P. b. b. Verlagspostamt 1040 Wien GZ 02Z034232 M

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2003 Ausgegeben am 28. November 2003 Teil II

548. Verordnung der Bundesregierung über die Informationssicherheit (Informationssicherheitsverordnung, InfoSiV)

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

Inhalt

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 Informationen, Tatsachen, Gegenstände und 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. elektronische Daten und Datenträger (E-Mail);
4. Tonträger;
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 und Deklassifizierung einer Information erfolgt durch ihren Urheber. Die Deklassifizierung ist schriftlich zu bestätigen. 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 **(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.

(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 hat jedenfalls die Kenntnisnahme der Bestimmungen des InfoSiG, dieser Verordnung, allfälliger weiterer schriftlich erlassener Durchführungsregelungen des Ressorts sowie der Folgen von Verstößen gegen die Geheimhaltungspflicht zu umfassen. Sie hat vor der Eröffnung des Zuganges zu klassifizierten Informationen zu erfolgen und ist jährlich zu wiederholen. Der Nachweis der durchgeführten Unterweisung ist schriftlich festzuhalten **(Anlage 2).**

(2) Mitarbeiter der Österreichischen Vertretung Brüssel, Mitglieder der nationalen Delegationen in EU-Gremien und sonstige Bedienstete, die mit EU-Verschlusssachen befasst sind, sind darüber hinaus über den Beschluss 2001/264/EG zu informieren.

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) Bei Hilfsmitteln, Material, Kanzleibehelfen und dergleichen, aus denen auf die klassifizierte Information geschlossen werden kann, hat deren Urheber dafür Sorge zu tragen, dass sie ebenso behandelt werden, wie die Information selbst.

(3) 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.

(4) Dokumente der Klassifizierungsstufe EINGESCHRÄNKT sind im verschlossenen Kuvert zu übermitteln. Dokumente der Klassifizierungsstufe VERTRAULICH oder höher sind grundsätzlich in einem doppelten undurchsichtigen Kuvert zu übermitteln, wobei am inneren Kuvert die Klassifizierungsstufe einschließlich der Anschrift des Empfängers anzugeben und eine Empfangsbestätigung beizulegen ist **(Anlage 3).**

(5) Bei der Übermittlung von klassifizierten Informationen wird wie folgt unterschieden:

1. mündliche Weitergabe: Bei Besprechungen mit einem Inhalt ab der Klassifizierungsstufe VERTRAULICH hat der Besprechungsleiter dafür Sorge zu tragen, dass die Teilnehmer entsprechend sicherheitsüberprüft und belehrt sind. Aufzeichnungen sind entsprechend zu klassifizieren. Bei der mündlichen Darlegung von Informationen, die als GEHEIM oder STRENG GEHEIM klassifiziert sind, sind abhörsichere Räume zu verwenden.
2. Telefongespräche und Fax: Die Weitergabe von klassifizierten Informationen hat grundsätzlich auf sicheren Leitungen zu erfolgen. Eine andere Weitergabe von klassifizierten Informationen der Klassifizierungsstufe VERTRAULICH ist nur in Ausnahmefällen bei Gefahr in Verzug zulässig und nach Identifikation des Empfängers so zu halten, dass der Sachverhalt Dritten unverständlich erscheint. Die Weitergabe von klassifizierten Informationen der Klassifizierungsstufe GEHEIM und STRENG GEHEIM bedarf entsprechender geschützter Informationswege, wobei der Inhalt zu verschlüsseln ist.
3. Persönliche Weitergabe: Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH, die persönlich verteilt 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.
4. Versendung durch die Post oder Zustelldienste: Innerhalb des Bundesgebietes darf die Übermittlung bis einschließlich der Klassifizierungsstufe GEHEIM durch die Post oder private Zusteller mit einer adäquaten Sicherheitsüberprüfung mittels Wertbrief oder Wertpaket erfolgen, wobei die Betragshöhe eine Ersatzzustellung ausschließen muss. Bei der Klassifizierungsstufe STRENG GEHEIM hat die Übermittlung durch Kurier zu erfolgen, wobei dieser entsprechend der Klassifizierungsstufe überprüft und ermächtigt **(Anlage 4)** sein muss. Die Versendung von klassifizierten

Informationen der Klassifizierungsstufe EINGESCHRÄNKT darf auf dem Postweg auch ins Ausland erfolgen, wobei dieselben Regeln wie für die Inlandszustellung einzuhalten sind.

5. Transport durch Kurier ins Ausland: Die Übermittlung von klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH hat unter Einhaltung des Abs. 4 im Wege diplomatischer oder militärischer Kuriere zu erfolgen. Stehen solche ausnahmsweise nicht zeitgerecht zur Verfügung, kann vom zuständigen Informationssicherheitsbeauftragten die persönliche Beförderung bis zur Klassifizierungsstufe GEHEIM gestattet werden, wobei der Beförderer selbst für die gesicherte Verwahrung verantwortlich ist.

Kennzeichnung

§ 8. (1) Klassifizierte Informationen sind eindeutig und gut erkennbar durch die im § 3 aufgezählten Bezeichnungen kenntlich zu machen. Bei schriftlichen Informationen ist auf jeder Seite der Vermerk am Kopf und am Fuß und eine Nummerierung anzubringen. Weiters ist das Datum und die Geschäftszahl, ab der Klassifizierungsstufe GEHEIM auf jeder Seite, anzubringen.

(2) Hinweise sind folgendermaßen anzubringen: Auf Dokumenten, die

1. als EINGESCHRÄNKT eingestuft sind, mit mechanischen oder elektronischen Mitteln,
2. als VERTRAULICH eingestuft sind, mit mechanischen Mitteln oder von Hand oder durch Druck auf vorgestempeltem, registriertem Papier,
3. als GEHEIM oder STRENG GEHEIM eingestuft sind, mit mechanischen Mitteln oder von Hand.

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

Elektronische Verarbeitung klassifizierter Informationen

§ 9. (1) Die Verarbeitung von klassifizierten Informationen mittels elektronischer Büro- und EDV-Geräte bedarf besonderer Sicherungsmaßnahmen, die abhängig sind von

– der Klassifizierungsstufe;
– dem Grad der Abstrahlsicherheit der Geräte;
– dem Ausmaß der Vernetzung;
– den Speichermöglichkeiten und
– den örtlichen Gegebenheiten.

(2) Klassifizierte Informationen der Klassifizierungsstufe VERTRAULICH dürfen auf allen Geräten verarbeitet werden, sofern keine Vernetzung mit Geräten außerhalb des Ressorts besteht. Klassifizierte Informationen der Klassifizierungsstufe GEHEIM dürfen überdies grundsätzlich nur auf Geräten verarbeitet werden, die als abstrahlungsarm deklariert sind; auf anderen Geräten nur in Ausnahmefällen, mit Zustimmung des Dienststellenleiters, kurzzeitig und in unregelmäßigen Abständen. Klassifizierte Informationen der Klassifizierungsstufe STRENG GEHEIM dürfen grundsätzlich nur auf Geräten verarbeitet werden, welche als abstrahlungsarm deklariert und nicht vernetzt sind; auf anderen nicht vernetzten Geräten nur in Ausnahmefällen, mit Zustimmung des Dienststellenleiters, kurzzeitig und in unregelmäßigen Abständen.

(3) Die Speicherung von klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH darf nur auf externen Datenträgern erfolgen. Auf demselben Datenträger dürfen dabei mehrere Informationen nur vom gleichen Bearbeiter gespeichert werden. Die Speicherung und Löschung ist am Geschäftsstück und in der Evidenz zu vermerken. Für die Speicherung von klassifizierten Informationen der Klassifizierungsstufe STRENG GEHEIM ist je Geschäftsstück ein eigener Datenträger zu verwenden.

(4) Auf Datenträgern gespeicherte Daten klassifizierten Inhalts ab der Klassifizierungsstufe VERTRAULICH sind nach Zweckerfüllung so zu löschen, dass eine Wiederherstellung nicht möglich ist. Die Löschung auf externen Datenträgern ist ausschließlich mittels systemimmanenten Löschungsprogrammen durchzuführen. Sollen alle Inhalte eines externen Datenträgers gelöscht werden, so ist dieser mechanisch zu vernichten.

(5) Eine Versendung von klassifizierten Informationen auf elektronischem Weg bedarf besonderer Schutzvorkehrungen, insbesondere der Verschlüsselung, die auf die jeweilige Klassifizierungsstufe abzustimmen ist.

(6) Externe Datenträger mit klassifiziertem Inhalt sind gemäß ihrer Klassifizierungsstufe zu kennzeichnen und getrennt nach Klassifizierungsstufen zu verwahren.

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.

Kanzleimäßige Behandlung

§ 11. (1) Klassifizierte Geschäftsstücke der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM sind in einem hiefür vorgesehenen Register (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 Kanzleisysteme 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 der Übermittlungsempfänger festzuhalten sind (Anlage 1). Nur der Leiter des Registers oder sein Stellvertreter dürfen den inneren Umschlag öffnen und den Empfang der klassifizierten Information bestätigen. Ist auf dem Umschlag ausdrücklich ein bestimmter Empfänger angeführt, so ist durch das Register lediglich der Eingang des Umschlages zu vermerken; nur der Empfänger darf den Umschlag öffnen und den Empfang der klassifizierten Information bestätigen.

(2) Die Registratur ist für die ordnungsgemäße Weitergabe von klassifizierten Informationen bei einem Zuständigkeitswechsel verantwortlich.

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. Sofern in diesen Räumen Informationen der Klassifizierungsstufe VERTRAULICH oder höher verwahrt und verarbeitet werden, ist für diese Räume eine vollständige Eingangs- und Ausgangskontrolle einzurichten, die sicherstellt, dass lediglich befugte und sicherheitsüberprüfte Personen und andere Personen ausschließlich in deren Begleitung den Bereich betreten können. Weiters ist darüber hinaus ein besonderes Sperrsystem und eine Kontrolle bzw. Überwachung der Räumlichkeiten außerhalb der Dienstzeiten erforderlich; sie sind erforderlichenfalls gegen Abhören zu sichern.

(2) Informationen gemäß § 2 Abs. 2 Z 1, 2 und 4 aller Klassifizierungsstufen sind in versperrbaren Behältnissen zu verwahren. Dabei sind für die Klassifizierungsstufe EINGESCHRÄNKT Aktenschränke, für VERTRAULICH Stahlschränke und für GEHEIM bzw. STRENG GEHEIM Tresore (im Sinne der ÖNORM EN 1143-1:1997, entsprechend der Zuordnung durch die Informationssicherheitskommission) zu verwenden. Die Schlüssel dieser Behältnisse sind kontrolliert in entsprechenden Sicherheitsbehältnissen zu verwahren und dürfen nicht aus den Amtsräumen verbracht werden; über die Ausgabe von Schlüsseln und Ersatzschlüsseln ist ein genaues Protokoll zu führen.

Kopien

§ 14. (1) Werden Kopien und Abschriften von Dokumenten der Klassifizierungsstufe VERTRAULICH oder GEHEIM angefertigt, so ist dies in geeigneter Weise festzuhalten. Jede Kopie ist durch einen geeigneten Zusatz zu individualisieren. Die Anfertigung von Kopien von Informationen der Klassifizierungsstufe STRENG GEHEIM durch Empfänger ist unzulässig. Kopien dürfen ausschließlich unter der unmittelbaren Verantwortung des jeweiligen Leiters der Organisationseinheit und unter Kennzeichnung als Kopie angefertigt werden.

(2) Dokumente der Klassifizierungsstufe VERTRAULICH oder GEHEIM dürfen nur von solchen Personen kopiert, abgeschrieben, 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 nachweislich zu vernichten; die Vernichtung von Informationen der Klassifizierungsstufen VERTRAULICH oder höher hat unter Anwesenheit von einer Person – bei der Klassifizierungsstufe STRENG GEHEIM von zwei Personen – zu erfolgen, die über eine Sicherheitsüberprüfung oder Verlässlichkeitsprüfung der entsprechenden Klassifizierungsstufe verfügen muss, und ist im Protokoll durch Unterschrift festzuhalten. **(Anlage 5)**

(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.

Verlust von klassifizierten Informationen

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

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 EDV-Systemen einer Überprüfung zu unterziehen. Liegen Informationen der Klassifizierungsstufe GEHEIM oder STRENG GEHEIM vor, so ist eine vollständige Überprüfung der Vorgänge des abgelaufenen Jahres vorzunehmen.

Schüssel Gorbach Ferrero-Waldner Gehrer Rauch-Kallat Grasser
Strasser Böhmdorfer Platter Pröll Haupt Bartenstein

Anlage 1

Register (Muster)

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

Evidenzliste gemäß §§ 5, 11 und 12 der Informationssicherheitsverordnung	
Dokumentenname	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang: ..... (Datum) ..... (Unterschrift)	
Eigene Geschäftszahl	
Entnahme: ..... (Datum) ..... (Unterschrift)	Rückgabe: ..... (Datum) ..... (Unterschrift)
…	
Weiterleitung/ Verteilung: ..... (Datum) ..... (Empfänger) ..... (Unterschrift des Übernehmers) *)	
…	
Vernichtung: ..... (Datum) ..... (Unterschrift)	

*) oder Beilage der Empfangsbestätigung

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)