Vorblatt

Probleme:

Aktuelle Entwicklungen im Rahmen der Europäischen Union sowie andere internationale Verpflichtungen Österreichs im Bereich der Sicherheitszusammenarbeit erfordern die Schaffung einer gesetzlichen Regelung über den Zugang zu klassifizierten Informationen und deren sichere Verwendung.

Ziele:

Umsetzung internationaler Verpflichtungen durch die Gewährleistung einheitlicher Informationssicherheitsstandards.

Inhalt:

Klassifizierung von Informationen und das Festlegen von Kriterien, unter denen einer Person Zugang zu einer schutzwürdigen Information gewährt werden kann. Regelung der Amtshilfe und internationaler Kooperation bei klassifizierter Information sowie Bestellung von Informationssicherheitsbeauftragten und Einrichtung einer Informationssicherheitskommission.

Alternativen:

keine

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

keine

Finanzielle Auswirkungen:

Keine zusätzlichen Kosten; der für die Durchführung dieses Gesetzes anfallende Personal- und Sachaufwand ist von jedem Bundesministerium im Rahmen der vorhandenen budgetären Mittel zu tragen.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Das vorliegende Gesetz bezweckt die Umsetzung des Beschlusses des Rates der EU 2001/264/EG vom 19. März 2001 über die Annahme der Sicherheitsvorschriften des Rates, ABl. Nr. L 101 vom 11. April 2001, den die Mitgliedstaaten gemäß seinem Art. 2 Abs. 3 vor dem 30. November 2001 umzusetzen haben.

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

Aktuelle Entwicklungen im Rahmen der Europäischen Union sowie andere internationale Verpflichtungen Österreichs im Bereich der Sicherheitszusammenarbeit erfordern die Schaffung einer gesetzlichen Regelung über den Zugang zu klassifizierten Informationen und deren sichere Verwendung.

Diese Verpflichtungen können wie folgt zusammengefasst werden:

1. Verpflichtungen im Bereich der Europäischen Union

Der Rat der EU fasste am 19. März 2001 den Beschluss 2001/264/EG über die Annahme der Sicherheitsvorschriften des Rates, ABl. Nr. L 101 vom 11. April 2001, S. 1 ff., den die Mitgliedstaaten gemäß seinem Art. 2 Abs. 3 vor dem 30. November 2001 umzusetzen haben. Sie haben dabei geeignete Maßnahmen zu treffen, um dafür zu sorgen, dass beim Umgang mit EU-Verschlusssachen innerhalb ihrer Dienste und Gebäude die Sicherheitsvorschriften des Rates eingehalten werden.

Überdies existieren Beschlüsse des Rates über den Zugang der Öffentlichkeit zu Dokumenten (93/731/EG idF 2000/527/EG), in denen auch Regelungen über die Einschränkung dieses Rechts aus Gründen der Informationssicherheit enthalten sind. Zudem regelt die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. Nr. L 145 vom 31. Mai 2001, S. 43 ff.) die allgemeinen Grundsätze und die Einschränkungen des Rechts auf Zugang zu Dokumenten. Ferner verpflichtet Art. 31 des Europol-Übereinkommens, BGBl. III Nr. 123/1998, die Mitgliedstaaten sicher zu stellen, dass von Europol verwendete geheimhaltungsbedürftige Informationen geschützt werden.

2. Verpflichtungen im Bereich der internationalen Sicherheitszusammenarbeit

Seit Beginn der Neunzigerjahre beteiligt sich Österreich zunehmend in solidarischer Weise an Maßnahmen im Rahmen der in Europa aufgebauten Sicherheitsstrukturen. Gleichzeitig mit dem Beginn seiner EU-Mitgliedschaft wurde Österreich mit 1. Jänner 1995 Beobachter bei der Westeuropäischen Union und wirkt darüberhinaus seit 10. Februar 1995 am Programm „Partnerschaft für den Frieden“ (Partnership for Peace“ - PfP) mit. Für diese Kooperation im sicherheitspolitischen Bereich hat Österreich einige völkerrechtliche Verträge abgeschlossen (beispielsweise der Beitritt zum PfP-Truppenstatut, BGBl. III Nr. 136/1998). Zur Sicherung des Schutzes von Informationen wurde 1995 ein Abkommen zwischen der Österreichischen Bundesregierung und der NATO über den Schutz von Informationen, BGBl. Nr. 18/1996, abgeschlossen, das unter einem allgemeinen Gesetzesvorbehalt steht.

Mit der WEU wurde am 18. November 1996 das Sicherheitsabkommen zwischen Österreich und der Westeuropäischen Union unterzeichnet, welches allerdings noch nicht ratifiziert wurde. Die WEU-Sicherheitsbestimmungen RS 100 stellen dabei einen integralen Vertragsbestandteil dar. Bei der Vorbereitung des innerstaatlichen Genehmigungsverfahrens wurde festgestellt, dass es zur Durchführung des Abkommens und insbesondere der Sicherheitsbestimmungen RS 100 noch innerstaatlicher Umsetzungsmaßnahmen bedürfen wird, also dem Nationalrat vorgeschlagen werden sollte, bei Genehmigung des Abkommens einen Beschuss gemäß Art. 50 Abs. 2 B-VG zu treffen.

Innerstaatliche Maßnahmen im Bereich der Informationssicherheit

Art. 20 Abs. 3 B-VG normiert die Pflicht zur Amtsverschwiegenheit. Die verfassungsrechtliche Verankerung des Schutzes von personenbezogenen Daten findet sich in § 1 des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999. Die im Informationssicherheitsgesetz umschriebenen Verpflichtungen zur Wahrung von Verschwiegenheit betreffen Bereiche, in denen das jeweilige Geheimhaltungsinteresse des Bundes in den verschiedenen Klassifikationsstufen zum Ausdruck kommt.

Zur Umsetzung der durch die erwähnten Verpflichtungen erforderlichen Sicherheitsüberprüfung wurde 1999 eine Novelle des Sicherheitspolizeigesetzes erlassen (SPG-Novelle 1999, BGBl. I Nr. 146/1999), deren §§ 55 ff. detaillierte Regelungen treffen. Um über die Sicherheitsüberprüfung hinaus, die allein aus kompetenzrechtlichen Gründen nur sicherheitspolizeiliche Aspekte berücksichtigen kann, auch spezifisch militärischen Anforderungen zu genügen, sehen die §§ 23 und 24 Militärbefugnisgesetz, BGBl. I Nr. 86/2000, eine Verlässlichkeitsprüfung von Personen, die Zugang zu militärischen Rechtsgütern nach § 1 Abs. 7 Z 3 MBG haben oder erlangen sollen, vor. Beide Gesetze normieren abgestufte Überprüfungen, abhängig von der Klassifikationsstufe, mit der eine Information versehen wird, zu der die betreffende Person Zugang bekommen soll.

Bereits in den Erläuterungen zu den Ziffern 22 und 23 der SPG-Novelle 1999 (RV 1479 BlgNR XX. GP) wurde hervorgehoben, dass es über die Sicherheitsüberprüfung hinaus weiterer Geheimschutzbestimmungen bedürfen wird.

Zur Gewährleistung einheitlicher Informationssicherheit in der Bundesverwaltung ist die Erlassung des Informationssicherheitsgesetzes erforderlich, das jedoch nähere Einzelheiten (insbesondere physische Schutzmaßnahmen, Regelung der Zuständigkeit zur Klassifizierung von Informationen usw.) einer Informationssicherheitsverordnung der Bundesregierung überlässt.

Mit Erlassung des Informationsschutzgesetzes kann auch das WEU-Sicherheitsabkommen ratifiziert werden.

Finanzielle Auswirkungen:

Hinsichtlich der zu treffenden physischen Informationssicherheitsmaßnahmen (z.B. Versperren in Panzerschränken) haben die von der Durchführung des Gesetzes hauptbetroffenen Ressorts (Bundeskanzleramt, Bundesministerien für auswärtige Angelegenheiten, für Inneres und für Landesverteidigung) bereits gewisse Maßnahmen im Hinblick auf die internationalen Verpflichtungen Österreichs getätigt. Insgesamt wird sich bei allen Ressorts ein Nachrüstbedarf ergeben, der vom ordentlichen Budget der Ressorts zu tragen ist.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Gesetzgebung im Bereich Informationssicherheit ergibt sich aus Art. 10 Abs. 1 Z 2 B-VG („äußere Angelegenheiten“), Art. 10 Abs. 1 Z 6 B-VG („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“) und Art. 10 Abs. 1 Z 15 B-VG („militärische Angelegenheiten“).

Besonderer Teil

Zu § 1:

Im Interesse der Rechtssicherheit soll der für den gesamten vorliegenden Gesetzentwurf wichtige Begriff der Informationssicherheit als Zielvorgabe umschrieben und dessen Anwendungsbereich festgelegt werden.

Der Informationsbegriff, als Schutzgegenstand der Informationssicherheit, von dem in diesem Gesetzentwurf ausgegangen wird, ist ein weiter, was dadurch zum Ausdruck kommen soll, dass in erster Linie das Interesse an der Regelung des Zugangs zu Informationen und an deren sicherer Verwendung und weniger die Darstellungsform bzw. das Trägermedium der Information Schutzmaßnahmen indizieren soll. Das heißt, schutzwürdig sind Informationen unabhängig von ihrer Darstellungsform. Damit können als schutzwürdige Informationen beispielsweise sowohl Weisungen, Dienstanweisungen, Berichte, Stellungnahmen,

Amtssiegel, Geschäftsbücher ebenso in Betracht kommen wie Leistungsdaten und die Beschaffenheit von Geräten unabhängig von den Datenträgern auf denen diese Information verfügbar ist. Als Trägermedium kommen insbesondere in Betracht: Papier, Filme, Tonträger, magnetische, elektronische und digitale Datenträger (Magnetbänder, Disketten, CD etc.) aber auch spezielle Metalllegierungen, Modelle und Ähnliches. Vom Begriff „Informationen“ im Sinne dieses Gesetzes sind daher die Begriffe „Information“ und „Material“ gleichermaßen umfasst, wie sie beispielsweise im Bereich der NATO üblich sind (und auch in Art. 1 lit. (i) des Abkommens zwischen der Österreichischen Bundesregierung und der NATO über den Schutz von Informationen, BGBl. Nr. 18/1996, verwendet werden). Des Weiteren soll durch diese Bestimmung klargestellt werden, dass sich der durch diesen Gesetzentwurf angestrebte Schutz ausschließlich auf Informationen beziehen soll, welche aus dem Bereich einer Dienststelle des Bundes stammen, soweit dies den ebenfalls angeführten Interessenlagen entspricht. Die betroffenen Interessenlagen beruhen – mit Einschränkungen – auf jenen des Art. 20 Abs. 3 B-VG (Amtsverschwiegenheit), wobei „im volkswirtschaftlichen Interesse des Bundes geboten“ eine deutliche Einschränkung gegenüber „im wirtschaftlichen Interesse einer Körperschaft des öffentlichen Rechtes“ (vgl. Art. 20 Abs. 3 B-VG) darstellt. Im Bereich der volkswirtschaftlichen Interessen des Bundes könnte sich eine Schutzwürdigkeit von Informationen besonders im Bereich der „dual-use“-Güter ergeben.

Zu § 2:

Abs. 1 dieser Bestimmung soll klarstellen, dass die Klassifizierung von Informationen bei Vorliegen der gesetzlichen Voraussetzungen verpflichtend zu erfolgen hat. Dies hat jedoch nur in dem unbedingt notwendigen Maß und für die erforderliche Dauer zu erfolgen. Die Beurteilung dieser Kriterien hat jeweils vom Verfasser der Information bzw. demjenigen zu erfolgen, der für den Schutz der Information verantwortlich zeichnet.

Abs. 2 legt die Bezeichnung der jeweiligen Klassifizierungsstufen sowie deren jeweiligen Schutzumfang fest und gibt somit die Kriterien für die Klassifizierung von Informationen im Sinne dieses Gesetzes vor. Dabei wird vorrangig an den Folgen angeknüpft, die durch eine Preisgabe dieser Informationen an Unbefugte entstehen können. Die Abs. 2 Z 2 bis 4 entsprechen den Klassifizierungsstufen, die in § 55 Abs. 3 SPG angeführt sind. Die niedrigste Schutzstufe („Eingeschränkt“) ist in Abs. Z 1 angeführt, findet sich jedoch nicht in § 55 Abs. 3 SPG, da der Zugang zu einer solcherart klassifizierten Information nicht von einer vorherigen Sicherheitsüberprüfung abhängt (siehe § 3 Abs. 1 Z 3). Von dieser Klassifizierungsstufe ist auch die in manchen Staaten übliche Klassifikation „nur für den Dienstgebrauch“ umfasst.

Das im Gesetz in Aussicht genommene vierstufige System folgt den internationalen Gepflogenheiten und berücksichtigt dabei auch die völkerrechtlichen Verpflichtungen der Republik Österreich auf dem Gebiet der Informationssicherheit. Diese Konvergenz ermöglicht, den Verwaltungsaufwand im Zusammenhang mit vom Ausland übermittelten Informationen so gering wie möglich zu halten.

Auf diese völkerrechtlichen Verpflichtungen wird auch insofern Rücksicht genommen, als in Abs. 3 festgeschrieben wird, dass die Klassifizierung von übermittelten Informationen internationaler Organisationen, sonstiger zwischenstaatlicher Einrichtungen oder fremder Staaten nach diesem Gesetz derart erfolgen soll, dass im Inland kein geringerer als der von der übermittelnden Stelle vorgesehene Schutz gewährleistet wird. Daraus folgt, dass nicht die Bezeichnung der Klassifizierungsstufe, sondern die getroffenen Schutzmaßnahmen das vorrangige Beurteilungskriterium bei der Klassifizierung derart übermittelter Informationen darstellen (materielle Gleichwertigkeit an Stelle formeller Gleichwertigkeit).

Gemäß § 5 des Bundesarchivgesetzes, BGBl. I Nr. 162/1999, ist Schriftgut, das bei Bundesdienststellen anfällt und nicht mehr für die laufenden Geschäfte benötigt wird, auszusondern und dem Österreichischen Staatsarchiv zur Übernahme anzubieten. Abs. 4 ermöglicht den jeweiligen Bundesdienststellen, Schriftgut, bei dem es sich um klassifizierte Informationen handelt und das nicht mehr für die laufenden Geschäfte benötigt wird, im Interesse der Informationssicherheit dennoch weiterhin im eigenen Bereich zu verwahren. Die Ausnahme vom Geltungsbereich des § 5 Bundesarchivgesetz gilt jedoch nur, solange die Klassifizierung der Informationen besteht.

Zu § 3:

Die Erreichung einer effizienten und glaubwürdigen Informationssicherheit macht die Festlegung der Kriterien, unter denen einer Person Zugang zu schutzwürdigen Informationen gewährt werden kann, unerlässlich. Diese Zugangskriterien orientieren sich an der Zweckmäßigkeit des dadurch erlangten Sicherheitsstandards und sind darüber hinaus mit den internationalen Grundsätzen und Mindeststandards der Informationssicherheit kompatibel.

Bei der Frage des Zugangs zu klassifizierten Informationen muss der Umstand berücksichtigt werden, dass schutzwürdige Informationen nicht nur Bediensteten des Bundes (Abs. 1 und 2), sondern fallweise auch Personen, welche keine Organwalter des Bundes sind, zur Kenntnis gelangen müssen (Abs. 3). Dabei ist vor allem an Angestellte von Unternehmen, die sich an Forschungsaktivitäten beteiligen, an Wartungspersonal privater Unternehmen oder an Bedienstete von ausgegliederten Rechtsträgern (Austrocontrol, Oesterreichische Nationalbank usw.) zu denken.

Abs. 1 normiert als Zugangsvoraussetzung für Bedienstete einer Dienststelle des Bundes ausdrücklich das „need to know"-Prinzip (Z 1) und das Erfordernis einer nachweislichen Unterweisung im Umgang mit klassifizierten Informationen (Z 2). Im Fall von Informationen gemäß § 2 Abs. 2 Z 2 bis 4 soll gemäß Z 3 zusätzlich dazu eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG die zur Bearbeitung erforderliche Vertrauenswürdigkeit ausweisen. Sofern eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG, BGBl. I Nr. 86/2000, vorgesehen ist, haben sich Bedienstete einer Dienststelle des Bundes einer solchen zu unterziehen.

Während die Sicherstellung der Maßnahmen nach Abs. 1 den Dienstgeber treffen, richtet sich Abs. 2 an den Bediensteten. Demnach darf er Zugang zu klassifizierter Information nur bei Vorliegen der in Abs. 1 normierten Voraussetzungen zu suchen. Das heißt, ein Bediensteter, der die Voraussetzungen des Abs. 1 nicht erfüllt, darf keine Handlungen setzen, um in Besitz klassifizierter Informationen zu gelangen.

Die Zugangskriterien für natürliche Personen, die keine Organwalter des Bundes sind, werden in Abs. 3 geregelt. Da die Schutzwürdigkeit der Information in gleicher Weise aufrecht bleibt wie bei deren Verbleib im Bereich einer Dienststelle des Bundes, trachten die diesen Bereich regelnden Bestimmungen den Schutz der Informationen auch außerhalb der Bundesverwaltung aufrecht zu erhalten. Somit sind Zugangskriterien dieser Personengruppe jenen der Bediensteten einer Dienststelle des Bundes insoweit nachempfunden, als dabei zu berücksichtigen ist, ob diese Person eine Tätigkeit ausübt, welche im öffentlichen Interesse gelegen ist und den Zugang zu klassifizierten Informationen erfordert (z.B. im Bereich der Vergabe von öffentlichen Aufträgen oder im Rahmen der Erstellung einer Studie). Abs. 3 Z 3 schreibt wiederum die Gleichwertigkeit der zu treffenden materiellen Schutzmaßnahmen vor.

Die Einhaltung der in den Zugangskriterien festgelegten Schutzmaßnahmen wird, anders als im öffentlichen Bereich, über entsprechende privatrechtliche Verpflichtungen durchzusetzen sein.

§ 3 Abs. 4 stellt klar, dass die Kautelen des § 3 Abs. 1 bis 3 dann nicht eingreifen, wenn ein Betroffener auf der Grundlage von § 26 DSG 2000 nur Zugang zu Informationen, die zu seiner Person gespeichert sind, sucht. Etwaige überwiegende Interessen, die auch in diesem Fall gegen eine Auskunftserteilung sprechen, sind nach § 26 Abs. 2 DSG zu berücksichtigen.

Zu § 4:

Durch § 4 wird die Verschwiegenheitspflicht ausdrücklich festgeschrieben und definiert; ihre Verletzung wird – soweit nicht § 9 zur Anwendung kommt – durch § 10 sanktioniert.

Zu § 5:

Durch diese Bestimmung sollen die Voraussetzungen festgeschrieben werden, unter denen es möglich sein soll, klassifizierte Informationen im Rahmen von Amtshilfe an ersuchende Organe, welche keine Dienststellen des Bundes sind, bzw. an ausländische Empfänger im gesetzlich festgelegten Rahmen zu übermitteln.

Anknüpfend an die Aufrechterhaltung der Informationssicherheit werden in Abs. 1 die Bedingungen geregelt, unter denen klassifizierte Informationen an ein ersuchendes Organ weitergegeben werden dürfen. Dabei soll die ersuchte Stelle nur dann zur Übermittlung der klassifizierten Informationen befugt werden, wenn das ersuchende Organ einen ausreichenden Schutzstandard gewährleisten kann.

Mit dieser Bestimmung wird die in Art. 22 B-VG normierte verfassungsrechtliche Verpflichtung zur Amtshilfe einfachgesetzlich konkretisiert bzw. auch eingeschränkt. Nach der Rechtsprechung des Verfassungsgerichtshofes ist Art. 22 B-VG unmittelbar anwendbar, d.h. auch ohne besondere einfachgesetzliche Ermächtigung besteht die Amtshilfeverpflichtung. Die unmittelbare Anwendbarkeit des Art. 22 B-VG steht jedoch einer näheren Regelung der vorgesehenen Hilfeleistungspflicht durch den einfachen Gesetzgeber nicht entgegen. *„Der verfassungsrechtliche Hintergrund spricht nicht grundsätzlich gegen die Annahme, dass Regelungen von derart eingeschränkter Bedeutung gleichwohl normative Wirkung auf die Behörden ausüben, deren Hilfeleistung erwartet wird. Es kann zur Sicherung der erwünschten Zusammenarbeit nötig sein, den Hilfeleistungsfall und das Verhalten der helfenden Behörde generell zu regeln“* (VfSlg 10.715/1985). Eine Konkretisierung des Art. 22 B-VG durch den einfachen Gesetzgeber in der Form, dass die Amtshilfeverpflichtung anstelle des Ersuchens der Behörde an einen Antrag des betroffenen Rechtsunterworfenen geknüpft wurde und dass für die zu leistende Amtshilfe das Formerfordernis einer Bescheinigung vorgesehen war, wurde vom VfGH ausdrücklich als zulässig qualifiziert (VfSlg 10.715/1985).

Allgemein wird aus der Formulierung in Art. 22 B-VG „im Rahmen des gesetzmäßigen Wirkungsbereiches“ eine Befugnis und auch Pflicht zur Interorgankontrolle abgeleitet. Das ersuchte Organ hat, bevor es dem Ersuchen zur Amtshilfe nachkommt, zu prüfen, ob das Hilfeleistungsersuchen in den allgemeinen gesetzlichen Wirkungsbereich des ersuchenden Organs fällt. In der Literatur wird der Hinweis auf den „gesetzlichen Wirkungsbereich“ in Art. 22 B-VG als Gesetzesvorbehalt verstanden, der dem einfachen Gesetzgeber die Möglichkeit bietet, die Amtshilfe als solche zum Gegenstand gesetzlicher Regelung zu machen und dabei eine Einschränkung der Hilfeleistungspflicht vorzusehen. Eine solche einfachgesetzliche Einschränkung des Art. 22 B-VG ist etwa auch in den §§ 7 bis 9 DSG 2000 vorgesehen, woraus sich eine entsprechende Erweiterung der Kontrollpflichten des ersuchten Organs ergibt.

Vor diesem Hintergrund kann die vorgesehene Bindung der Amtshilfe an bestimmte Voraussetzungen als eine zur Sicherung der erwünschten Zusammenarbeit nötige generelle Regelung angesehen werden (VfSlg 10.715/1985).

Dem immer mehr an Bedeutung gewinnenden Informationsaustausch im Rahmen der Zusammenarbeit auf bilateraler wie multilateraler Ebene tragen die Bestimmungen der Abs. 2 und 3 Rechnung.

Abs. 2 sieht vor, dass die Bundesregierung Regierungsübereinkommen abschließen kann, wenn ein gleichwertiger Schutzstandard gewährleistet ist. Durch den Abschluss von im Abs. 2 angeführten Übereinkommen soll eine Evaluierung der jeweiligen Informationssicherheit mit dem Ziel erfolgen, dass in weiterer Folge bei zukünftigen Übermittlungen von klassifizierten Informationen die erforderlichen Schutzmaßnahmen nicht in jedem Einzelfall überprüft werden müssen. Daher dient diese Vorgehensweise auch der Verwaltungsvereinfachung und beschleunigt nicht zuletzt die Geschwindigkeit des Informationsaustausches.

Für all jene Fälle, in denen ein Übereinkommen nach Abs. 2 nicht besteht, soll Abs. 3 klarstellen, dass von der ersuchten Stelle zu prüfen ist, ob die Übermittlung der klassifizierten Informationen im öffentlichen Interesse gelegen ist, ob die Zustimmung des Urhebers der Information zur Übermittlung vorliegt und ob der Empfänger in der Lage ist, keinen geringeren als den von der übermittelnden Stelle vorgesehenen Schutzstandard zu gewährleisten.

Zu § 6:

Eine im gesamten Anwendungsbereich dieses Bundesgesetzes einheitliche Vollziehung soll durch die Erlassung einer für alle Dienststellen des Bundes verbindlichen Informationssicherheitsverordnung der

Bundesregierung erreicht werden. In dieser Verordnung werden insbesondere physische Schutzmaßnahmen (Z 2) und die Frage, wie die Klassifizierung (Z 6) und die Deklassifizierung (Z 8) von Informationen festgelegt wird, zu regeln sein. Die Ausgestaltung der technischen Datensicherheitsmaßnahmen (Z 7) hat sich an § 14 DSG 2000 zu orientieren.

Zu § 7:

Gemäß Abs. 1 ist jeder Bundesminister verpflichtet, einen Informationssicherheitsbeauftragten und einen Stellvertreter für den jeweiligen Ressortbereich zu bestellen.

Wie Abs. 2 ausführt, obliegt diesem die Überwachung der Einhaltung der Bestimmungen dieses Bundesgesetzes, der Informationssicherheitsverordnung und der sonstigen Informationssicherheitsvorschriften sowie die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen und die Berichterstattung darüber an die Informationssicherheitskommission. Darüber hinaus hat dieser im Falle der Wahrnehmung eines Mangels auf dessen unverzügliche Behebung hinzuwirken.

Die detaillierte Umsetzung und Regelung der Aufgaben der Informationssicherheitsbeauftragten kann im Erlassweg (z.B. im Rahmen einer generellen Weisung zur Informationssicherheit) erfolgen; dies gilt insbesondere für Abs. 3.

Um dies zu gewährleisten, kann der Informationssicherheitsbeauftragte gemäß Abs. 4 den zuständigen Bundesminister in Angelegenheiten der Informationssicherheit beraten und erforderlichenfalls Vorschläge zur Verbesserung erstatten.

Sofern der Informationssicherheitsbeauftragte Zugang zu klassifizierten Informationen haben wird, ist § 3 Abs. 1 und 2 auf ihn anzuwenden, d.h. ist dieser einer Sicherheitsüberprüfung oder allenfalls einer Verlässlichkeitsprüfung zu unterziehen.

Zu § 8:

Die Einsetzung einer Informationssicherheitskommission soll eine einheitliche Informationssicherheit sowie deren Koordination in der Bundesverwaltung sicherstellen. Dies erfolgt unter anderem durch einen Erfahrungsaustausch zwischen den Sicherheitsbeauftragten und durch die Erstattung von Vorschlägen zur Verbesserung der Informationssicherheit (Abs. 1 Z 2). Dies beinhaltet auch die Möglichkeit, Vorschläge zur Verbesserung der gemäß § 6 zu erlassenden Informationssicherheitsverordnung zu unterbreiten. Mindestens alle drei Jahre und bei Bedarf auch in kürzeren Abständen hat die Informationssicherheitskommission der Bundesregierung auf Grundlage von Beiträgen der einzelnen Informationssicherheitsbeauftragten Bericht zu erstatten (Abs. 1 Z 3).

Darüber hinaus trägt die Errichtung der Informationssicherheitskommission zur Erfüllung der internationalen Verpflichtungen der Republik Österreich insoweit bei, als die bisher auf Grund des § 8 Abs. 1 und 2 BMG befristet errichtete „Kommission zum Schutz des Informationsaustausches mit internationalen Organisationen“ (BGBl. II Nr. 42/1997 idgF) nunmehr durch die Informationssicherheitskommission abgelöst wird (Abs. 1 Z 4). Das heißt, dass die Informationssicherheitskommission als nationale Sicherheitsorganisation im Sinne der Sicherheitsvorschriften des EU-Rates sowie als „National Security Authority“ (NSA) im Sinne der mit NATO und WEU abgeschlossenen Abkommen über die Sicherheit von Informationen fungieren wird.

Durch Abs. 3 soll sichergestellt werden, dass die Informationssicherheitskommission zur ordnungsgemäßen Wahrnehmung ihrer Aufgaben auch sonstige Experten ihren Sitzungen beiziehen kann. Dabei ist sowohl an Personen aus dem Bereich der Bundesverwaltung als auch an keiner Gebietskörperschaft angehörende Personen gedacht. Der Bedarf hiezu kann sich vor allem bei der Erörterung außerordentlicher Problemlagen wie z.B. Fragen im Bereich der EDV ergeben. Auf diese Weise soll der Informationssicherheitskommission ermöglicht werden, ihrer Rolle als INFOSEC-Stelle zu entsprechen.

Zu § 9:
Unter gerichtliche Strafe gestellt werden soll die Offenbarung und Verwertung von Informationen der Klassifizierungsstufen „Vertraulich“, „Geheim“ und „Streng geheim“. Dies ist insbesondere notwendig, um eine effiziente Umsetzung der völkerrechtlichen Verpflichtungen Österreichs zur Geheimhaltung (vgl. dazu auch den Allgemeinen Teil) zu gewährleisten.

Eine sonstige Verletzung der Verschwiegenheitspflicht soll - soweit kein Tatbestand einer gerichtlich strafbaren Handlung erfüllt ist - als Verwaltungsübertretung geahndet werden (siehe dazu § 10).

Der Tatbestand ist weitgehend an § 310 StGB angelehnt, die Strafdrohungen sowie die Qualifizierung in Abs. 2 orientieren sich systemkonform an §§ 121 f. StGB, die die Verletzung bestimmter Geheimnisse durch Personen erfassen, die im Gegensatz zu dem mit einer höheren Strafdrohung belegten § 310 StGB nicht Beamte sein müssen.

Durch den Verweis auf § 3 Abs. 1 und Abs. 3 werden Bedienstete des Bundes und natürliche Personen, die keine Organwalter des Bundes sind, erfasst. Eine Geheimnisverletzung durch Organwalter des Bundes wird in der Regel bereits durch § 310 StGB (Verletzung des Amtsgeheimnisses) unter Strafe gestellt sein, doch sollen durch die Zitierung auch des Abs. 1 mögliche Lücken geschlossen und eine allfällige Schlechterstellung von Personen, die keine Organwalter des Bundes sind, vermieden werden.

Die Subsidiaritätsklausel stellt klar, dass bei gleichzeitiger Verletzung von nach anderen Bundesgesetzen bestehenden Geheimhaltungspflichten (insbesondere §§ 252, 253, 254 oder 310 StGB; §§ 26, 27 MilStG) die Strafbarkeit nach dem strenger bestraften Delikt vorgeht. Die vorliegende Strafbestimmung erfasst daher primär die Offenbarung oder Verwertung durch natürliche Personen, die nicht Organwalter des Bundes sind.

Die Tathandlungen entsprechen jenen in §§ 121, 122 und 310 StGB. Eine entsprechend klassifizierte Information „offenbart”, wer sie einem oder mehreren anderen, die nicht zum Kreis der Informationsträger gehören, oder der Öffentlichkeit mitteilt oder sonst zugänglich macht. Eine solche Information „verwertet”, wer sich ihre Kenntnis wirtschaftlich zunutze macht. Wie bei § 310 StGB soll für die gerichtliche Strafbarkeit die bloße Verletzung des Geheimnisses nicht genügen, sondern der Anwendungsbereich von § 9 auf Fälle beschränkt bleiben, in denen durch den Geheimnisverrat eines der ausdrücklich genannten öffentlichen Interessen verletzt werden könnte. Der Eintritt eines Schadens ist in keinem Fall vorausgesetzt; es genügt vielmehr die abstrakte Eignung der Offenbarung oder Verwertung zur Verletzung eines der genannten öffentlichen Interessen.

Auf der inneren Tatseite ist Vorsatz erforderlich; bedingter Vorsatz genügt.

Die Qualifikation in Abs. 2 verändert an sich das objektive Tatbild des Abs. 1 nicht, fügt aber als überschießende Innentendenz eine besondere Absicht iS des § 5 Abs. 2 StGB hinzu. Diese Absicht kann entweder darin bestehen, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Bei der Absicht, einem anderen einen Nachteil zuzufügen, muss es sich um keinen Nachteil vermögensrechtlicher Art handeln. Unter „Anderen“ werden in diesem Zusammenhang sowohl Privatpersonen als auch juristische Personen, auch solche des öffentlichen Rechts (Republik Österreich), zu verstehen sein.

Abs. 3 ist § 310 Abs. 3 StGB nachempfunden. Die Strafbarkeit als Verwaltungsübertretung nach § 4 bleibt jedoch gegeben.

Im Übrigen wird auf Judikatur und Lehre zu § 310 StGB verwiesen.

Zu § 10:
Als Verwaltungsübertretung soll jede sonstige Verletzung der Verschwiegenheitspflicht nach § 4, insbesondere also in Bezug auf als „Eingeschränkt“ klassifizierte Informationen, bestraft werden. Ebenso bleibt

die gemäß § 9 Abs. 3 (gerichtlich) straflose Offenbarung von verfassungsgefährdenden Tatsachen (§ 252 Abs. 3 StGB) nach dieser Bestimmung als Verwaltungsübertretung strafbar.

Eine Verletzung der Verschwiegenheitspflicht (Abs. 1 Z 1) liegt in der mündlichen oder schriftlichen Weitergabe von klassifizierten Informationen.

Abs. 1 Z 2 erfasst jeden Verstoß gegen vorgesehene Schutzsstandards, wenn dadurch Unbefugte nach diesem Gesetz geschützte Informationen tatsächlich zur Kenntnis nehmen konnten. Den bloßen Verstoß gegen die Schutzstandards auch dann zu bestrafen, wenn sozusagen kein Schaden eingetreten ist, ist wohl nicht erforderlich. Die Schutzstandards verfolgen ja einzig den Zweck, die Kenntnisnahme durch Unbefugte zu verhindern. Wenn dies trotz Verletzung der Vorschrift nicht eingetreten ist, erscheint die Strafwürdigkeit fraglich.

Zu § 13:

Durch die in Abs. 1 vorgesehene Legisvakanz soll sichergestellt werden, dass sich die einzelnen Dienststellen des Bundes auf die Durchführung der in diesem Gesetz vorgesehenen Maßnahmen vorbereiten können. Zudem ermöglicht Abs. 2 bereits die Ausarbeitung der Informationssicherheitsverordnung (§ 6) vor Inkrafttreten des Gesetzes.

Bundesgesetz über den Zugang zu klassifizierten Informationen und deren sichere Verwendung (Informationssicherheitsgesetz), InfoSiG

Der Nationalrat hat beschlossen:

Ziel und Anwendungsbereich des Gesetzes

§ 1. Ziel dieses Bundesgesetzes ist die Regelung des Zugangs zu klassifizierten Informationen im Bereich der Dienststellen des Bundes, unabhängig von Darstellungsform und Datenträger, und der sicheren Verwendung dieser Informationen, soweit dies im Interesse der Aufrechterhaltung der öffentlichen Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen oder im volkswirtschaftlichen Interesse des Bundes geboten ist (Informationssicherheit).

Klassifizierung von Informationen

§ 2. (1) Informationen sind zu klassifizieren, wenn zur Wahrung der in § 1 genannten Interessen eine gesetzliche oder völkerrechtliche Verpflichtung zur Geheimhaltung besteht. Informationen sind jedenfalls nur in dem unbedingt notwendigen Maß und für die erforderliche Dauer zu klassifizieren.

(2) Wenn Informationen gemäß Abs. 1 zu klassifizieren sind, ist eine der folgenden Klassifizierungsstufen zu wählen:

1. „EINGESCHRÄNKT“, wenn die unbefugte Weitergabe der Informationen den in § 1 genannten Interessen zuwiderlaufen würde;
2. „VERTRAULICH“, wenn die Informationen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist;
3. „GEHEIM“, wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in § 1 genannten Interessen schaffen würde;
4. „STRENG GEHEIM“, wenn die Informationen geheim sind und überdies ihr Bekanntwerden eine schwere Schädigung der in § 1 genannten Interessen wahrscheinlich machen würde.

(3) Informationen, die von einer internationalen Organisation, einer sonstigen zwischenstaatlichen Einrichtung oder einem fremden Staat übermittelt worden sind, sind so zu klassifizieren, dass im Inland kein geringerer als der von der übermittelnden Stelle vorgesehene Schutz gewährleistet wird.

(4) Solange Informationen klassifiziert sind, findet auf sie § 5 des Bundesarchivgesetzes, BGBl. I Nr. 162/1999, keine Anwendung.

Zugang zu klassifizierten Informationen

§ 3. (1) Einem Bediensteten einer Dienststelle des Bundes kann der Zugang zu klassifizierten Informationen gewährt werden, wenn

1. der Zugang zu diesen Informationen für die Erfüllung seiner dienstlichen Aufgaben erforderlich ist,
2. er nachweislich ausreichend über den Umgang mit klassifizierten Informationen unterwiesen wurde und
3. soweit Informationen gemäß § 2 Abs. 2 Z 2 bis 4 betroffen sind eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG, BGBl. Nr. 566/1991 idF BGBl. I Nr. 146/1999, oder, sofern gesetzlich vorgesehen, eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG, BGBl. I Nr. 86/2000, durchgeführt wurde.

(2) Ein Bediensteter einer Dienststelle des Bundes darf den Zugang zu klassifizierten Informationen nur unter den Voraussetzungen des Abs. 1 suchen.

(3) Einer natürlichen Person, die kein Organwalter des Bundes ist, darf der Zugang zu klassifizierten Informationen nur gewährt werden, wenn

1. dies für die Ausübung einer im öffentlichen Interesse gelegenen Tätigkeit erforderlich ist,
2. die Voraussetzungen des Abs. 1 Z 2 und 3 vorliegen und
3. kein geringerer als der von der zuständigen Dienststelle vorgesehene Schutzstandard gewährleistet wird.

(4) Die nach § 26 DSG 2000 den Bediensteten einer Dienststelle des Bundes sowie sonstigen natürlichen Personen in ihrer Eigenschaft als Betroffene (im Sinne des § 4 Z 3 DSG 2000) zustehenden Rechte werden durch die Regelungen der Abs. 1 bis 3 nicht berührt.

Verschwiegenheitspflicht

§ 4. Jede Person, der auf Grund dieses Bundesgesetzes Zugang zu klassifizierten Informationen gewährt wird,

1. ist zur Verschwiegenheit über die ihr dadurch zur Kenntnis gelangten Informationen verpflichtet und
2. hat durch Einhaltung der vorgesehenen Schutzstandards dafür Sorge zu tragen, dass kein Unbefugter

Kenntnis von den klassifizierten Informationen erlangt.

Amtshilfe und internationale Kooperation

§ 5. (1) Im Rahmen der Leistung von Amtshilfe dürfen klassifizierte Informationen nur übermittelt werden, wenn das ersuchende Organ dies ausdrücklich begehrt und den erforderlichen Schutzstandard zu gewährleisten vermag. Im Begehren ist anzugeben, bis zu welcher Klassifizierungsstufe für einen ausreichenden Schutzstandard vorgesorgt ist.

(2) Sofern die Bundesregierung zum Abschluss von Übereinkommen gemäß Art. 66 Abs. 2 B-VG ermächtigt ist, kann sie völkerrechtliche Vereinbarungen über das Übermitteln klassifizierter Informationen schließen. Hiebei ist vorzusehen, dass klassifizierte Informationen nur dann übermittelt werden dürfen, wenn beim Empfänger kein geringerer als der von der übermittelnden Stelle vorgesehene Schutzstandard gewährleistet wird.

(3) Unbeschadet der Bestimmung des Abs. 2 dürfen einer internationalen Organisation, einer sonstigen zwischenstaatlichen Einrichtung oder einem fremden Staat klassifizierte Informationen nur übermittelt werden, wenn die Übermittlung im öffentlichen Interesse gelegen ist, der Urheber der Information der Übermittlung zugestimmt hat und beim Empfänger kein geringerer als der von der übermittelnden Stelle vorgesehene Schutzstandard gewährleistet wird.

Informationssicherheitsverordnung

§ 6. Die Bundesregierung hat für die Dienststellen des Bundes durch Verordnung Vorschriften über die Informationssicherheit zu erlassen. Diese haben jedenfalls zu regeln:

1. die Kennzeichnung von klassifizierten Informationen,
2. Maßnahmen und Verhaltensregeln für den Umgang mit klassifizierten Informationen, insbesondere hinsichtlich der Übermittlung, der Vervielfältigung, der Aufbewahrung und der Vernichtung der Informationen,
3. Verhaltensregeln im Falle der Wahrnehmung eines Mangels im Bereich der Informationssicherheit,
4. Zugangsbeschränkungen, die nach Klassifizierungsstufen zu unterscheiden sind,
5. Maßnahmen zur Gewährleistung der Feststellbarkeit des Zugangs zu klassifizierten Informationen,
6. die Organisation der Klassifizierung von Informationen und deren periodische Überprüfung,
7. zu Zwecken der Informationssicherheit erforderliche technische Datensicherheitsmaßnahmen sowie
8. die Vorgangsweise bei der Deklassifizierung von Informationen.

Informationssicherheitsbeauftragte

§ 7. (1) Jeder Bundesminister bestellt für seinen Wirkungsbereich einen Informationssicherheitsbeauftragten und dessen Stellvertreter.

(2) Dem Informationssicherheitsbeauftragten obliegt die Überwachung der Einhaltung der Bestimmungen dieses Bundesgesetzes, der Informationssicherheitsverordnung und der sonstigen Informationssicherheitsvorschriften sowie die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen und die Berichterstattung darüber an die Informationssicherheitskommis-

sion nach § 8. Im Falle der Wahrnehmung eines Mangels hat der Informationssicherheitsbeauftragte auf die unverzügliche Behebung des Mangels hinzuwirken.

(3) Der Informationssicherheitsbeauftragte trägt dafür Sorge, dass in seinem Ressortbereich alle Personen, auf die die Voraussetzungen des § 3 Abs. 1 bis 3 zutreffen, sicherheitsüberprüft werden.

(4) Der Informationssicherheitsbeauftragte hat den zuständigen Bundesminister in Angelegenheiten der Informationssicherheit zu beraten und erforderlichenfalls Vorschläge zu deren Verbesserung zu erstatten.

Informationssicherheitskommission

§ 8. (1) Es wird eine Informationssicherheitskommission eingerichtet, der die Informationssicherheitsbeauftragten aller Bundesministerien angehören. Den Vorsitz führt der Informationssicherheitsbeauftragte des Bundeskanzleramts. Die Informationssicherheitskommission hat

1. auf eine bundesweite Einheitlichkeit von Schutzmaßnahmen und deren Koordination im Bereich der Bundesverwaltung, insbesondere bei der Leistung von Amtshilfe nach § 5, hinzuwirken,
2. einen Erfahrungsaustausch hinsichtlich der Einhaltung von Schutzmaßnahmen nach § 7 Abs. 2 im jeweiligen Ressortbereich durchzuführen und gegebenenfalls Vorschläge zur Verbesserung der Informationssicherheit zu erstatten,
3. der Bundesregierung bei Bedarf, jedoch mindestens alle drei Jahre, einen Bericht über den Stand der Informationssicherheit auf Grundlage von Beiträgen der einzelnen Informationssicherheitsbeauftragten zu erstatten,
4. Maßnahmen zum Schutz des Austauschs klassifizierter Informationen zwischen Österreich und internationalen Organisationen, sonstigen zwischenstaatlichen Einrichtungen oder fremden Staaten zu setzen beziehungsweise vorzuschlagen, sofern sie zur Durchführung der mit diesen über den Schutz und die Sicherheit klassifizierter Informationen getroffenen Vereinbarungen erforderlich sind.

(2) Die Informationssicherheitskommission gibt sich durch einstimmigen Beschluss eine Geschäftsordnung, die jedenfalls Regelungen hinsichtlich der Einberufung und des Geschäftsgangs von Sitzungen, der Organisation der Arbeiten sowie hinsichtlich der Willensbildung enthält.

(3) Soweit es für die ordnungsgemäße Wahrnehmung ihrer Aufgaben erforderlich ist, kann die Informationssicherheitskommission ihren Sitzungen auch sonstige Experten beiziehen. Näheres bestimmt die Geschäftsordnung.

Gerichtlich strafbare Handlungen

§ 9. (1) Wer eine ihm ausschließlich aufgrund von § 3 Abs. 1 oder 3 dieses Bundesgesetzes anvertraute oder zugänglich gewordene Information der Klassifizierungsstufe „Vertraulich“ (§ 2 Abs. 2 Z 2), „Geheim“ (§ 2 Abs. 2 Z 3) oder „Streng geheim“ (§ 2 Abs. 2 Z 4) offenbart oder verwertet, deren Offenbarung oder Verwertung geeignet ist, die öffentliche Sicherheit, die umfassende Landesverteidigung, die auswärtigen Beziehungen oder volkswirtschaftliche Interessen des Bundes (§ 1) zu beeinträchtigen, ist, sofern die Tat nicht nach anderen Bundesgesetzen mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu 6 Monaten oder mit Geldstrafe bis zu 360 Tagessätze zu bestrafen.

(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(3) Offenbart der Täter Informationen, die verfassungsgefährdende Tatsachen (§ 252 Abs. 3 StGB) betreffen, so ist er nur zu bestrafen, wenn er in der Absicht handelt, private Interessen zu verletzen oder der Republik Österreich einen Nachteil zuzufügen. Die irrtümliche Annahme verfassungsgefährdender Tatsachen befreit den Täter nicht von Strafe.

Verwaltungsübertretung

§ 10. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung erfüllt, begeht eine Verwaltungsübertretung,

1. wer die Verschwiegenheitspflicht nach § 4 Z 1 verletzt oder
2. wer entgegen § 4 Z 2 Schutzstandards nicht einhält, wenn dadurch ein Unbefugter Kenntnis von klassifizierten Informationen erlangt.

(2) Verwaltungsübertretungen nach Abs. 1 sind von der Bezirksverwaltungsbehörde mit Geldstrafe bis zu 5000 Euro zu bestrafen.

Sprachliche Gleichbehandlung

§ 11. Die in diesem Bundesgesetz verwendeten personenbezogenen Ausdrücke betreffen soweit es inhaltlich in Betracht kommt, Frauen und Männer gleichermaßen.

Verweisungen

§ 12. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze verweisen auf deren jeweils geltende Fassung.

Inkrafttreten

§ 13. (1) Dieses Bundesgesetz tritt mit ... in Kraft.

(2) Bereits von dem der Kundmachung folgenden Tag kann die Verordnung gemäß § 6 erlassen werden; sie darf aber erst mit dem Inkrafttreten dieses Bundesgesetzes in Wirksamkeit gesetzt werden.

Vollziehung

§ 14. Mit der Vollziehung dieses Bundesgesetzes ist die Bundesregierung, jedoch in Angelegenheiten, die nur den Wirkungsbereich eines Mitglieds der Bundesregierung betreffen, dieses betraut.