Geheimschutzordnung des Bundes - GehSO

Auf Grund des § 12 Bundesministeriengesetz 1986, BGBl. Nr. 76, in der Fassung des Bundesgesetzes, BGBl. I Nr. 6/2007, wird verordnet:

Inhalt

Gegenstand

§ 1. (1) Art. 20 Abs. 3 B-VG verpflichtet alle mit Aufgaben der Bundes-, Landes- und Gemeindeverwaltung betrauten Organe, soweit gesetzlich nicht anderes bestimmt ist, zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordenen Tatsachen (Amtsverschwiegenheit).

(2) Die GehSO trifft nähere Regelungen über die Amtsverschwiegenheit und regelt darüber hinaus den Umgang mit Informationen, die einer besonderen Geheimhaltung unterliegen (klassifizierte Informationen). Die Rechtsgrundlage für die GehSO bildet § 12 des Bundesministeriengesetzes.

(3) Die GehSO gibt einen verbindlichen Mindeststandard für die einheitliche Behandlung klassifizierter Information vor, der aus Anlass der Umsetzung eine Ergänzung oder Präzisierung durch ressortspezifische Bestimmungen erfahren kann, welche sich im Inhalt und Aufbau an das System der GehSO halten. Zu diesen ist die Informationssicherheitskommission (ISK) zu hören.

(4) Ziel der GehSO ist das Erreichen eines Sicherheitsniveaus, das national klassifizierte Informationen bei moderaten Zusatzkosten adäquat schützt, sich an internationalen Bestimmungen und Begriffen orientiert und eine praktikable Handhabung von national klassifizierten Informationen ermöglicht. Wegen des mit der Klassifizierung von Informationen verbundenen Aufwandes ist streng darauf zu achten, dass nur solche Informationen klassifiziert werden, bei denen dies unabdingbar notwendig ist.

(5) Die Behandlung international klassifizierter Informationen aufgrund völkerrechtlicher Verpflichtungen ist im Informationssicherheitsgesetz (InfoSiG), BGBl. I Nr. 23/2002 idF 10/2006 bzw. in der Informationssicherheitsverordnung (InfoSiV), BGBl. II Nr. 548/2003, geregelt. Die GehSO folgt der Systematik dieser Vorschriften.

(6) Für interne Informationen der Verwaltung, die nicht in den Bereich klassifizierter Informationen im Sinn des §3 fallen und einen geringeren Schutzbedarf aufweisen, ist eine ausreichende Einschränkung der Zugriffsrechte vorzusehen.

Geltungsbereich

§ 2. Der Anwendungsbereich der GehSO erstreckt sich gemäß § 12 des Bundesministeriengesetzes auf die Zentralstellen der Bundesministerien.

Klassifizierte Informationen und Klassifizierungsstufen

§ 3. (1) Klassifizierte Informationen im Sinne der GehSO sind materielle und immaterielle Informationen, unabhängig von Darstellungsform und Datenträger, die auf Grund ihres Inhalts einer besonderen Geheimhaltung bedürfen und die daher nur einem begrenzten Personenkreis zugänglich gemacht werden sollen.

(2) Klassifizierte Informationen sind folgenden Klassifizierungsstufen zuzuordnen:

EINGESCHRÄNKT, wenn die unbefugte Weitergabe der Informationen Interessen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung, der auswärtigen Beziehungen, den wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder dem überwiegenden Interesse der Parteien zuwiderlaufen würde und die Informationen eines über die bloße Amtsverschwiegenheit hinausgehenden Schutzes bedürfen.

VERTRAULICH, wenn die Informationen eingeschränkt sind und die Preisgabe der Informationen die Gefahr einer Schädigung der Interessen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung oder der auswärtigen Beziehungen, der wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder der überwiegenden Interessen der Parteien schaffen würde,

GEHEIM, wenn die Informationen vertraulich sind und ihre Preisgabe die Gefahr einer erheblichen Schädigung der Interessen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung oder der auswärtigen Beziehungen, der wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder der überwiegenden Interessen der Parteien schaffen würde,

STRENG GEHEIM, wenn die Informationen geheim sind und überdies ihr bekannt werden eine schwere Schädigung der Interessen der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, der umfassenden Landesverteidigung oder der auswärtigen Beziehungen, der wirtschaftlichen Interessen einer Körperschaft des öffentlichen Rechts, der Vorbereitung einer Entscheidung oder der überwiegenden Interessen der Parteien wahrscheinlich machen würde.

(3) Bei der Wahl der Klassifizierungsstufe ist durch eine umsichtige und sachgerechte Vorgehensweise darauf zu achten, dass die tatsächlich geheimhaltungsbedürftigen Informationen effektiv geschützt und unnötige Sicherheitskosten vermieden werden.

Klassifizierung / Deklassifizierung

§ 4. (1) Klassifizierung bedeutet die Zuordnung einer Information zu einer Klassifizierungsstufe.

(2) Die Zuordnung von Informationen zu einer Klassifizierungsstufe hat durch die Urheber der Information oder deren Vorgesetzte zu erfolgen und ist im Anlassfall zu überprüfen.

(3) Deklassifizierung bedeutet die Aufhebung der Zuordnung zu einer Klassifizierungsstufe.

(4) Die Aufhebung bzw. die Herabsetzung der Zuordnung zu einer Klassifizierungsstufe hat ausschließlich durch die Urheber der Information oder deren Vorgesetzte zu erfolgen. Die Veränderung ist in jedem Falle zu dokumentieren.

(5) Wird die Information deklassifiziert, sind die Empfänger falls erforderlich davon zu benachrichtigen.

(6) Für Informationen, die aus einer nicht trennbaren Zusammenfassung von Informationen verschiedener Klassifizierungsstufen bestehen, ist zumindest die höchste im Paket auftretende Einzel-Klassifizierungsstufe zu verwenden, oder sofern erforderlich, eine höhere.

Kennzeichnung

§ 5. (1) Klassifizierte Informationen gemäß § 3 werden mit folgenden Klassifizierungsstufen gekennzeichnet:

EINGESCHRÄNKT
VERTRAULICH
GEHEIM
STRENG GEHEIM

(2) Diese Klassifizierung ist eindeutig und gut erkennbar anzubringen. Bei schriftlichen Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM sind auf jeder Seite der Klassifizierungsvermerk, eine Seitennummerierung, die Geschäftszahl und gegebenenfalls die Nummer der Ausfertigung zu vermerken.

Zugang zu klassifizierten Informationen

§ 6. (1) Bediensteten des Bundes darf der Zugang zu klassifizierten Informationen nur gewährt werden, wenn

1. dies für die Erfüllung der dienstlichen Aufgaben erforderlich ist,

2. der/die Bedienstete nachweislich gemäß § 7 Abs. 3 über den Umgang mit klassifizierten Informationen unterwiesen wurde und
3. bei Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM eine Sicherheitsüberprüfung gemäß Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991 idgF, §§ 55 bis 55b oder eine Verlässlichkeitsprüfung gemäß Militärbefugnisgesetz (MBG), BGBl. I Nr. 86/2000, idgF §§ 23 und 24 durchgeführt wurde. In besonderen Dringlichkeitsfällen kann vom Erfordernis gemäß § 7 Abs. 1 Z 3 abgesehen werden, wenn ansonsten eine rechtzeitige Bearbeitung einer Information der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM nicht möglich ist und die Verzögerung zu einem Schaden führen könnte, der das mit dem nicht Vorliegen einer Sicherheitsüberprüfung verbundene Schadensrisiko übersteigt. Eine entsprechende Sicherheitsüberprüfung bzw. Verlässlichkeitsprüfung ist jedoch umgehend nachzuholen.

(2) 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. 1 Z 2 und 3 vorliegen und der in der GehSO für diese Klassifizierungsstufe vorgesehene Schutzstandard gewährleistet wird.

(3) In jedem Ressort ist durch geeignete organisatorische 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 oder Verlässlichkeitsprüfung möglich ist. Dies gilt sinngemäß auch für den Zugang sonstiger Personen gem. Abs. 2.

(4) Ein/eine Bediensteter/Bedienstete hat sich vor dem Zugang zu klassifizierten Informationen zu vergewissern, dass die Voraussetzungen nach Abs. 1 gegeben sind.

Dienstpflichten

§ 7. (1) Die Dienstvorgesetzten haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche Mitarbeiter im Rahmen ihrer dienstlichen Aufgaben 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 eines unberechtigten Zugangs und ungewöhnliche Umstände im Zusammenhang mit der Sicherheit von Informationen umgehend der zuständigen Organisationseinheit bzw. Person zu melden. Andere gesetzliche Meldepflichten bleiben unberührt.

(3) Vor der Eröffnung des Zuganges zu klassifizierten Informationen hat eine nachweisliche Unterweisung der betroffenen Person zu erfolgen. Die Unterweisung hat jedenfalls die Kenntnisnahme dieser Geheimschutzordnung, allfälliger weiterer schriftlich erlassener Durchführungsregelungen des Ressorts sowie der Folgen von Verstößen gegen die Geheimhaltungspflicht zu umfassen.

Registrierung von klassifizierten Informationen

§ 8. (1) Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH sind zu registrieren. Dabei sind die Registrierungsnummer, die Urheber, die Geschäftszahl (sofern zu diesem Zeitpunkt bekannt), der Betreff, gegebenenfalls die Ausfertigungsnummer, das Datum des Geschäftstücks und die Klassifizierungsstufe zu vermerken. Bei klassifizierten Informationen, die nicht auf Papier vorliegen, ist analog vorzugehen. Dabei sind möglichst ein entsprechender Vermerk, der einen eindeutigen Zusammenhang mit der Registrierung herstellt, sowie die Klassifizierungsstufe auf der Information festzuhalten.

(2) Jeder Eingang und Ausgang eines klassifizierten Geschäftsstückes ab der Stufe VERTRAULICH ist zu registrieren, wobei die Urheber oder Absender, der Zeitpunkt des Einlangens, der Zeitpunkt der Übermittlung und die Übermittlungsempfänger festzuhalten sind.

(3) Die Registraturen sind von den zuständigen Stellen festzulegen.

Verwahrung von klassifizierten Informationen

§ 9. (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, die ausnahmslos von befugten und sicherheitsüberprüften Personen begleitet werden, den Bereich betreten können. Weiters ist darüber hinaus ein besonderes Sperrsystem und eine Kontrolle oder Überwachung der Räumlichkeiten außerhalb der Dienstzeiten erforderlich.

(2) Klassifizierte Informationen sind in versperrbaren Behältnissen zu verwahren. Dabei sind für die Klassifizierungsstufe EINGESCHRÄNKT Büromöbel, für VERTRAULICH, GEHEIM bzw. STRENG GEHEIM Tresore (entsprechend der Zuordnung durch die Informationssicherheitskommission) zu verwenden. Die Schlüssel dieser Behältnisse sind kontrolliert zu verwahren. Ab der Klassifizierungsstufe VERTRAULICH ist über die Ausgabe dieser Schlüssel (Zugangsmittel, Codes) ein Protokoll zu führen.

(3) Sofern für die Gebäude-, Personen- und Zutrittskontrolle zu den Räumlichkeiten ausreichende Maßnahmen zur Sicherstellung des erforderlichen Schutzniveaus gesetzt sind, können in den ressortspezifischen Durchführungsbestimmungen andere Regelungen hinsichtlich der Verwahrung von klassifizierten Informationen in Behältnissen vorgegeben werden. Die Beurteilung der Eignung hat im Einvernehmen mit dem übermittelnden Ressort und in Abstimmung mit der ISK zu erfolgen.

Übermittlung klassifizierter Informationen

§ 10. (1) Vor der Übermittlung von klassifizierten Informationen ist durch Prüfung im Einzelfall oder durch Einhaltung der hiefür vorgesehenen generellen Regelungen sicherzustellen, dass auf Empfängerseite die Voraussetzungen dieser Geheimschutzordnung eingehalten werden.

(2) 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/der Empfängers/Empfängerin anzugeben und eine Empfangsbestätigung beizulegen ist.

(3) Bei der mündlichen Weitergabe und bei Besprechungen mit einem Inhalt ab der Klassifizierungsstufe VERTRAULICH ist 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 soweit vorhanden abhörsichere Räume bzw. entsprechend geschützte Lokationen zu verwenden.

(4) Die Weitergabe von klassifizierten Informationen mittels Kommunikationsdiensten wie Telefon und Fax ist durch adäquate Schutzmechanismen abzusichern, die dem technischen Standard entsprechen. Für VERTRAULICH, GEHEIM und STRENG GEHEIM sind entsprechende durch die ISK zugelassene kryprographische Methoden einzusetzen. Abweichend davon dürfen durch Standardschutzmechanismen geschützte Verbindungen nur verwendet werden,

- wenn bei Telefongesprächen mit bis VERTRAULICH eingestuftem Inhalt die Erledigung der Angelegenheit dringlich ist und die schriftliche oder sonstige sichere Übermittlung einen unvertretbaren Zeitverlust bedeutete; die Gespräche sind so zu führen, dass der Sachverhalt Dritten nicht verständlich wird. Ist der Gesprächspartner nicht mit Sicherheit zu identifizieren, ist ein Kontrollanruf erforderlich
- wenn bei dringlichen Fax der Klassifizierungsstufe bis VERTRAULICH zwischen Absender und Empfänger für die erforderliche Übertragungsart keine Schutzmöglichkeit besteht; die absendende Stelle hat durch geeignete Maßnahmen vor der Übertragung zu gewährleisten, dass die Nachricht nur den/die berechtigten/berechtigte Empfänger/Empfängerin erreicht
- wenn in außergewöhnlichen Fällen aufgrund der Beurteilung der Dienststellenleitung eine rechtzeitige Beförderung der Information auf anderem Wege nicht möglich ist und eine Verzögerung zu einem Schaden führt, der den mit einer Preisgabe der Information verbundenen Schaden deutlich überwiegt.

(5) Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH, die persönlich verteilt werden, sind gegen Empfangsbestätigung zu übergeben. Die Übermittlung hat durch Personen zu erfolgen, die für die betreffende Klassifizierungsstufe ermächtigt sind. Dabei ist ein verschlossenes Kuvert zu verwenden, auf dem nur der Name des/der Empfängers/Empfängerin aufscheint; die Entgegennahme ist mit Empfangsbestätigung zu quittieren.

(6) Bei Versendung durch die Post oder Zustelldienste darf innerhalb des Bundesgebietes die Versendung von klassifizierten Informationen der Klassifizierungsstufen EINGESCHRÄNKT und VERTRAULICH nur mittels eingeschriebener Sendung erfolgen, wobei für die Klassifizierungsstufe VERTAULICH eine eigenhändige Zustellung erfolgen muss. Die Übermittlung von klassifizierten Informationen der Klassifizierungsstufen GEHEIM und STRENG GEHEIM darf nur mittels überprüften und geschulten Kurieren erfolgen.

(7) Die Versendung von klassifizierten Informationen der Klassifizierungsstufe EINGESCHRÄNKT darf auf dem Postweg auch ins Ausland erfolgen. Die Übermittlung von klassifizierten Informationen der Klassifizierungsstufe VERTRAULICH in das Ausland kann im Wege diplomatischer Kuriersendungen im Sinne des Art. 27 WDK (Wiener Übereinkommen über diplomatische Beziehungen) erfolgen. Klassifizierte Informationen der Klassifizierungsstufe GEHEIM und STRENG GEHEIM sind ausschließlich durch entsprechend überprüfte und geschulte Kuriere zu übermitteln.

Elektronische Verarbeitung / IKT-Systeme

§ 11. (1) Klassifizierte Informationen dürfen nur mit IKT-Systemen, Algorithmen und in Arbeitsprozessen verarbeitet, gespeichert und übermittelt werden, welche für die jeweiligen Klassifizierungsstufen geeignet sind. Die Beurteilung der Eignung ist vom jeweiligen Ressort in Abstimmung mit den Vorgaben der ISK zu treffen, wobei eine regelmäßige Überprüfung in Bezug auf geänderte Rahmenbedingungen durchzuführen ist.

(2) Die elektronische Verarbeitung von klassifizierten Informationen 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.

(3) Die Übermittlung von klassifizierten Informationen (elektronischer Transport klassifizierter Informationen oder Transport klassifizierter Informationen auf externen Datenträgern außerhalb gesicherter Bereiche bzw. kontrollierter Umgebungen) hat grundsätzlich mittels kryptographischer Produkte und Verfahren, die auf die jeweilige Klassifizierungsstufe abzustimmen und von der ISK zugelassen sind, zu erfolgen. Unverschlüsselte Dateinamen, Überschriften und Beschriftungen etc. dürfen dabei keine Rückschlüsse auf die klassifizierten Inhalte zulassen. Für die Übermittlung von klassifizierten Informationen ab der Stufe VERTRAULICH bedürfen die verwendeten Systeme der Zulassung durch die ISK.

(4) Findet die Übertragung innerhalb gesicherter Bereiche bzw. kontrollierter Umgebungen statt, kann unter Beachtung der Vorgaben der ISK bis zur Klassifizierungsstufe GEHEIM von einer Verschlüsselung abgesehen werden.

(5) Für die Klassifizierungsstufe EINGESCHRÄNKT ist je nach Gegebenheit sowohl eine Sicherung des Übertragungsweges mit kryptographischen Maßnahmen als auch eine Ende-zu-Ende-Verschlüsselung zulässig, wobei die hiefür eingesetzten Komponenten im Einflussbereich der jeweiligen Organisationseinheit liegen müssen. Beim Ausdruck EINGESCHRÄNKT klassifizierter Dokumente ist darauf zu achten, dass der Zugang zum Ausdruck nur für entsprechend unterwiesene Personen möglich sein darf.

(6) Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH dürfen nur auf Systemen verarbeitet werden, bei denen keine Vernetzung mit Systemen außerhalb des Ressorts besteht oder bei denen der Zugang mit geeigneten Methoden und Verfahren abgesichert ist. Außerdem ist der Zugang zu allen Geräten durch organisatorische, bauliche und technische Maßnahmen entsprechend zu schützen. Der Ausdruck von klassifizierten Dokumenten gilt als Kopie und ist daher als solche zu registrieren und gem. § 12 zu behandeln. Die elektronische Datensicherung von klassifizierten Informationen ab der Stufe VERTRAULICH darf nur in verschlüsselter Form entsprechend den Vorgaben der ISK unter sinngemäßer Anwendung des § 12 erfolgen.

(7) Klassifizierte Informationen ab der Klassifizierungsstufe GEHEIM dürfen nur auf Geräten verarbeitet werden, die als abstrahlungsarm deklariert sind. Werden anstelle dessen andere Schutzmaßnahmen ergriffen, kann von einer Verarbeitung auf abstrahlarmen Geräten abgesehen werden.

(8) Klassifizierte Informationen der Klassifizierungsstufe STRENG GEHEIM dürfen überdies nicht auf vernetzten Geräten verarbeitet werden.

(9) In IKT-Systemen ist sicherzustellen, dass der Zugriff zu klassifizierten Informationen nur unter der Voraussetzung des § 6 erfolgt und ab der Klassifizierungsstufe VERTRAULICH fälschungssicher protokolliert wird. Für jedes IKT-System, in dem klassifizierte Informationen verarbeitet werden, ist ein entsprechender Zugriffsschutz auf das System sicherzustellen.

Kopien

§ 12. (1) Werden Kopien oder Abschriften von Dokumenten der Klassifizierungsstufe VERTRAULICH oder GEHEIM angefertigt, so ist dies in geeigneter Weise festzuhalten und die Kopie als solche zu kennzeichnen und zu registrieren. 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/der jeweiligen Leiters/Leiterin der Organisationseinheit angefertigt werden.

(2) Dokumente der Klassifizierungsstufe EINGESCHRÄNKT, VERTRAULICH oder GEHEIM dürfen nur von solchen Personen kopiert, abgeschrieben, gescannt, archiviert oder verarbeitet werden, welche die Voraussetzungen des § 6 Abs. 1 und 2 erfüllen.

(3) Elektronisch vorliegende klassifizierte Informationen dürfen nur auf zugelassenen Systemen und unter sinngemäßer Anwendung der Bestimmungen der Abs. 1 und 2 kopiert werden. Die Protokollierung oder Dokumentation ist gemäß den für das jeweilige System verfügten Regelungen durchzuführen.

(4) Bei Kopiergeräten, auf denen klassifizierte Informationen verarbeitet werden, ist die unbefugte Reproduktion durch geeignete Maßnahmen zu verhindern. Dabei ist auch auf den Umgang mit den im Kopiergerät verwendeten Speichermedien zu achten.

Vernichtung von klassifizierten Informationen

§ 13. (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 einer weiteren Person – bei der Klassifizierungsstufe STRENG GEHEIM von zwei weiteren Personen – zu erfolgen, die über eine Sicherheitsüberprüfung oder Verlässlichkeitsprüfung der entsprechenden Klassifizierungsstufe verfügen müssen. Sie ist im Protokoll durch Unterschrift festzuhalten.

(2) Die verfassende Stelle hat auf den Ausfertigungen grundsätzlich zu vermerken, ob die klassifizierte Information zu einem bestimmten Zeitpunkt, nach Zweckerfüllung oder auf Weisung zu vernichten ist. Ist kein Vermerk angebracht, so hat die Dienststellenleitung der aufbewahrenden Stelle festzulegen, wann die klassifizierte Information zu vernichten ist. Erfolgt keine Festlegung, so ist die Information nach zehn Jahren zur Skartierung freigegeben.

(3) Datenträgern, insbesondere Festplatten, mit gespeicherten Informationen klassifizierter Art sind nach Zweckerfüllung unter Beachtung der Vorgaben der ISK zu vernichten.

(4) Beim Einsatz von Aktenvernichtungssystemen sind für den Zweck der sicheren Vernichtung entwickelte, handelsübliche Produkte unter Beachtung der Vorgaben der ISK zu verwenden.

Ungewöhnliche Vorfälle mit klassifizierten Informationen

§ 14. Ungewöhnliche Vorfälle, wie Verlust, das Nichtauffinden oder die Verfälschung von klassifizierten Informationen, sind unverzüglich der Dienststellenleitung und der mit der Sicherheit von klassifizierten Informationen zuständigen Organisationseinheit 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

§ 15. Das System der Informationssicherheit ist durch die zuständige Organisationseinheit einmal jährlich nachweislich zu überprüfen oder überprüfen zu lassen. Dabei sind insbesondere die Vollständigkeit der Aufzeichnungen, die Sicherheit der Behältnisse, das Schlüsselsystem und die Sicherungsmaßnahmen von IKT-Systemen einer Überprüfung zu unterziehen. Liegen Informationen der Klassifizierungsstufe STRENG GEHEIM vor, so ist eine vollständige Überprüfung der Vorgänge des abgelaufenen Jahres vorzunehmen.

Bundesministerium für Inneres

Richtlinien zur Anwendung der Geheimschutzordnung des Bundes

1. Allgemeines

Die GehSO ersetzt die bisherige Verschlusssachenordnung und gibt ressortübergreifend Mindeststandards zum Schutz national klassifizierter Informationen vor. Diese Standards orientieren sich im Wesentlichen an jenen, wie sie gemäß dem Informationssicherheitsgesetz (InfoSiG) für international klassifizierte Informationen gelten.

2. GehSO – Informationssicherheitsgesetz (InfoSiG)

Die GehSO regelt nur den Umgang mit national klassifizierten Informationen.
Sie gilt daher nicht für international klassifizierte Informationen gemäß § 2 Abs. 1 InfoSiG, die Österreich im Einklang mit völkerrechtlichen Regelungen erhalten hat, wie insb. EU-Dokumente. Derartige Dokumente unterliegen weiterhin ausschließlich den Regelungen des InfoSiG und der Informationssicherheitsverordnung (vgl. § 1 Abs. 5 GehSO). Ebenso bleiben die im Bereich des InfoSiG bestehenden Zuständigkeiten des Informationssicherheitsbeauftragten des BM.I gemäß § 7 InfoSiG sowie der [redacted] unberührt.
Inhaltlich folgt die GehSO weitestgehend der Systematik des InfoSiG, sodass die Systeme für national und international klassifizierte Informationen im Wesentlichen identisch sind; dies jedoch mit der Maßgabe, dass für nationale Informationen neben den vom InfoSiG übernommenen Klassifizierungen „Eingeschränkt" bis „Streng Geheim" weiterhin auch die Klassifizierung „Verschluss" als unterste Stufe zur Verfügung steht.

3. Klassifizierungsstufen

Auf Grundlage der GehSO können nationale Informationen in aufsteigender Reihenfolge folgenden Geheimhaltungsstufen zugeordnet werden:

1. Verschluss
   1.1. Verschluss - sensibel
2. Eingeschränkt
3. Vertraulich
4. Geheim
5. Streng Geheim

Mit diesen Klassifizierungen sind in aufsteigender Reihenfolge mit zunehmendem Geheimhaltungsinteresse auch zunehmend stringentere Mindestsicherheitsstandards und damit ein-

hergehend entsprechende Sicherheitskosten und Einschränkungen des Berechtigtenkreises sowie der faktischen Bearbeitungsmöglichkeiten verbunden.

Es ist daher darauf hinzuweisen, dass wegen des mit einer Klassifizierung verbundenen zusätzlichen Aufwandes nur solche Informationen klassifiziert werden, bei denen dies unabdingbar erforderlich ist, wobei bejahendenfalls – wie bisher – grundsätzlich mit der Stufe „Verschluss" (bzw. „Verschluss – sensibel") das Auslangen gefunden werden sollte.

Insbesondere aber sollte die Verwendung von „Vertraulich" oder höher im Hinblick auf die dann zur Anwendung gelangenden sehr hohen Sicherheitsstandards mit allen damit verbundenen Kosten und Einschränkungen nur auf allfällige exemplarische Ausnahmefälle beschränkt bleiben.

Zuordnungen zu einer Klassifizierungsstufe dürfen von Bediensteten nur soweit vorgenommen werden, als diese auch selbst die Zugangsvoraussetzungen für Informationen der jeweiligen Klassifizierungsstufe erfüllen (z.B. Sicherheitsüberprüfung bei Dokumenten ab „Vertraulich"). Unter Beachtung dieses Grundsatzes erfolgt die Zuordnung einer Information zu einer Klassifizierungsstufe durch die Urheber der Information oder deren Vorgesetzte.
Generell wird empfohlen, allfällige Klassifizierungen, insbesondere aber solche ab der Stufe „Vertraulich", nur nach vorhergehender Absprache mit dem unmittelbaren Vorgesetzten vorzunehmen.
Bei der Wahl des Empfängerkreises ist immer nach dem Grundsatz „Kenntnis nur wenn unbedingt nötig" vorzugehen.

4. Mindestsicherheitsstandards

Allgemein gilt, dass nur jene Bediensteten Zugang zu klassifizierten Informationen haben sollen, für die dies zur Erfüllung ihrer dienstlichen Aufgaben erforderlich ist (Eingeschränkter Zugang).
Vor jeder Übermittlung ist durch die übermittelnde Organisationseinheit zu prüfen, ob die Einhaltung der notwendigen Sicherheitsstandards auch auf Empfängerseite sichergestellt ist.
Die Sicherheitsstandards für die Originale gelten in gleicher Weise auch für Kopien.
Ebenso gelten die bei Papierdokumenten zu beachtenden Sicherheitsstandards, z.B. hinsichtlich der Aufbewahrung, in analoger Weise für elektronische Informationen auf externen Datenträgern (DVD, CD, Disketten, etc.).
Die Klassifizierungsstufen und die hierbei jeweils einzuhaltenden wesentlichen Mindestsicherheitsstandards sind in nachstehender Übersicht zusammenfassend dargestellt.

Übersicht der wesentlichen Mindestsicherheitsstandards

Sicherheitsmaßnahmen	GehSO	Verschluss	Eingeschränkt	Vertraulich	Geheim	Strong Geheim
Kennzeichnungspflicht	§ 5	Ja (auf der 1. Seite)	Ja (auf der 1. Seite)	Ja (auf jeder Seite)	Ja (auf jeder Seite)	Ja (auf jeder Seite)
Eingeschränkter Zugang	§ 6 Abs. 1 Z 1	Ja	Ja	Ja	Ja	Ja
Nachweisliche Unterweisung durch den Dienstvorgesetzten	§ 6 Abs. 1 Z 2	Möglich	Ja	Ja	Ja	Ja
Sicherheitsüberprüfung	§ 6 Abs. 1 Z 3	Nein	Nein	Ja	Ja	Ja
Registrierung	§ 8	Nein	Nein	Ja	Ja	Ja
Aufbewahrung - Raum	§ 9 Abs. 1	Normaler Raum	Normaler Raum	Raum mit Ein- und Ausgangskontrolle, Sperrsystem und Überwachung auch außerhalb der Dienstzeiten	Raum mit Ein- und Ausgangskontrolle, Sperrsystem und Überwachung auch außerhalb der Dienstzeiten	Raum mit Ein- und Ausgangskontrolle, Sperrsystem und Überwachung auch außerhalb der Dienstzeiten
Aufbewahrung - Behältnis	§ 9 Abs. 2	Versperrbare Büromöbel	Versperrbare Büromöbel	Tresore (Abhängig von den sonst. Sicherheitsmaßnahmen und in Abstimmung mit der ISK Ausnahmen möglich)	Tresore (Abhängig von den sonst. Sicherheitsmaßnahmen und in Abstimmung mit der ISK Ausnahmen möglich)	Tresore (Abhängig von den sonst. Sicherheitsmaßnahmen und in Abstimmung mit der ISK Ausnahmen möglich)
Übermittlung	§ 10 Abs. 2 u. 5	Einfach verschlossenes Kuvert	Einfach verschlossenes Kuvert	Doppeltes Kuvert	Doppeltes Kuvert	Doppeltes Kuvert
Empfangsbestätigung	§ 10 Abs. 2 u. 5	Nein	Nein	Ja	Ja	Ja
Versendung per Post	§ 10 Abs. 6	Eingeschrieben	Eingeschrieben	Eigenhändige Zustellung	Nein, Kurier	Nein, Kurier
Raum für Besprechungen	§ 10 Abs. 3	Normaler Raum	Normaler Raum	Normaler Raum	Abhörsicherer Raum bzw. entsprechend geschützte Lokation	Abhörsicherer Raum bzw. entsprechend geschützte Lokation
Telefon, Fax	§ 10 Abs. 4	Ja	Ja	Verschlüsselt (Ausnahmen in Dringlichkeitsfällen möglich)	Verschlüsselt	Verschlüsselt
Elektronische Verarbeitung	§ 11	Ja	Ja mit Verschlüsselung	Wie Eingeschränkt + Gerät ohne externe Vernetzung + Zugriffsprotokollierung + weitere Maßnahmen zum Schutz des Zugangs zu den Geräten	Wie Vertraulich + abstrahlungsarmes Gerät (oder adäquate Schutzmaßnahmen)	Wie Geheim + Gerät ohne (externe oder interne) Vernetzung
Elektronische Übermittlung	§ 11	Ja	Ja mit Verschlüsselung	Von der ISK zugelassene Systeme	Von der ISK zugelassene Systeme	Von der ISK zugelassene Systeme
Elektronische Datensicherung	§ 11 Abs. 6 u. § 12	Ja	Ja	Verschlüsselt mit Kennzeichnung als Sicherung und Registrierung	Verschlüsselt mit Kennzeichnung als Sicherung und Registrierung	Verschlüsselt mit Kennzeichnung als Sicherung und Registrierung; nicht durch Empfänger erlaubt
Protokollierung des elektronischen Zugriffs	§ 11 Abs. 9	Nein	Nein	Fälschungssicher protokolliert	Fälschungssicher protokolliert	Fälschungssicher protokolliert
Elektr. Verarbeitung / Übermittlung im **ELAK**	§ 11	Ja	Ja mit Verschlüsselung der Inhalte	Nein	Nein	Nein
Elektr. Verarbeitung / Übermittlung auf „normalen" **BAKS**-Geräten, **E-Mail**	§ 11	Ja	Ja mit Verschlüsselung der Inhalte	Nein	Nein	Nein
Anfertigung von Kopien und Ausdrucken	§ 12	Ja	Ja	Ja mit Kennzeichnung als Kopie, entsprechender Dokumentation und Registrierung	Ja mit Kennzeichnung als Kopie, entsprechender Dokumentation und Registrierung	Wie Geheim, jedoch keine Kopien durch Empfänger
Vernichtung	§ 13	Nachweisliche Vernichtung	Nachweisliche Vernichtung	Vernichtungsprotokoll bei Anwesenheit von 1 weiteren Person	Vernichtungsprotokoll bei Anwesenheit von 1 weiteren Person	Vernichtungsprotokoll bei Anwesenheit von 2 weiteren Person

Im Folgenden wird auf einige der notwendigen Sicherheitsmaßnahmen im Zusammenhang mit der jeweiligen Klassifizierung näher eingegangen.

4.1. Verschluss

„Verschluss" ist die Klassifizierung gem. § 1 Abs. 6 GehSO für besonders schutzbedürftige ressortinterne Informationen unterhalb der Geheimhaltungsstufen „Eingeschränkt" bis „Streng Geheim" gemäß § 3 GehSO.

Auf Informationen der Stufe „Verschluss" finden die für „Eingeschränkt" vorgesehenen Bestimmungen der GehSO mit folgenden Besonderheiten Anwendung:

- Eine nachweisliche Unterweisung der mit Verschlussinformationen befassten Bediensteten durch den Dienstvorgesetzten ist nicht zwingend erforderlich.
- Die elektronische Verarbeitung/Übermittlung, insb. auch im ELAK, ist unter Beachtung des Prinzips des eingeschränkten Zugangs zu Verschlussinformationen zulässig. Eine Verschlüsselung der Informationen ist im Gegensatz zu „Eingeschränkt" nicht notwendig.
- Im ELAK haben die im Workflow ad personam beteiligten Benutzer, deren Vorgesetze und – falls vorhanden – ein Verschlussbearbeiter sowie die zuständigen Kanzlisten Zugriffsrechte (neben den generellen aus technischen Gründen notwendigen Rechten von Ressort- und Domänenadministratoren sowie allfälligen im Anlassfall eingerichteten Rechten von Revisoren).

Ansonsten gelten die für „Eingeschränkt"-Informationen vorgesehenen Standards, wie z.B.:

- Kennzeichnung der Information mit der Klassifizierungsstufe
- Übermittlung in einem einfach verschlossenen Kuvert
- Aufbewahrung in versperrbaren Aktenschränken
- Nachweisliche Vernichtung

Zusammengefasst entspricht daher die Stufe „Verschluss" im Wesentlichen dem bisherigen „Verschluss" gemäß der Verschlusssachenordnung.

4.1.1 Verschluss - sensibel

Die Sonderform „Verschluss – sensibel" ist im ELAK verfügbar und bewirkt eine weitere Einschränkung der Zugriffsrechte im Vergleich zum normalen „Verschluss", indem bei dieser Klassifizierung Kanzlisten im ELAK keinen Zugriff mehr auf den betreffenden Akt haben.

4.2. Eingeschränkt

Die wesentlichen Sicherheitsstandards für Informationen ab der Stufe „Eingeschränkt" sind insbesondere:

- Kennzeichnung der Information mit der Klassifizierungsstufe
- Nachweisliche Unterweisung der mit „Eingeschränkt"-Informationen befassten Bediensteten durch den Dienstvorgesetzten (Anlage 2); dem Bediensteten ist eine Ausfertigung des „Nachweises der Unterweisung" auszuhändigen, das Original verbleibt beim Dienstvorgesetzten.
- Übermittlung in einem einfach verschlossenen Kuvert
- Aufbewahrung in versperrbaren Aktenschränken
- Nachweisliche Vernichtung (es genügt der Hinweis in einem Aktenverwaltungsystem auf die erfolgte Skartierung; ein eigenes Vernichtungsprotokoll ist im Gegensatz zu Informationen ab der Stufe „Vertraulich" nicht erforderlich)
- Die elektronische Verarbeitung/Übermittlung ist nur unter der Voraussetzung der Verschlüsselung der Inhaltsdaten zulässig; dies gilt insb. auch für den ELAK, die Bearbeitung auf BAKS-Geräten, Übermittlungen per E-Mail, etc.

4.3. Vertraulich oder höher

Ab der Stufe „Vertraulich" sind weitergehende, besondere Sicherheitsmaßnahmen zu treffen.

4.3.1 Zuständige Registraturen gemäß § 8 Abs. 3 GehSO (Geheimschutzkanzleien)

Klassifizierte Informationen der Stufe „Vertraulich" oder höher sind gemäß § 8 GehSO zu registrieren.

Die hierfür zuständige Registratur gemäß § 8 Abs. 3 GehSO ist für das Bundesministerium für Inneres, [redacted].

Für [redacted] sind die dortigen Kanzleien auch zuständige Registraturen gemäß § 8 Abs. 3 GehSO.

Im Bedarfsfall können nach vorgehender Genehmigung durch die Sektion I weitere Registraturen für einzelne Bereiche eingerichtet werden.

4.3.2 Sicherheitsüberprüfung

Der Zugang zu Informationen ab der Stufe „Vertraulich" darf nur Bediensteten gewährt werden, die die für die jeweilige Klassifizierungsstufe notwendige Sicherheitsüberprüfung gemäß dem SPG aufweisen. Entsprechende Anträge auf Sicherheitsüberprüfung sind im Bedarfsfall von den jeweiligen Fach-OE an das BVT zu richten.

Über die Berechtigung, nach erfolgter Sicherheitsüberprüfung klassifizierte Informationen einzusehen bzw. zu übermitteln, ist den Bediensteten von der/dem Leiter/in der Fach-OE eine Bescheinigung auszustellen (Anlage 4). Eine Ausfertigung der Bescheinigung ist der Abteilung I/2 zu übermitteln.
Nur unter den Voraussetzungen gemäß § 6 Abs. 1 Z 3 GehSO kann in besonderen Dringlichkeitsfällen vom Erfordernis einer Sicherheitsüberprüfung vorerst abgesehen werden. In diesen Fällen ist die Sicherheitsüberprüfung umgehend nachzuholen.

4.3.3 Registrierung

Alle nationalen Informationen der Stufe „Vertraulich" oder höher, die beim BM.I einlangen oder innerhalb des BM.I erstellt werden, sind der zuständigen Registratur zur Registrierung zu übermitteln bzw. vorzulegen. Das Register wird inhaltlich gemäß beiliegendem Muster (Anlage 1) geführt.

4.3.4 Aufbewahrung

Die Aufbewahrung erfolgt im Wege der Registratur unter Beachtung der Vorgaben gemäß § 9 GehSO (insb. hinsichtlich der Aufbewahrung in Tresoren in Räumen mit vollständiger Eingangs- und Ausgangskontrolle, inkl. einer Kontrolle und Überwachung der Räumlichkeiten auch außerhalb der Dienstzeiten).
Im Falle [redacted] erfolgt die Aufbewahrung in einem Tresor im [redacted]. Zugang zu Tresor und Raum haben [redacted]. Auch im Falle [redacted] erfolgt die Aufbewahrung im [redacted], jedoch in einem separaten Tresor. Zugang zu diesem Tresor und Raum haben [redacted].

4.3.5 Einsichtnahme/Entnahme

Einsichtnahmen/Entnahmen erfolgen gegen Vorlage der Bescheinigung über die Zugangsberechtigung zu klassifizierten Informationen (Anlage 4) im Wege der Registratur im Aufbewahrungsraum.
Kurzfristige Entnahmen von klassifizierten Informationen aus dem Aufbewahrungsraum sind zulässig, wenn – gegebenenfalls nach vorhergehender Absprache mit der Registratur – sichergestellt ist, dass die Dokumente am selben Arbeitstag wieder rückgemittelt werden.
Darüber hinausgehende längerfristige Entnahmen von klassifizierten Informationen aus dem Aufbewahrungsraum sind nur zulässig, wenn beim Empfänger die Einhaltung der für die Verwahrung geltenden Sicherheitsvorschriften gem. § 9 GehSO sichergestellt ist.
Entnahme und Rückgabe sind im Register zu verbuchen.

4.3.6 Übermittlung

Die Übermittlung erfolgt grundsätzlich in einem doppelten undurchsichtigen Kuvert und gegen Empfangsbestätigung (Anlage 3).

Die Übermittlung darf nur durch Personen zu erfolgen, die für die jeweilige Klassifizierungsstufe ermächtigt, d.h. insbesondere sicherheitsüberprüft sind.

Die postalische Übermittlung von Dokumenten der Stufe „Vertraulich" ist als Zustellung zu eigenen Handen möglich. Dokumente der Stufen „Geheim" und „Streng Geheim" dürfen nur mittels eigens überprüften und geschulten Kurieren übermittelt werden.

4.3.7 Elektronische Verarbeitung

Die Verarbeitung von Informationen ab der Stufe „Vertraulich" auf Standard-BAKS-Geräten ist zum gegenwärtigen Zeitpunkt, insb. wg. deren Anbindung an externe Systeme (insb. Internet), ausgeschlossen.

Dokumente der Stufe „Vertraulich" dürfen nur auf Geräten ohne externe Vernetzung mit fälschungssicherer Zugriffsprotokollierung und Dokumente der Stufe „Geheim" zudem nur auf sog. „abstrahlungsarmen" Geräten verarbeitet werden. Dokumente der Stufe „Streng Geheim" dürfen überhaupt nur auf (Stand-Alone)Geräten ohne jedwede externe oder interne Vernetzung verarbeitet werden.

In allen Fällen ist der Zugang zu den Geräten, auf denen Informationen ab der Stufe „Vertraulich" verarbeitet werden sollen, zusätzlich durch entsprechende organisatorische, bauliche und technische Maßnahmen – ähnlich den Maßnahmen, wie sie für die Aufbewahrung von vergleichbaren Papierdokumenten vorgesehen sind – zu schützen.

Es wird empfohlen, diese Grundsätze bereits bei der Erstellung von vorerst noch nicht klassifizierten elektronischen Dokumenten zu beachten, wenn diese für eine Klassifizierung ab der Stufe „Vertraulich" vorgesehen sind.

4.3.8 Elektronische Übermittlung

Die interne oder externe elektronische Übermittlung von Dokumenten ab der Stufe „Vertraulich" ist nur auf bzw. im Rahmen von Systemen zulässig, die von der im Bundeskanzleramt eingerichteten Informationssicherheitskommission (ISK) zugelassen worden sind. Da dies auf die vom BM.I betriebenen Systeme zum gegenwärtigen Zeitpunkt nicht zutrifft, ist die interne oder externe elektronische Übermittlung (insb. per E-Mail) von Dokumenten ab der Stufe „Vertraulich" zum gegenwärtigen Zeitpunkt ausgeschlossen.

4.3.9 Vernichtung

Die Vernichtung von „Vertraulich"- und „Geheim"-Informationen ist unter Anwesenheit von einer, die Vernichtung von „Streng Geheim"-Dokumenten unter Anwesenheit von zwei weiteren Personen in einem Vernichtungsprotokoll (Anlage 5) festzuhalten, wobei die von der im

Bundeskanzleramt eingerichteten Informationssicherheitskommission (ISK) vorgesehenen Vernichtungsmethoden anzuwenden sind.

Anlagen[1]

Anlage 1: Inhalt des Registers gemäß § 8 GehSO

Anlage 2: Nachweis der Unterweisung gemäß § 7 Abs. 3 GehSO

Anlage 3: Empfangsbestätigung gemäß § 10 Abs. 5 GehSO

Anlage 4: Bescheinigung über die Zugangsberechtigung zu klassifizierten Informationen

Anlage 5: Vernichtungsprotokoll gemäß § 13 Abs. 1 GehSO

[1] Die Anlagen stehen auch im BM.I-Intranet im Downloadbereich der Sektion I zur Verfügung.

Inhalt des Registers gemäß § 8 GehSO

• Dokumentenname/Betreff		
• Geschäftszahl (Fremdzahl)		
• Ausfertigungsnummer		
• Datum		
• Seitenumfang		
• Klassifizierungsstufe		
• Urheber		
• Eingang:	..... (Datum) ..... (Unterschrift)	
• Registernummer		
• 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

gemäß § 7 Abs. 3 GehSO

Hiermit wird bestätigt, dass

Herr/Frau .....

gemäß § 7 Abs. 3 der Geheimschutzordnung eine Ausfertigung der Geheimschutzordnung sowie der BM.I-internen Richtlinien zu deren Anwendung erhalten hat, über die sich daraus ergebenden Pflichten und über die Folgen von Verstößen gegen die Geheimschutzordnung informiert wurde.

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

Anlage 3

Empfangsbestätigung

gemäß § 10 Abs. 5 GehSO

Der/die Empfänger/in ..... bestätigt den Empfang von

Stückzahl	Absender	GZ, Ausfertigungsnummer	Beilagen

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

.....
Name in Druckschrift

.....
Unterschrift

....
(Dienststelle/Organisationseinheit) (Datum)

Bescheinigung

über die Zugangsberechtigung zu klassifizierten Informationen

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

Dienstausweis(Personal)-Nr.:.....

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

klassifizierte Informationen
EINGESCHRÄNKT *)
VERTRAULICH *)
GEHEIM *)
STRENG GEHEIM *)

für .....
(Dienststelle/Organisationseinheit)

ZU ÜBERMITTELN *)

ZU ÜBERMITTELN UND EINZUSEHEN *)

.

Der/die Leiter/in:

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

*) Nichtzutreffendes streichen

Vernichtungsprotokoll

gemäß § 13 Abs. 1 GehSO

Folgendes klassifiziertes Dokument wurde vernichtet:

Dokumentenname	
Registernummer	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang	

Art der Vernichtung:

Name/n des/der Zeugen in Druckschrift:

Organisationseinheit:

..... (Datum)

..... (Unterschrift)