941 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP

Nachdruck vom 18. 12. 2001

Bericht

des Außenpolitischen Ausschusses

über die Regierungsvorlage (753 der Beilagen): Bundesgesetz, über den Zugang zu klassifizierten Informationen und deren sichere Verwendung (Informationssicherheitsgesetz), InfoSlG

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, sicherzustellen, 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 darüber hinaus 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 Beschluss 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 BglNR 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 Informationssicherheitsgesetzes kann auch das WEU-Sicherheitsabkommen ratifiziert werden.

Finanzielle Auswirkungen:

Hinsichtlich der zu treffenden physischen Informationssicherheitsmaßnahmen (zB 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“).

Der Außenpolitische Ausschuss hat die gegenständliche Regierungsvorlage in seiner Sitzung am 13. November 2001 in Verhandlung genommen.

Nach Berichterstattung durch den Abgeordneten Dr. Gerhart **Bruckmann** hat der Ausschuss einstimmig beschlossen, die Verhandlungen zu vertagen.

In seiner Sitzung vom 6. Dezember 2001, die nach Unterbrechnung durch den Ausschussobmann am 11. Dezember 2001 fortgesetzt wurde, hat der Ausschuss die Verhandlungen wieder aufgenommen.

An der Debatte beteiligten sich die Abgeordneten Dr. Michael **Spindelegger,** Dr. Peter **Pilz,** Wolfgang **Jung,** Mag. Walter **Posch,** Dr. Gerhard **Kurzmann,** Dr. Johannes **Jarolim,** Mag. Ulrike **Lunacek,** Wolfgang **Grossruck,** Dr. Caspar **Einem** und der Ausschussobmann, Abgeordneter Peter **Schieder,** sowie die Bundesministerin für auswärtige Angelegenheiten Dr. Benita **Ferrero-Waldner.**

Die Abgeordneten Dr. Michael **Spindelegger** und Wolfgang **Jung** brachten einen Abänderungsantrag ein, dem folgende Begründung beigegeben war:

„Der Nationalrat hat im Zusammenhang mit der Verwaltungsreform ein Deregulierungsgesetz beschlossen, um sicherzustellen, dass EU-Richtlinien nicht ‚übererfüllt‘ werden. Diesem Gesetz Rechnung

tragend soll durch diesen Abänderungsantrag nunmehr sichergestellt werden, dass in Österreich für Informationen, die von internationalen Organisationen klassifiziert worden sind, ein gleichartiger Schutz gewährleistet werden kann. Darüber hinausgehende Regelungen über die Klassifizierung innerstaatlicher Dokumente bleiben hiedurch jedoch unberührt.

Wie auch in anderen Staaten sollen für die Obersten Organe und die Gerichtsbarkeit Sonderregelungen getroffen werden, wobei davon ausgegangen wird, dass diese in ihrem eigenen Bereich Vorkehrungen für die sichere Verwendung von klassifizierten Informationen treffen. Dies gilt insbesondere für den parlamentarischen Bereich, in dem die Zugänglichkeit auch zu klassifizierten Informationen zur Erfüllung der Aufgaben, insbesondere im Sinne der Artikel 23e und 23f B-VG, erforderlich ist. Die in § 1 Abs. 2 für den Bereich des National- und des Bundesrates normierte Ausnahme soll jedoch nur für die Abgeordneten und Bundesräte, die Parlamentsdirektion und die parlamentarischen Klubs, nicht jedoch für persönliche Mitarbeiter von Abgeordneten gelten. Diese fallen unter den Anwendungsbereich des § 3 Abs. 1 Z 2.

Soweit der parlamentarische Bereich betroffen ist, ist auf bereits bestehende Regelungen in den §§ 31b Abs. 2 und 31c Abs. 4 GOG-NR zu verweisen, die durch eine Richtlinie des Präsidenten des Nationalrates – nach Beratung in der Präsidialkonferenz – näher ausgestaltet ist und dadurch ein dem internationalen Bereich vergleichbares Schutzniveau sicherstellt.“

Weiters brachte der Abgeordnete Dr. Peter **Pilz** einen Abänderungsantrag ein, den er wie folgt begründet hatte:

„Ein möglichst offener Zugang zu Informationen und Dokumenten ist Wesensmerkmal einer demokratischen Gesellschaft und daher unabdingbar. Er stärkt das Vertrauen der Öffentlichkeit in die Vollziehung.

Die Ergänzung bezieht sich auf 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, die auch in der Regierungsvorlage (753 der Beilagen) als Anlass und Grundlage für die Schaffung eines Informationssicherheitsgesetzes herangezogen wird. In Abs. 4 fasst die Verordnung das Ziel zusammen: ‚Diese Verordnung soll dem Recht auf Zugang der Öffentlichkeit zu Dokumenten größtmögliche Wirksamkeit verschaffen und gemäß Art. 255 Abs. 2 des EG-Vertrags die allgemeinen Grundsätze und Einschränkungen dafür festlegen.‘

Das aktuelle Urteil des Europäischen Gerichtshofes vom 6. Dezember 2001 (Rechtssache Case C-353/99P) unterstreicht die Notwendigkeit des Transparenzprinzips für die Behandlung von Informationen und Dokumenten. Der Gerichtshof stellt fest, dass der Verhältnismäßigkeitsgrundsatz es verlange, dass Ausnahmen nicht über das zur Erreichung des verfolgten Zieles angemessene und erforderliche Maß hinausgehen dürfen.

Insbesondere kann die Vertraulichkeit von Information dadurch erreicht werden, dass nach einer Prüfung nur diejenigen Teile einer Information unkenntlich zu machen sind, deren Weitergabe gegen die völkerrechtliche Verpflichtung verstoßen würde.

Weitere Verfahren für den Zugang zu Informationen sind anhängig.

(Verfassungsausschuss des Europäischen Parlaments, Schweden und Niederlanden)

Der Abänderungsantrag soll sicherstellen, dass die Klassifizierung auf Grund des InfoSiG auf das notwendige und gesetzeskonforme Mindestmaß beschränkt bleibt.“

Bei der Abstimmung wurde der von der Bundesregierung vorgelegte Gesetzentwurf unter Berücksichtigung des Abänderungsantrages der Abgeordneten Dr. Michael **Spindelegger** und Wolfgang **Jung** mit Stimmenmehrheit angenommen. Der Abänderungsantrag des Abgeordneten Dr. Peter **Pilz** fand nicht die Zustimmung der Ausschussmehrheit.

Als Ergebnis seiner Beratungen stellt der Außenpolitische Ausschuss den **Antrag,** der Nationalrat wolle dem **angeschlossenen Gesetzentwurf** die verfassungsmäßige Zustimmung erteilen.

Wien, 2001 12 11

Dr. Gerhart Bruckmann	**Peter Schieder**
Berichterstatter	Obmann

Anlage

Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG)

Der Nationalrat hat beschlossen:

Ziel und Anwendungsbereich des Gesetzes

§ 1. (1) Ziel dieses Bundesgesetzes ist die Umsetzung völkerrechtlicher Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen, unabhängig von Darstellungsform und Datenträger, im Bereich der Dienststellen des Bundes.

(2) Die Voraussetzungen für den Zugang zu klassifizierten Informationen nach § 3 Abs. 1 gelten nicht für den Bundespräsidenten, den Bereich des Nationalrates und des Bundesrates, die Mitglieder der Bundesregierung, die Staatssekretäre, die Gerichtsbarkeit, den Verfassungsgerichtshof und den Verwaltungsgerichtshof, den Rechnungshof und die Volksanwaltschaft. Die Weitergabe von klassifizierten Informationen an diese Organe und Einrichtungen unterliegt keinen Berschränkungen nach diesem Bundesgesetz, jedoch völkerrechtlich vorgesehenen Einschränkungen.

(3) Dieses Bundesgesetz berührt nicht die den in Abs. 2 genannten Organen und Einrichtungen übertragenen Verpflichtungen und Aufgaben.

Beschränkung des Zugangs zu klassifizierten Informationen

§ 2. (1) Der Zugang zu klassifizierten Informationen, die Österreich im Einklang mit völkerrechtlichen Regelungen erhalten hat, ist in dem von den übermittelnden Stellen vorgesehenen Maß und für die von diesen vorgesehene Dauer zu beschränken, wenn dies gemäß Art. 20 Abs. 3 B-VG geboten ist.

(2) Gemäß Abs. 1 erhaltene klassifizierte Informationen sind zur Wahrung des von den übermittelnden Stellen vorgesehenen Schutzes einer der folgenden Klassifizierungsstufen zuzuordnen:

1. „EINGESCHRÄNKT“, wenn die unbefugte Weitergabe der Informationen den in Art. 20 Abs. 3 B-VG genannten Interessen zuwiderlaufen würde;
2. „VERTRAULICH“, wenn die Informationen nach anderen Bundesgesetzen 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 Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde;
4. „STRENG GEHEIM“, wenn die Informationen geheim und überdies ihr Bekanntwerden eine schwere Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen wahrscheinlich machen würde.

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

Voraussetzungen für den Zugang zu klassifizierten Informationen

§ 3. (1) Unbeschadet des § 1 darf der Zugang zu klassifizierten Informationen den jeweils betroffenen Personen nur unter folgenden Voraussetzungen gewährt werden:

1. einem Bediensteten einer Dienststelle des Bundes, wenn
   a) der Zugang zu diesen Informationen für die Erfüllung seiner dienstlichen Aufgaben erforderlich ist,
   b) er nachweislich ausreichend über den Umgang mit klassifizierten Informationen unterwiesen wurde und,

c) soweit Informationen betroffen sind, die als „VERTRAULICH“, „GEHEIM“ oder „STRENG GEHEIM“ klassifiziert wurden, eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG, BGBl. Nr. 566/1991, oder, sofern gesetzlich vorgesehen, eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG, BGBl. I Nr. 86/2000, durchgeführt wurde.

2. sonstigen Personen, wenn
   a) dies für die Ausübung einer im öffentlichen Interesse gelegenen Tätigkeit erforderlich ist,
   b) die Voraussetzungen der Z 1 lit. b und c vorliegen und
   c) kein geringerer als der von der zuständigen Dienststelle vorgesehene Schutzstandard gewährleistet wird.

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

(3) die nach § 26 DSG 2000 den Bediensteten einer Dienststelle des Bundes sowie sonstigen Personen in ihrer Eigenschaft als Betroffene (im Sinne des § 4 Z 3 DSG 2000) zustehenden Rechte werden durch die Regelungen der Abs. 1 und 2 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 Übereinkommen

§ 5. (1) Im Rahmen der Leistung von Amtshilfe dürfen klassifizierte Informationen nur weitergegeben 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 die Übermittlung klassifizierter Informationen schließen. Hiebei ist vorzusehen, dass klassifizierte Informationen nur dann übermittelt werden dürfen, wenn beim Empfänger ein Schutzstandard gewährleistet ist, der dem der übermittelnden Stelle gleichwertig ist.

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 Fall 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. Maßnahmen zur Überprüfung der weiteren Notwendigkeit der Klassifizierung,
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 Informationssicherheits-

kommission 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 Z 1 bis 2 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 Bundeskanzleramtes. 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 Austausches 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 entgegen den Bestimmungen dieses Bundesgesetzes eine ihm ausschließlich auf Grund von § 3 Abs. 1 dieses Bundesgesetzes anvertraute oder zugänglich gewordene, als „VERTRAULICH“, „GEHEIM“ oder „STRENG GEHEIM“ klassifizierte Information offenbart oder verwertet, deren Offenbarung oder Verwertung geeignet ist, die öffentliche Sicherheit, die umfassende Landesverteidigung oder die auswärtigen Beziehungen zu beeinträchtigen, ist, sofern die Tat nicht nach anderen Bundesgesetzen mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tag 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 3 000 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.

Vollziehung

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