlinie bieten, die von der Informationssicherheitskommission (§ 8) erarbeitet wird.

Die Zuordnung einer Information zu einer Klassifizierungsstufe manifestiert sich durch die Vornahme verpflichtender Schutzmaßnahmen, welche in der Informationssicherheitsverordnung beschrieben werden.

Die Definitionen der Klassifizierungsstufen wurden angepasst, um eine Einheitlichkeit mit jenen des § 4 Abs. 1 InfOG zu schaffen. Die dort angeführten Interessen entsprechen jenen des Art. 22a Abs. 2 Bundes-Verfassungsgesetz (B-VG), der den Umfang der Informationsfreiheit definiert. Der Verweis in der Definition der Klassifizierungsstufe EINGESCHRÄNKT auf den „besonderen organisatorischen Schutz“ impliziert eine deutliche Hürde für die Klassifizierung einer Information. Somit soll eine Überklassifizierung, insbesondere bei der untersten Klassifizierungsstufe EINGESCHRÄNKT, vermieden werden. Selbiges gilt auch für die in den übrigen Klassifizierungsstufen beschriebenen Schwellen. Diese sind daher so zu verstehen, dass eine Klassifizierung nur bei absoluter Notwendigkeit vorgenommen werden darf. Im Zusammenspiel zwischen InfoSiG und IFG besteht daher ein Äquivalent zu den nicht-öffentlichen Informationen im Sinne des InfOG. Die Bewertungen einer Information nach InfoSiG und IFG sind allerdings getrennt voneinander durchzuführen.

Die Zuordnung einer Information zu einer bestimmten Klassifizierungsstufe hat immer durch den Urheber der Information oder auf dessen Veranlassung zu erfolgen und ist dabei auf das notwendige Ausmaß zu beschränken. Darüber hinaus ist auch regelmäßig zu prüfen, ob die Voraussetzungen der Klassifizierung weiterhin bestehen.

Urheber klassifizierter Informationen kann ausschließlich ein gesetzlich eingerichtetes Organ des Bundes sein. Dadurch ist gewährleistet, dass nach Ausscheiden einzelner Personen die Urheberschaft weiter bestehen bleibt. Dieses Konzept sowie die Terminologie entsprechen internationaler Praxis. Der Begriff darf daher nicht mit dem Urheber im Sinne des Urheberrechts verwechselt werden. Demnach ist Urheber stets jene Person, die die Letztverantwortung im Bereich der jeweiligen Dienststelle trägt. Der Begriff des Urhebers entspricht auch jenem des § 3 Abs. 5 InfOG. Im Bereich der Bundesministerien ist somit das oberste Organ Urheber einer im jeweiligen Wirkungsbereich erzeugten klassifizierten Information. Die tatsächliche Einstufung der Information kann in diesem Fall immer nur von jenen Bediensteten vorgenommen werden, die eine Ermächtigung zur selbständigen Behandlung gem. § 10 BMG besitzen. Unabhängig von der Dienststelle müssen diese Personen zusätzlich, je nach Klassifizierungsstufe, die Weitergabevoraussetzungen des § 3 Abs. 1 Z 2 und 3 erfüllen und die Auswirkungen einer Preisgabe der betroffenen Information abschätzen können, um eine entsprechende Zuordnung vornehmen zu können. Im Zuge von klassifizierten Aufträgen zwischen der Republik Österreich und der Industrie ist es möglich, dass auch Dritte derartig schutzbedürftige Informationen erzeugen. In einem solchen Fall erfolgt jedoch die Klassifizierung auf Veranlassung des jeweiligen Organs (als Urheber), sodass Dritte in keinem Fall Urheber klassifizierter Informationen im Sinne dieses Bundesgesetzes sein können.

Bei der Behandlung klassifizierter Informationen, die eine Person in Österreich auf Grund völkerrechtlicher Vereinbarungen, wie beispielsweise Abkommen zum gegenseitigen Austausch und Schutz klassifizierter Informationen gemäß § 14, erhalten hat, erfolgt keine neuerliche Bewertung des potentiell eintretenden Schadens bei der Preisgabe der Information. Diese sind den Klassifizierungsstufen in Abs. 2 in Übereinstimmung mit der in der völkerrechtlichen Vereinbarungen enthaltenen Äquivalenztabelle zuzuordnen und unter Berücksichtigung der jeweiligen Schutzstandards und Handlungsanweisungen so wie national klassifizierte Informationen zu schützen.

**Zu Z 4 (§ 3):**

Durch die Änderung des Wortlauts in Abs. 2 wird klargestellt, dass die Weitergabe klassifizierter Informationen an Dritte ausschließlich im Rahmen der industriellen Sicherheit unter Berücksichtigung der Voraussetzungen der §§ 11 und 12 zu erfolgen hat. Der vorgesehene Schutzstandard des bisherigen § 3 Abs. 1 Z 2 lit. c wird somit ebenfalls im Rahmen des Verfahrens zur Erlangung einer Sicherheitsunbedenklichkeitsbescheinigung beurteilt.

Abs. 3 bezieht sich auf jene Fälle, in welchen bei der Weitergabe klassifizierter Informationen von der Erfüllung der Voraussetzung der Sicherheitsüberprüfung nach den §§ 55 bis 55b Sicherheitspolizeigesetz – SPG, BGBl. Nr. 566/1991, bzw. der Verlässlichkeitsprüfung nach den §§ 23 und 24 Militärbefugnisgesetz – MBG, BGBl. I Nr. 86/2000, abgegangen werden kann. Dies ist nur in besonders dringlichen Ausnahmefällen möglich, in denen die Verarbeitung der klassifizierten Informationen nicht ohne die Möglichkeit eines größeren Schadens aufgeschoben werden kann und keine Alternativen zur Verfügung stehen. Die Inanspruchnahme einer solchen Ausnahme ist zudem nicht möglich, wenn der betroffenen Person in der Vergangenheit bereits die Sicherheitsüberprüfung beziehungsweise die Verlässlichkeitsüberprüfung entzogen wurde oder diesbezügliche Gründe vorliegen, welche die nationale Sicherheit gefährden könnten. Die ressortinternen Zutrittsregelungen bleiben durch diese Bestimmung unberührt. Die Genehmigung der außerordentlichen Weitergabe muss von der

zuständigen Führungskraft für den jeweiligen Bundesminister vorgenommen werden. Dadurch ist auch die Weitergabe im Ausnahmefall durch Dritte nicht möglich. Der schriftliche Vermerk ist zur Nachvollziehbarkeit in der zuständigen Registratur gemäß § 12 InfoSiV zu hinterlegen. Bei international klassifizierten Informationen ist eine derartige Weitergabe auchder nationalen Sicherheitsbehörde zu melden, um bestehenden Berichtspflichten nachkommen zu können.

Wie im gesamten § 3, ist auch hier eine gemäß § 2a Staatsschutz- und Nachrichtendienst-Gesetz – SNG, BGBl. I Nr. 5/2016, durchgeführte Vertrauenswürdigkeitsprüfung einer Sicherheitsüberprüfung nach SPG gleichzusetzen.

**Zu Z 5 (§ 6):**

In Z 2 wird der Begriff „Umgang“ durch den Begriff „Handhabung“ ersetzt, um den gesamten Lebenszyklus einer klassifizierten Information zu erfassen. Durch die angefügte Z 10 wird der Bundesregierung im Rahmen der Informationssicherheitsverordnung zusätzlich auferlegt, Vorgaben zu erlassen, die bei der Erstellung von Klassifizierungsrichtlinien durch die jeweiligen Dienststellen des Bundes zu beachten sind.

**Zu Z 7 (§ 9):**

Die Terminologie bzw. die Strafdrohung des § 9 Abs. 1 werden an den § 310 StGB angepasst. Dieser sieht für die Verletzung der dienstrechtlichen Geheimhaltungsverpflichtung eine Freiheitsstrafe von bis zu drei Jahren vor. Um das Verhältnis zwischen den Strafbestimmungen in Bezug auf die Verletzung von Verschwiegenheitspflichten zu klären, wurde eine klare Subsidiarität der Strafbestimmung des InfoSiG geschaffen. Der bisherige Abs. 2 wird dadurch obsolet.

Da durch die Tathandlung ein in § 2 Abs. 2 Z1 genanntes Interesse gefährdet sein muss, wird die Weitergabe einer fälschlicherweise klassifizierten Information keine Strafbarkeit auslösen.

Der neue Abs. 2 erfasst jenen Personenkreis, dem auch der Schutz des Redaktionsgeheimnisses gemäß § 31 Mediengesetz zukommt. Die verwendeten Begriffe entsprechen den Legaldefinitionen des § 1 Mediengesetz, die nach der Judikatur des Obersten Gerichtshofes auch für andere Rechtsmaterien gelten (vgl. ausdrücklich OGH MR 1989, 128). Der Begriff Medieninhaber umfasst z. B. auch Blogger.

Vorbildbestimmung des vorgeschlagenen § 9 Abs. 2 ist § 18 Abs. 2 InfOG. Dieser ist in seiner Formulierung in Hinblick auf den angesprochenen Täterkreis nicht klar: „Beteiligte im Sinne von § 12 Strafgesetzbuch“ sind nämlich nicht nur der – offenbar gemeinte – Beitragstäter (§ 12 dritter Fall StGB), sondern auch der Bestimmungstäter (§ 12 zweiter Fall StGB) und der unmittelbare Täter selbst (§ 12 erster Fall StGB). Zur Klarstellung soll dies in der hier vorgeschlagenen Bestimmung konkretisiert werden.

Die Streichung des Abs. 3 dient der Rechtsbereinigung, da schon die Klassifizierung voraussetzt, dass ein oder mehrere der in § 6 IFG genannten Interessen geschädigt werden könnten, was bei verfassungsgefährdenden Tatsachen nicht in Betracht kommt.

**Zu Z 9 (§ 11):**

Die Abschnittsüberschrift wird im Hinblick auf den Gegenstand der §§ 11 bis 13, nämlich den Themenkomplex der Industriellen Sicherheit, geändert. Die bisherige Abschnittsüberschrift wird zur Überschrift des § 11, wobei neben Unternehmen und Anlagen nun auch Einrichtungen in der Überschrift selbst erfasst werden.

Durch die Zusammenführung des nationalen und des internationalen Geheimschutzes ergibt sich die Notwendigkeit einer Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen, Einrichtungen und Anlagen nicht mehr aus völkerrechtlicher Verpflichtungen in unmittelbar anwendbaren Staatsverträgen gemäß Art. 50 Abs. 1 B-VG und Übereinkommen gemäß § 14, sondern direkt aus dem Wortlaut des § 11.

Um auf nationaler Ebene alle Anwendungsfälle für die Notwendigkeit einer Sicherheitsunbedenklichkeitsbescheinigung zu erfassen, wurde § 11 durch den Wortlaut „Erfüllung staatlicher Aufgaben“ ergänzt. Damit werden jene Fälle erfasst, in welchen die Erfüllung gesetzlicher Aufträge den Zugang zu klassifizierten Informationen erforderlich macht. Die Weitergabe klassifizierter Informationen an Unternehmen, Einrichtungen und Anlagen erfolgt daher ausschließlich auf Basis der §§11ff.Durch die Umformulierung des Wortlauts wird klargestellt, dass eine Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen, Einrichtungen und Anlagen erforderlich ist, bevor national oder international klassifizierte Informationen an diese weitergegeben werden.

**Zu Z 10 (§ 12 Abs. 3 bis 4b):**

Durch die Änderung des Wortlauts des Abs. 3 wird klargestellt, dass alle natürlichen Personen, an die im Rahmen einer industriellen Tätigkeit im Sinne des 2. Abschnitts für die Erfüllung ihrer beruflichen

Pflichten (Need-to-Know) klassifizierte Informationen weitergegeben werden, die Voraussetzungen analog zu § 3 Abs. 1 Z 2 und 3 erfüllen müssen. Dies wird im Rahmen des Prozesses der Erlangung einer Sicherheitsunbedenklichkeitsbescheinigung für das Unternehmen, die Einrichtung oder die Anlage geprüft. Durch die Präzisierung des Anwendungsbereiches werden diese Personen somit sowohl von der Verpflichtung der Verschwiegenheit gemäß § 4 als auch vom Straftatbestand des § 9 erfasst.

Auf Grund der Konsolidierung des nationalen und internationalen Geheimschutzes sind von diesen Bestimmungen nunmehr nicht nur die völkerrechtlichen, sondern auch die nationalen Verpflichtungen umfasst.

**Zu Z 13 (§ 15):**

In § 15 erfolgt die Anpassung der Geschlechterformulierung an die jüngere Judikatur.

**Zu Z 14 (§ 17):**

Die Betrauung des Bundeskanzlers mit der Vollziehung dieses Bundesgesetzes konkretisiert den schon in der Ursprungsfassung des InfoSiG (2002) bestehenden Willen des Gesetzgebers und bringt diesen klar zum Ausdruck. Daneben gibt es weiterhin Bereiche, wie beispielsweise jenen der industriellen Sicherheit in §§ 11 bis 13, die nur den Wirkungsbereich eines Mitglieds der Bundesregierung betreffen und weiterhin von diesem vollzogen werden.