Bundesministerium für Landesverteidigung
GZ S90619/1-Präs/2025

Geheimschutzvorschrift

WIEN, 18. September 2025

Genehmigung und Herausgabe

Geheimschutzvorschrift

Dieser Erlass tritt mit dem Genehmigungsdatum in Kraft.

**Mit dem gleichen Datum wird dessen Vorversion,
GZ S90619/1-S I/2011, außer Kraft gesetzt.**

Genehmigt:

WIEN, 18. September 2025
Für die Bundesministerin:
AbtLtr Mag. Christoph MOSER

VORWORT

Die Geheimschutzvorschrift (GehSchV) **bezweckt** die Sicherstellung berechtigter Geheimhaltungsinteressen, den Schutz von Staatsgeheimnissen und militärischen Geheimnissen sowie die Umsetzung der völkerrechtlichen/internationalen Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen im Ressortbereich des Bundesministeriums für Landesverteidigung (BMLV) mit Einschluss des ÖBH.

Sie **beschreibt** den Vorgang der Klassifizierung von Informationen und definiert die einzelnen Klassifizierungsstufen, enthält die Aufgaben und den Verantwortungsbereich des Informationssicherheitspersonals und regelt den Umgang mit klassifizierten Informationen, sowohl für den nationalen als auch den internationalen Bereich.

Die vorliegende Neufassung berücksichtigt die Erfahrungen aus dem bisherigen Anwendungszeitraum seit dem Jahr 2011 sowie insbesondere die Bestimmungen des mit 1. September 2025 in Kraft getretenen Informationsfreiheitsgesetzes (IFG).

Fachliche Anmerkungen sowie allfällige Anpassungsnotwendigkeiten aufgrund der Erfahrungen der praktischen Anwendung der Geheimschutzvorschrift sind **schriftlich auf dem Dienstweg an die Abteilung Präsidiale** zu melden.

Mit Vorliegen der Erfahrungsberichte wird die Geheimschutzvorschrift evaluiert. Allfällige weitere Änderungen werden durch die Abteilung Präsidiale im Einvernehmen mit dem AbwA festgelegt.

Sprachliche Gleichbehandlung

Die in dieser Dienstvorschrift verwendeten personenbezogenen Ausdrücke betreffen – soweit dies inhaltlich in Betracht kommt – Frauen und Männer gleichermaßen.

ZUORDNUNG

Eine Zuordnung im herkömmlichen Sinn ist durch die digitale Bereitstellung mit Druckberechtigung nicht erforderlich.

Die Verteilung innerhalb der Kommanden (ab Einheitsebene) und Dienststellen obliegt den jeweiligen Kommandanten bzw. Dienststellenleitern.

HINWEIS:	Unterlagen zum Themenbereich Geheimschutz stehen auf der Homepage der Abteilung Präsidiale im Intranet zum Download bereit.

ERGÄNZUNGS- UND ÄNDERUNGSBLATT

lfd. Nr.	Ergänzungs- und Änderungserlass	Datum der Durchführung

INHALTSVERZEICHNIS

A. ALLGEMEINES

I. Rechtsgrundlagen

Rechtsgrundlagen für die Geheimschutzvorschrift – in der Folge auch unter der Abkürzung GehSchV verwendet – sind **insbesondere:** **1**

- Art. 22a Abs. 2 des Bundes-Verfassungsgesetzes (B-VG),
- Informationssicherheitsgesetz (InfoSiG),
- Informationsfreiheitsgesetz (IFG),
- Datenschutzgesetz (DSG),
- Informationssicherheitsverordnung (InfoSiV),
- § 46 des Beamten-Dienstrechtgesetzes (BDG),
- § 5 des Vertragsbedienstetengesetzes (VBG),
- § 11 Abs. 2 des Wehrgesetzes 2001 (WG 2001),
- §§ 26 bis 28 des Militärstrafgesetzes (MilStG),
- §§ 252 bis 255 und § 310 des Strafgesetzbuches (StGB),
- § 1 Abs. 5 des Militärbefugnisgesetzes (MBG),
- § 12 des Bundesministeriengesetzes (BMG).

II. Geltungsbereich

2 Die **Geheimschutzvorschrift gilt im gesamten Ressortbereich** des Bundesministeriums für Landesverteidigung (BMLV).

3 Als **Dienststellen** im Sinne dieser Dienstvorschrift gelten im Bereich der Zentralstelle des BMLV auch die Organisationseinheiten gemäß Bundesministeriengesetz.

4 Die **Leiter** des **Heeres-Nachrichtenamtes** und des **Abwehramtes** regeln für ihren jeweiligen Wirkungsbereich den Verkehr mit klassifizierten Informationen in Anlehnung an die Bestimmungen dieser Dienstvorschrift nach den besonderen Erfordernissen der militärischen Nachrichtendienste.

5 Die Geheimschutzvorschrift ist sowohl auf **nationale** als auch **internationale klassifizierte Informationen** anzuwenden.

Sofern aufgrund völkerrechtlicher Vereinbarungen **strengere Geheimschutzbestimmungen** festgelegt wurden, sind diese für die betreffenden klassifizierten Informationen anzuwenden.

Diese werden im Bedarfsfall durch den **Ltr des Abwehramtes** in seiner Funktion **als Informationssicherheitsbeauftragter** festgelegt.

6 Im **Einsatz** und bei **Übungen** obliegt es den **Kommandanten, abweichende Regelungen** für den Geheimschutz zu verfügen.

III. Grundsätze

Zielsetzung dieser Dienstvorschrift ist die **Gleichbehandlung von nationalen und internationalen Informationen,** um die Akzeptanz zu erhöhen und die administrativen und formalen Maßnahmen für Bedienstete im Bereich des Geheimschutzes möglichst einfach zu halten. **7**

entfällt **8**

entfällt **9**

Personen darf der **Zugang zu klassifizierten Informationen** nur gewährt werden, **10**

– wenn und solange dies für die Erfüllung ihrer dienstlichen Aufgaben erforderlich ist (**„need to know" Prinzip**) und
– wenn sie entsprechend unterwiesen und ab der Klassifizierungsstufe VERTRAULICH aufwärts überprüft wurden (s. RdNr. 52 - 58).

Weiterns gilt für alle Bediensteten im Ressort die **„Clear Desk Policy"**. Das bedeutet, dass außerhalb der Dienstzeit keine dienstlichen Schriftstücke, Arbeitsunterlagen, Stempel, Chipkarten etc. in den Kanzleiräumen frei zugänglich sein dürfen. **11**

Der **Bestand** an klassifizierten Informationen ist möglichst **gering** zu **halten.** **12**

Klassifizierte Informationen sind entsprechend dieser Dienstvorschrift zu **kennzeichnen**. **13**

Entsprechend dieser Dienstvorschrift sind **14**

– der Bestand,
– der Zugang,
– die Übergabe und
– die Vernichtung

von klassifizierten Informationen zu dokumentieren.

15 Klassifizierte Informationen sind **gesichert zu verwahren** und vor **unbefugtem Zugriff** zu schützen.

16 **Informations**- und **Kommunikationstechnik** zur Verarbeitung, Übertragung und Speicherung von klassifizierten Informationen ist vor Verwendung im BMLV einem **Zulassungsverfahren** zu unterziehen.

17 **Internationale klassifizierte Informationen** gemäß dieser Dienstvorschrift sind alle klassifizierten Informationen, die unter Zugrundelegung völkerrechtlicher Verpflichtungen oder Bestimmungen klassifiziert wurden.

18 **Multilateral klassifizierte Informationen** gemäß dieser Dienstvorschrift sind klassifizierte Informationen, die mit Klassifizierungsvermerken nach den Bestimmungen der NATO und der EU versehen sind.

19 Im **multilateralen Bereich** nehmen die **Zentralregister EU und NATO** bei BMLV/MilPol die Rechte des Verfassers wahr.

20 **Register** bezeichnet in dieser Vorschrift das jeweils zu Anwendung kommende Instrument zur Registrierung und/oder Verbuchung von klassifizierten Informationen. Es können dies sowohl Bestandverzeichnisse oder Geschäftsbücher als auch Datenbanken in zugelassenen IKT-Systemen sein.

B. KLASSIFIZIERTE INFORMATIONEN

I. Begriff

Klassifizierte Informationen sind Informationen, Tatsachen, Gegenstände und Nachrichten (unabhängig von Darstellungsform und Datenträger), die eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen. **21**

Klassifizierte Informationen **können insbesondere sein:** **22**

- Schriftstücke,
- Zeichnungen,
- Pläne,
- Karten,
- Bildmaterial,
- elektronische Daten und Datenträger,
- Tonträger,
- Amtssiegel,
- technische Geräte,
- technische Systeme und/oder deren Teilkomponenten, sofern darauf klassifizierte Informationen enthalten sind oder verarbeitet werden,
- Geschäftsbücher und Bestandsverzeichnisse (auch als Datenbank in zugelassenen IKT-Systemen).

Arbeitsbehelfe, Entwürfe, Konzepte, Besprechungs- und/oder Unterrichtsunterlagen, sind aufgrund ihres Inhaltes und der in Aussicht genommenen Klassifizierung nach den Bestimmungen dieser Vorschrift zu behandeln. Sofern sie nicht für die Nachvollziehbarkeit und Dokumentation von Geschäftsfällen benötigt werden, können sie nach Zweckerfüllung vernichtet werden.

II. Klassifizierung

23 Die **Klassifizierung einer Information** ist die Zuordnung einer Klassifizierungsstufe für diese Information.

24 Die **Klassifizierungsstufe** ist auf Grund des Schutzbedarfes der Information hinsichtlich des Schutzes vor Zugriff durch Unbefugte unter Berücksichtigung der in RdNr. 34 bis RdNr. 37 bei den einzelnen Klassifizierungsstufen angeführten Kriterien durch den Verfasser der Information festzulegen.

25 Die Zuordnung einer Klassifizierungsstufe hat unter **Abwägung** der erforderlichen **administrativen** und **sicherheitsmäßigen Aufwendungen** gegenüber **dem im Fall einer Preisgabe zu erwartenden Schaden** zu erfolgen.

26 **Ab** der **Klassifizierungsstufe VERTRAULICH** hat die Festlegung der Klassifizierungsstufe durch den Kommandanten/Dienststellenleiter (Ebene kleiner Verband/Abteilung) zu erfolgen.

27 Die **Deklassifizierung** ist die ersatzlose Aufhebung der Klassifizierung einer Information.

28 Wenn sich auf Grund einer **Änderung der Sachlage** oder **auf Grund des Zeitablaufes der Schutzbedarf** einer Information ändert, ist die Klassifizierungsstufe durch jene Stelle, welche die Klassifizierungsstufe festgelegt hat, entsprechend anzupassen oder aufzuheben.

29 Die **Hinaufsetzung oder Herabsetzung** der Klassifizierungsstufe oder die Deklassifizierung ist zu **dokumentieren.** Die **Empfänger** der klassifizierten Information sind davon **in Kenntnis** zu **setzen.**

Die **Änderung** der Klassifizierung von **multilateral klassifizierten Informationen** ist nur auf schriftliche Weisung der Zentralregistratur BMLV zulässig. **30**

Informationen, die sich auf **klassifizierte Informationen beziehen** (zB Stellungnahmen, Berichtigungen, Ergänzungen, Einladungen zu Besprechungen), sind, sofern sie keinen oder nur einen geminderten Rückschluss auf einen Inhalt zulassen, entweder mit einer herabgesetzten Klassifizierungsstufe zu versehen oder nicht zu klassifizieren. **31**

Haben zusammengefasste/zusammengeführte klassifizierte Informationen **verschiedene Klassifizierungsstufen**, so ist für die zusammengefasste/zusammengeführte klassifizierte Information die **jeweils höchste Klassifizierungsstufe** zu verwenden. Die Teile (zB Beilagen) behalten ihre Klassifizierungsstufe und können für sich alleine nach dieser Klassifizierungsstufe behandelt werden. **32**

Darüber hinaus ist zu prüfen, ob nicht aufgrund des Zusammenschlusses mehrerer klassifizierter Informationen die **Schutzwürdigkeit gestiegen** und daher eine **höhere Klassifizierungsstufe erforderlich** ist. **33**

Bei Geräten oder Komponenten, die als schutzwürdig zu beurteilen sind, hat die systemverantwortliche Dienststelle bei der Herstellung der Verwendungsreife in der Einführungsphase die Klassifizierung festzulegen und in der Beschreibung zu dokumentieren. Bei Bestandsgerät ist durch die systemverantwortliche Dienststelle sinngemäß zu verfahren.

III. Klassifizierungsstufen

1. EINGESCHRÄNKT (E)

34 **Eingeschränkt** sind klassifizierte Informationen, deren unbefugte Weitergabe den in § 6 Abs. 1 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG) genannten Interessen zuwider laufen würde. Zu diesen zählen:

1. zwingende integrations- oder außenpolitische Gründe, insbesondere auch gemäß unmittelbar anwendbaren Bestimmungen des Rechts der Europäischen Union oder zur Einhaltung völkerrechtlicher Verpflichtungen,
2. Interesse der nationalen Sicherheit,
3. Interesse der umfassenden Landesverteidigung,
4. Interesse der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit,
5. Interesse der unbeeinträchtigten Vorbereitung einer Entscheidung, im Sinne der unbeeinträchtigten rechtmäßigen Willensbildung und ihrer unmittelbaren Vorbereitung, insbesondere
   a) von Handlungen des Bundespräsidenten, der Bundesregierung, der Bundesminister, der Staatssekretäre, der Landesregierung, einzelner Mitglieder derselben und des Landeshauptmannes, der Bezirksverwaltungsbehörden, der Organe der Gemeinde und der Organe der sonstigen Selbstverwaltungskörper,
   b) im Interesse eines behördlichen oder gerichtlichen Verfahrens, einer Prüfung oder eines sonstigen Tätigwerdens des Organs sowie zum Schutz der gesetzlichen Vertraulichkeit von Verhandlungen, Beratungen und Abstimmungen,
6. Abwehr eines erheblichen wirtschaftlichen oder finanziellen Schadens der Organe, Gebietskörperschaften oder sonstigen Selbstverwaltungskörper
7. überwiegende berechtigte Interessen eines anderen, insbesondere
   a) Wahrung des Rechts auf Schutz der personenbezogenen Daten,
   b) Wahrung von Berufs-, Geschäfts- oder Betriebsgeheimnissen,
   c) Wahrung des Bankgeheimnisses
   d) Wahrung des Redaktionsgeheimnisses
   e) Wahrung der Rechte am geistigen Eigentum

2. VERTRAULICH (V)

35 **Vertraulich** sind klassifizierte Informationen, deren unbefugte Weitergabe den in § 6 Abs. 1 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG) genannten Interessen zu-

wider laufen würde und die zusätzlich nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und deren Geheimhaltung im öffentlichen Interesse gelegen ist.

3. GEHEIM (Geh)

Geheim sind klassifizierte Informationen, die vertraulich sind und deren Preisgabe zudem die Gefahr einer erheblichen Schädigung der im § 6 Abs. 1 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG) genannten Interessen schaffen würde. **36**

4. STRENG GEHEIM (StrGeh)

Streng Geheim sind klassifizierte Informationen, die geheim sind und deren Bekanntwerden überdies eine schwere Schädigung der in § 6 Abs. 1 des Bundesgesetzes über den Zugang zu Informationen (Informationsfreiheitsgesetz – IFG) genannten Interessen wahrscheinlich machen würde. **37**

IV. Kennzeichnung

38 **Klassifizierte Informationen sind eindeutig und gut erkennbar durch Anbringen der Klassifizierungsstufe in Großbuchstaben und ausgeschrieben kenntlich zu machen (Klassifizierungsvermerk)** (s. Beilage VIII).

Sofern eine farbliche Kennzeichnung als zweckmäßig beurteilt und angeordnet wird, ist folgendes Farbschema einzuhalten:

GRÜN	EINGESCHRÄNKT
BLAU	VERTRAULICH
ROT	GEHEIM und STRENG GEHEIM

39 Bei **schriftlichen Informationen** ist **auf jeder Seite in der Kopf- und der Fußzeile** der Klassifizierungsvermerk anzubringen.

In der **Kopfzeile** ist überdies folgende **Seitennummerierung** anzubringen: Seite x von y (x = aktuelle Seitennummer, y = Gesamtzahl aller Seiten des Dokuments).

40 Bei den **Klassifizierungsstufen GEHEIM und STRENG GEHEIM** ist überdies in der **Kopfzeile jeder Seite**

– die Geschäftszahl,
– das Datum der Genehmigung und
– die Nummer der Ausfertigung

anzubringen.

Im Geschäftsstück ist die **Zuordnung der Ausfertigungen** anzugeben.

41 Schriftliche Informationen, die **automatisiert mit zugelassenen IKT-Systemen erstellt** wurden, können aus zwingenden technischen Gründen bis zu einer Anpassung im nationalen Bereich davon **abweichende Kennzeichnungen** aufweisen.

Auf der ersten Seite von Dokumenten der **Klassifizierungsstufe VERTRAULICH** oder höher sind alle Beilagen (Anhänge und Beilagen) konkret aufzulisten. **42**

Die **Beilagen** sind **wie das Dokument** selbst zu **kennzeichnen**, darüber hinaus sind sie **durchzunummerieren** und in der **Kopfzeile** jeder Seite ist der **Vermerk „Beilage xxx zu GZ ...“** anzubringen. **43**

Beilagen, die automatisiert mit zugelassenen IKT-Systemen erstellt wurden, können aus zwingenden technischen Gründen bis zu einer Anpassung im nationalen Bereich, davon **abweichende Kennzeichnungen** aufweisen. **44**

Auf **national klassifizierten Informationen** sind Klassifizierungsvermerke **ausschließlich** in **deutscher Sprache** anzubringen. **45**

Bei **klassifizierten Informationen** im **internationalen Bereich** ist die Kennzeichnung **zweizeilig** wie folgt vorzunehmen: **46**

- **die erste Zeile** enthält die **deutschen Begriffe** und setzt sich aus folgenden Elementen zusammen:
  - Länderbezeichnung: AUT,
  - Klassifizierungsgrad,
  - Formulierung „FREIGEGEBEN FÜR“,
  - Angabe des Empfängers (Organisation, Länderbezeichnung oder Koalition, zB EU, DEU, NATO);
- unmittelbar unter diese deutsche Kennzeichnung ist die entsprechende **englische Kennzeichnung** zu setzen (**zweite Zeile**):

AUT GEHEIM FREIGEGEBEN für GBR
AUT SECRET RELEASABLE TO GBR

(s. Beilage IX)

- wird **in AUT eine EU-klassifizierte Information** erstellt, ist die Kennzeichnung **einzeilig**, unter Verwendung der entsprechenden

französischen oder englischen Klassifizierungsvermerke zu setzen wie zB:

SECRET UE / **EU SECRET**

Im **Geschäftsverkehr mit der NATO/PfP** – in weiterem Gebrauch in dieser Vorschrift nur mehr als NATO bezeichnet – sind die Klassifizierungsvermerke in englischer Sprache, mit der EU jene in französischer oder englischer Sprache zu verwenden (s. RdNr. 48). **47**

Die **Zuordnung** internationaler bzw. bilateraler Klassifizierungsvermerke zu den jeweiligen nationalen Klassifizierungsvermerken ist der nachstehenden Tabelle zu entnehmen: **48**

BMLV (national)	**NATO**	**EU**
EINGESCHRÄNKT	NATO RESTRICTED	RESTREINT UE / EU RESTRICTED
VERTRAULICH	NATO CONFIDENTIAL	CONFIDENTIEL UE / EU CONFIDENTIAL
GEHEIM	NATO SECRET	SECRET UE / EU SECRET
STRENG GEHEIM	COSMIC TOP SECRET	TRÈS SECRET UE / EU TOP SECRET

Bei von **internationalen Organisationen erhaltenen klassifizierten Informationen,** ist die jeweilige **Kennzeichnung beizubehalten**. **49**

Sollten **klassifizierte NATO oder EU Beilagen** einem (nationalen) **Geschäftsstück beigefügt** werden, so ist für dieses Geschäftsstück zumindest die jeweils höchste NATO/EU Klassifizierungsstufe zu verwenden. **50**

Sollte dies aus Gründen des nationalen Geheimschutzes nicht zweckmäßig sein, sind die **Beilagen gesondert** zu verteilen.

C. ZUGANG ZU KLASSIFIZIERTEN INFORMATIONEN

I. Voraussetzungen für den Zugang

Der **Zugang zu klassifizierten Informationen** ist nur unter den nachstehenden **Voraussetzungen** zulässig: **51**

- Erfordernis für die Erfüllung der dienstlichen Aufgaben (**„need to know“** Prinzip),
- nachweisliche **Unterweisung** über den Umgang mit klassifizierten Informationen,
- ab der Klassifizierungsstufe VERTRAULICH eine der Klassifizierungsstufe entsprechende Prüfbescheinigung oder das Ergebnis einer gleichwertigen Überprüfung:

Klassifizierungsstufe	**Anforderungen**
EINGESCHRÄNKT	need to know Geheimschutzunterweisung
VERTRAULICH	need to know Geheimschutzunterweisung einfache Verlässlichkeitsprüfung
GEHEIM	need to know Geheimschutzunterweisung erweiterte Verlässlichkeitsprüfung
STRENG GEHEIM	need to know Geheimschutzunterweisung erweiterte Verlässlichkeitsprüfung durch AbwA

II. Unterweisung

52 Personen, denen Zugang zu klassifizierten Informationen gewährt werden soll, sind **vor dem ersten Zugang einer Unterweisung** (s. Beilage I) über den Umgang mit klassifizierten Informationen durch den Geheimschutzbeauftragten zu unterziehen.

53 Diese **Unterweisung** hat jedenfalls Informationen über nachstehende **Themen zu umfassen:**

- die Bestimmungen dieser Dienstvorschrift,
- notwendige technische/organisatorische/personelle Absicherungsmaßnahmen gem. den nationalen und völkerrechtlichen Dienstvorschriften,
- Verpflichtung zur **unverzüglichen Meldung** von **allen ungewöhnlichen Umständen mit Bezug zum Geheimschutz,**
- den Hinweis auf die Informationsblätter und das Informationsportal des Abwehramtes,
- weitere gesetzliche oder erlassmäßige Bestimmungen abhängig von der Aufgabenstellung und der Art der zur Verfügung gestellten klassifizierten Informationen (s. Beilage I).

54 Bedienstete der Militärvertretung BRÜSSEL, Mitglieder nationaler Delegationen in multilateralen Gremien und sonstige Bedienstete, die mit EU und/oder NATO-Informationen befasst sind, sind **darüber hinaus nachweislich** über die gültigen Sicherheitsvorschriften des Rates der EU und/oder der NATO zu informieren.

55 Die Unterweisung ist **regelmäßig, alle fünf Jahre,** zu wiederholen.

56 Der **Nachweis** der **durchgeführten Unterweisung** ist schriftlich festzuhalten (s. Beilage I). Der Nachweis ist vom Geheimschutzbeauftragten zu verwahren.

Die **Unterweisung** für die **Geheimschutzbeauftragten** (GehSchB) erfolgt jeweils durch die J2/S2/Sicherheitsbeauftragten. **57**

Die **Unterweisung** der **Geheimschutzbeauftragten** der **Zentralstelle** des BMLV sowie **unmittelbar Nachgeordneter** erfolgt durch das Abwehramt. **58**

III. Dokumentation des Zuganges

59 Der **tatsächliche Zugang** zu Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM, im Fall von NATO-klassifizierten Informationen bereits ab der Klassifizierungsstufe NATO-RESTRICTED, ist im jeweiligen **Register oder Geschäftsbuch bzw. Bestandsverzeichnis zu dokumentieren**.

60 Die **Dokumentation** hat

- den Namen der Person der Zugang gewährt wurde,
- den Zeitpunkt des Zuganges sowie
- die Bezeichnung der Information, zu welcher der Zugang gewährt wurde,

zu enthalten.

61 Sofern für die **Dokumentation des Zuganges ein IKT-System** gem. RdNr. 75 verwendet wird, ist sicherzustellen, dass alle Zugriffe auf diese Informationen im System unveränderbar dokumentiert werden.

Eine **schriftliche Dokumentation** des Zuganges im Register **entfällt** in diesem Fall.

D. GEHEIMSCHUTZPERSONAL

I. Allgemeines

Zum **Geheimschutzpersonal** zählen **62**

- der Informationssicherheitsbeauftragte (InfoSihB) und sein Stellvertreter,
- die Geheimschutzbeauftragten (GehSchB) und deren Stellvertreter sowie
- die J2/S2/Sicherheitsbeauftragten und deren Stellvertreter.

Das Geheimschutzpersonal muss über eine **gültige Prüfbescheinigung** verfügen (s. RdNr. 51). **63**

II. Verantwortlichkeit der Kommandanten und Leiter

64 Die **Kommandanten (Dienststellenleiter)** sind **verantwortlich**, dass in ihrem Zuständigkeitsbereich die Bestimmungen über den Umgang mit klassifizierten Informationen bekannt sind und eingehalten werden.

Sie haben dafür zu sorgen, dass der Zugang zu klassifizierten Informationen nur nach den Bestimmungen dieser Dienstvorschrift erfolgt.

65 Die Kommandanten (Dienststellenleiter) **legen fest,** welche **Funktionen ihrer Dienststelle** Zugang zu klassifizierten Informationen welcher Klassifizierungsstufe benötigen (s. RdNr. 51 ff).

III. Informationssicherheitsbeauftragter (InfoSihB)

Der **Informationssicherheitsbeauftragte** (§ 4 Abs. 1 InfoSiV) des BMLV ist der Leiter des Abwehramtes. **66**

Seine Aufgaben sind im § 4 Abs. 2 InfoSiV geregelt.

Sein Stellvertreter ist der stellvertretende Leiter des Abwehramtes.

Die **Organe des Abwehramtes** sind berechtigt, im Auftrag des InfoSihB in der Zentralstelle des BMLV und bei allen nachgeordneten Dienststellen die Maßnahmen des Geheimschutzes und der Informationssicherheit jederzeit zu überprüfen. **67**

IV. Geheimschutzbeauftragter (GehSchB)

68 Der Kommandant (Dienststellenleiter) bestimmt den **GehSchB und dessen Stellvertreter** für seinen Bereich. Wird für eine Dienststelle kein GehSchB bestimmt, so hat der Kommandant (Dienststellenleiter) diese Funktion selbst auszuüben.

69 Im Bereich der **Zentralstelle des BMLV** sind grundsätzlich bis Abteilungsebene (oder für gleichzuhaltende Organisationseinheiten) ein GehSchB und ein Stellvertreter zu bestimmen.

70 Fällt in einem Organisationsbereich nur eine **geringe Anzahl** von klassifizierten Informationen an, muss kein GehSchB bestimmt werden.

In diesem Fall sind die Aufgaben durch den Kommandanten (Dienststellenleiter) wahrzunehmen (s. RdNr. 68). Als Stellvertreter kann auch der GehSchB der übergeordneten Organisationsebene eingeteilt werden.

71 Wenn bei Dienststellen klassifizierte Informationen in **erheblichem Ausmaß** anfallen, können für einzelne Organisationselemente dieser Dienststellen oder für bestimmte Kategorien von klassifizierten Informationen eigene GehSchB bestellt werden.

72 Der **Stellvertreter** vertritt den GehSchB in dessen Abwesenheit, **ohne** dass **zwingend eine Übergabe** der klassifizierten Informationen zu erfolgen hat.

Der Name des Vertreters und der Zeitraum der Vertretung ist in den **Registern** auf geeignete Weise zu **vermerken**.

Der Geheimschutzbeauftragte hat in Bezug auf zu registrierende klassifizierte Informationen insbesondere folgende **Aufgaben** wahrzunehmen: **73**

- Entgegennehmen klassifizierter Informationen (elektronisch und in Papier),
- Prüfung der Umhüllung auf Unversehrtheit und der Sendung auf Vollzähligkeit,
- Führen der Register/Geschäftsbücher/Bestandsverzeichnisse für klassifizierte Informationen,
- Verteilen der klassifizierten Informationen mittels Zustellnachweis zur Bearbeitung,
- Abfertigen und Versenden von klassifizierten Informationen,
- Verwahren und Vernichten von klassifizierten Informationen,
- Durchführen der Unterweisung gemäß RdNr. 52,
- Kontrollieren des Bestandes klassifizierter Informationen.

Als **J2/S2/Sicherheitsbeauftragte** eingeteilte Funktionsträger dürfen nicht als GehSchB oder Stellvertreter eingeteilt werden, sie unterstützen jedoch die GehSchB bei der Unterweisung gem. RdNr. 52. **74**

E. BEHANDLUNG VON KLASSIFIZIERTEN INFORMATIONEN

I. Elektronische Verarbeitung

Klassifizierte Informationen dürfen nur mit für die jeweiligen Klassifizierungsstufen zugelassenen IKT-Systemen (Hardware und Software) unter Einhaltung der entsprechenden Vorgaben verarbeitet, bearbeitet, übermittelt und gespeichert werden. **75**

Klassifizierte Informationen sind bei Verfügbarkeit über entsprechend zugelassene elektronische Systeme zu **übermitteln**. **76**

Die Weitergabe bzw. Vernichtung von Ausfertigungen in **Papierform** ist gem. RdNr. 179 zu dokumentieren. **77**

In IKT-Systemen gem. RdNr. 75 ist sicherzustellen, dass auch alle **Lesezugriffe** auf verarbeitete klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH und höher bzw. der entsprechenden internationalen Klassifizierung **protokolliert** werden. **78**

Bei **NATO klassifizierten Informationen** ist diese Protokollierung bereits ab der Klassifizierungsstufe NATO RESTRICTED erforderlich. **79**

In diesen Systemen ist eine sinngemäße Abbildung der Bestimmungen der Kapitel II. bis VIII. sicherzustellen. **80**

II. Kanzleimäßige Behandlung

81 Bei klassifizierten Informationen der **Klassifizierungsstufe GEHEIM oder höher** ist anstelle eines Verteilers eine Empfängerliste zu verwenden, in welcher die Empfänger oder Funktionen konkret angeführt werden.

82 **Ausfertigungen** von klassifizierten Informationen der **Klassifizierungsstufe GEHEIM oder höher** sind durch eine fortlaufende Nummer (Ausfertigungsnummer) so zu kennzeichnen, dass jede Ausfertigung einem bestimmten Empfänger zugeordnet werden kann. Die Zuordnung der Ausfertigungsnummern zu den Empfängern muss aus der Empfängerliste ersichtlich sein.

83 Als **Ausfertigungen** gelten die an die Empfänger ergehenden Erledigungen und die vom Originalakt oder den Ausfertigungen angefertigten Kopien.

84 Für **multilateral klassifizierte Informationen** erfolgt die Verteilung durch die Zentralregister des BMLV.

85 Klassifizierte Informationen mit der Klassifizierungsstufe STRENG GEHEIM sind immer mit einem **Öffnungsvermerk** zu versehen.

86 Bei den **anderen klassifizierten Informationen** sind **Öffnungsvermerke** nur im Bedarfsfall auf Grund inhaltlicher Besonderheiten zu verwenden.

87 Der **Öffnungsvermerk** hat den **Wortlaut**

„Nur zu öffnen durch ...“

und die Funktion zu enthalten. Der Öffnungsberechtigte ist grundsätzlich durch seine Funktion (zB S2) zu bezeichnen. Nur in begründeten **Ausnahmefällen** darf im Öffnungsvermerk auch der Name des Öffnungsberechtigten angeführt werden.

Sofern ein System gem. RdNr. 75 bis 78 verwendet wird, ist anstelle des Öffnungsvermerks die Information funktionsbezogen so zu adressieren, dass nur die in Frage kommenden Personen Zugriff erhalten (keine Adressierung an Organisationseinheiten). **88**

III. Empfangsbestätigung

89 Der **Empfang** klassifizierter Informationen
- ab der Klassifizierungsstufe VERTRAULICH,
- bei NATO-Informationen ab der Stufe NATO RESTRICTED und höher bzw. der entsprechenden internationalen Klassifizierung,

ist vom Empfänger mittels einer der klassifizierten Information beigelegten Empfangsbestätigung (s. Beilage II) zu bestätigen.

90 Die Empfangsbestätigung ist an den Absender innerhalb von vierzehn Tagen zu retournieren und in geeigneter Weise dem (Original-)Geschäftsstück anzuschließen.

91 Bei **Übermittlung von klassifizierten Informationen** durch Systeme gem. RdNr. 75 bis 78 entfällt die Bestätigung des Empfanges, wenn durch das System die Zustellung dokumentiert wird und dem Absender diese Dokumentation zugänglich ist.

IV. Öffnen klassifizierter Informationen ab Klassifizierungsstufe VERTRAULICH

92 Der **innere Umschlag** (s. RdNr. 130), welcher die klassifizierten Informationen enthält, darf nur vom Kommandanten (Dienststellenleiter), GehSchB oder angeführten Empfänger geöffnet werden.

Der **Öffnungsberechtigte** hat die unverzügliche Registrierung der klassifizierten Information zu veranlassen.

93 Unterlagen im Zusammenhang mit **Verlässlichkeitsprüfungen** dürfen nur von Organen der nachrichtendienstlichen Abwehr geöffnet werden (§ 20 Abs. 3 MBG).

94 Der Öffnungsberechtigte hat die **Umhüllung** auf **Unversehrtheit** und die **Sendung auf Vollzähligkeit** zu prüfen.

Fehlende Stücke sind dem Absender unverzüglich anzuzeigen und bei der Übernahme in der Empfangsbestätigung zu vermerken.

Bei **Verdacht der unbefugten Öffnung** von klassifizierten Informationen sind durch den GehSchB unverzüglich die Maßnahmen gemäß RdNr. 191 bis 198 einzuleiten.

95 Bei **Übermittlung** von klassifizierten Informationen **durch IKT-Systeme** ist durch die Systemkonfiguration und durch die Aufstellung der Endgeräte sicher zu stellen, dass nur Berechtigte Zugang zu den übermittelten klassifizierten Informationen haben.

V. Verbuchung und Registrierung

96 Die **Klassifizierungsstufe** der **Geschäftsbücher** und **Bestandsverzeichnisse** für VERTRAULICH und GEHEIM ist EINGESCHRÄNKT.

Das Geschäftsbuch und die Bestandsverzeichnisse für STRENG GEHEIM sind als GEHEIM klassifiziert.

97 Als **EINGESCHRÄNKT** klassifizierte Informationen sind gemäß den Bestimmungen der Büroordnung (Kanzleiordnung)

- in zugelassenen Systemen gem. RdNr. 75 bis 78 oder
- in den allgemeinen Geschäftsbüchern zu verbuchen (s. Beilage IV)

Bei der **Verbuchung** ist der Klassifizierungsvermerk „EINGESCHRÄNKT“ ersichtlich zu machen.

98 Als **VERTRAULICH** klassifizierte Informationen sind in der Zentralstelle des BMLV und den diesen unmittelbar nachgeordneten Ämtern im allgemeinen Geschäftsbuch gemäß den Bestimmungen der Büroordnung (Kanzleiordnung) zu verbuchen.

Im Geschäftsbuch ist der Klassifizierungsvermerk „VERTRAULICH“ ersichtlich zu machen und der Vermerk über die Vernichtung anzubringen.

Multilateral klassifizierte Informationen werden durch die Zentralregister BMLV verwaltet und vernichtet.

99 Bei sonstigen nachgeordneten Dienststellen sind für klassifizierte Informationen mit der Klassifizierungsstufe VERTRAULICH eigene getrennte Geschäftsbücher zu führen, in welchen diese mit eigener Geschäftszahl zu verbuchen sind.

100 Als **GEHEIM oder STRENG GEHEIM** klassifizierte Informationen sind getrennt in eigenen Geschäftsbüchern gemäß Beilage IV oder mit zugelassenen IT-Systemen gem. RdNr. 75 bis 78 mit eigenen Geschäftszahlen zu verbuchen.

Klassifizierte Informationen der Klassifizierungsstufe VERTRAULICH oder höher, die im **Einsichtsverkehr** vorgeschrieben werden, sind ebenso in **fortlaufender Reihenfolge des Einlangens** – **getrennt nach ihrer Klassifizierungsstufe ohne Vergabe einer eigenen Geschäftszahl** – in den Registern bzw. Geschäftsbüchern zu registrieren (s. Beilage IV). Nach **Weitergabe** des Geschäftsstückes ist die Eintragung zu **streichen**. **101**

Diese Registrierung entfällt bei Übermittlung in einem zugelassenen System gem. RdNr. 75 bis 78.

Die **Geschäftszahl** (Beispiel: 515-Geh/GDPräs/2025) für jene klassifizierten Informationen, die in eigenen Registern zu verbuchen sind, besteht aus: **102**

- der fortlaufenden Zahl innerhalb des laufenden Kalenderjahres (zu Jahresbeginn jeweils mit 1 beginnend),
- dem durch einen Bindestrich getrennten Klassifizierungsvermerk in abgekürzter Form (Geh bzw. StrGeh),
- der durch einen Schrägstrich getrennten Kurzbezeichnung der Organisationseinrichtung gemäß Geschäftseinteilung der Zentralstelle bzw. gemäß aktuellem Abkürzungsverzeichnis,
- der durch einen Schrägstrich getrennten Jahreszahl (vierstellig).

In **Systemen gem. RdNr. 75 bis 78** dürfen Informationen verschiedener Klassifizierungsstufen gemeinsam behandelt werden, sofern das System den Anforderungen der höchsten zu verarbeitenden Klassifizierungsstufe entspricht. **103**

Dienststellen, die **keine Geschäftsbücher** führen, aber klassifizierte Informationen ständig oder vorübergehend verwahren, haben nach Klassifizierungsstufen und Herkunft (national/EU/NATO) **getrennte** Register (**Bestandsverzeichnisse**) zu führen (s. Beilage III). **104**

Sollte darüber hinaus aus Gründen der Übersichtlichkeit ein Nachweis über klassifizierte Geschäftsstücke notwendig werden, ist das Führen zusätzlicher Register anzuordnen.

105 Sofern ein System gem. RdNr. 75 bis 78 verwendet wird, ist der **Vorgang des Einbringens** der klassifizierten Information in das System einer **Registrierung gleichzuhalten**.

In diesem Fall sind auch klassifizierte Informationen in Papierform oder anderen Medien bis zur jeweils höchsten zugelassenen Stufe **in diesem System zu verbuchen**.

106 Bei den Registern, **Geschäftsbüchern und Bestandsverzeichnissen** sind die **Buchseiten** zu **nummerieren**. Die **Seitenanzahl** ist am inneren, vorderen Umschlag zu vermerken und vom GehSchB zu bestätigen.

107 Die Register, **Geschäftsbücher und Bestandsverzeichnisse** sind am **Jahresende** abzuschließen und dem Kommandanten (Dienststellenleiter) vorzulegen. Von diesem ist nach Überprüfung die **ordnungsgemäße Führung durch Abzeichnung zu bestätigen**.

VI. Registrierung multilateral klassifizierter Informationen

Alle multilateral klassifizierten Informationen (NATO, EU), die dem BMLV zugehen, sind an die in der **Zentralstelle des BMLV eingerichteten Zentralregister weiterzuleiten**. **108**

Die **Registrierung** von multilateralen Informationen **109**
- mit den Klassifizierungsstufen CONFIDENTIAL, CONFIDENTIEL,
- bei NATO ab der Stufe RESTRICTED
- und höher

erfolgt **ausschließlich bei den Zentralregistern BMLV** in eigenen **Registern**.

Andere Dienststellen, die international klassifizierte Informationen **110**
- mit den Klassifizierungsstufen CONFIDENTIAL, CONFIDENTIEL,
- bei NATO/PfP ab der Stufe (NATO) RESTRICTED
- und höher

ständig oder vorübergehend verwahren, haben **Bestandsverzeichnisse** zu führen.

Geschäftsbücher und Register sind getrennt nach multilateraler Organisation und Klassifizierungsstufe zu führen. **111**

Multilateral klassifizierte Informationen bleiben stets im **Eigentum** der jeweiligen **multilateralen Organisation**. **112**

Daher dürfen die Originaldokumente nicht als Beilagen zum Akt in den Kanzleien und Archiven hinterlegt werden, sondern sind bei den dafür vorgesehenen Registern des BMLV zu verwahren.

VII. Überführung von Papier in elektronische Form (Scannen)

113 Für das **Überführen** von klassifizierten Informationen, die in Papierform vorliegen, in elektronische Form (zB durch Einscannen) dürfen **nur Systeme** verwendet werden, die **gem. RdNr. 75 bis 78** dafür zugelassen wurden.

114 In Papierform vorliegende klassifizierte Informationen

- der **Klassifizierungsstufe STRENG GEHEIM und GEHEIM** dürfen nur vom **Verfasser**,
- der **Klassifizierungsstufe VERTRAULICH** nur mit **Genehmigung des Kommandanten (Dienststellenleiters)**

gescannt werden.

115 Bei der Überführung **multilateral klassifizierter Informationen** in elektronische Systeme übernehmen die **jeweiligen Zentralregister BMLV** die **Aufgaben** des **Verfassers**.

VIII. Überführung elektronischer Informationen in Papierform

Die **Überführung** von klassifizierten Informationen, die in elektronischer Form vorliegen, in Papierform (zB durch Ausdrucken) hat unter Verwendung der **gem. RdNr. 75 bis 78 angeführten Systeme** und Verfahren zu erfolgen. **116**

Die **verwendeten Systeme** haben die der jeweiligen Klassifizierungsstufe **entsprechende Dokumentation sicherzustellen**.

Mit den **Ausdrucken** ist nach den Bestimmungen dieser Dienstvorschrift für klassifizierte Informationen in Papierform vorzugehen. **117**

IX. Kopieren

118 Unter **„Kopieren“** ist in dieser Dienstvorschrift die Übertragung von klassifizierten Informationen von einem Medium oder System auf ein anderes zu verstehen, wobei die Originalinformation erhalten bleibt, wie zB:

- **Kopie** im herkömmlichen Sinn – von Papier auf Papier,
- **Kopie in elektronischer/digitaler Form** – von Datenträger auf Datenträger,
- **Scannen** – von Papier zu IKT-System,
- **Ausdrucken** – von IKT-System zu Papier.

119 **Nicht** unter **„Kopieren“** fällt das Weitergeben oder Weiterleiten von Informationen (zB Die Belastung oder die Erteilung einer Leseberechtigung in einem ELAK-System).

120 **Kopien** von in **Papierform** vorliegenden klassifizierten Informationen der **Stufe EINGESCHRÄNKT** dürfen von dem **zum Empfang** und **zur Bearbeitung berechtigten Personenkreis** in dem für die Bearbeitung unmittelbar erforderlichen Ausmaß angefertigt werden.

Bei der **Weitergabe** sind die Kriterien für den Zugang zu klassifizierten Informationen (s. RdNr. 51) zu berücksichtigen.

Diese Kopien sind **unmittelbar nach Zweckerfüllung zu vernichten**.

121 In Papierform vorliegende klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH** dürfen nur mit Genehmigung des **Kommandanten (Dienststellenleiters)** kopiert werden.

Die erteilte **Genehmigung** und die **Anzahl** der Kopien sind auf dem Original, das kopiert wird, durch den Genehmigenden mit Datum und Unterschrift zu vermerken.

Die **Anzahl** der hergestellten Kopien sowie die **Empfänger** sind gemäß den Bestimmungen der RdNr. 97 ff zu verbuchen.

In Papierform vorliegende klassifizierte Informationen der Stufen **GEHEIM** und **STRENG GEHEIM** dürfen **durch die Empfänger nicht kopiert** werden. Es ist beim **Ersteller** eine zusätzliche Ausfertigung anzufordern. **122**

Das Kopieren von **multilateralen klassifizierten Informationen** der Klassifizierungsstufe CONFIDENTIEL UE, bei NATO RESTRICTED und höher, ist nur mit schriftlicher Genehmigung der Zentralregister des BMLV (s. RdNr. 108) zulässig, diese Kopien sind zu verbuchen und nach Zweckerfüllung dem Vernichtungsprozedere zuzuführen. **123**

Die **Herstellung von Auszügen** aus Geschäftsstücken der Klassifizierungsstufen **GEHEIM und STRENG GEHEIM**, sofern diese zur Erstellung eigener Geschäftsstücke dienen, ist mit **Genehmigung des Kommandanten (Dienststellenleiters)** zulässig. **124**

Dabei ist eine Neubeurteilung der Klassifizierungsstufe vorzunehmen.

Elektronisch vorliegende klassifizierte Informationen dürfen nur auf zugelassenen Systemen RdNr. 75 bis 78 und unter sinngemäßer Anwendung der Bestimmungen in den RdNr. 118 ff kopiert werden. **125**

Die **Protokollierung/Dokumentation** ist gemäß den für das jeweilige System verfügten Regelungen durchzuführen.

F. ÜBERMITTLUNG KLASSIFIZIERTER INFORMATIONEN

I. Allgemeines

Sofern **zugelassene elektronische Systeme** zur Verfügung stehen, sind diese zur Übermittlung zu verwenden. **126**

Die **Abfertigung** von klassifizierten Informationen der **Klassifizierungsstufe EINGESCHRÄNKT** ist – sofern sie nicht elektronisch erfolgt – vom zuständigen Kanzleileiter oder einem hiezu Beauftragten zu veranlassen. **127**

Die **Abfertigung** von klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM** ist – sofern diese nicht auf elektronischem Wege erfolgt – vom zuständigen GehSchB zu veranlassen. **128**

Dokumente der **Klassifizierungsstufe EINGESCHRÄNKT** sind im verschlossenen Kuvert zu übermitteln. **129**

Dokumente der **Klassifizierungsstufe VERTRAULICH** oder höher sind in einem doppelten undurchsichtigen verschlossenen Kuvert zu übermitteln, wobei nur am inneren Kuvert die Klassifizierungsstufe anzugeben und eine Empfangsbestätigung beizulegen ist (s. Beilage II). **130**

Am **äußeren Kuvert** sind lediglich der Empfänger und der Absender anzugeben. **131**

Das innere Kuvert ist mit einem geeigneten Sicherheitsklebeband so zu verschließen, dass eine Öffnung oder Öffnungsversuche während des Transportes zum Empfänger erkennbar sind. **132**

II. Verbringung, Versand, Übermittlung und Mitnahme

133 Die **Verbringung** von klassifizierten Informationen der **Klassifizierungsstufe EINGESCHRÄNKT** darf sowohl **innerhalb des Bundesgebietes** als auch **in das Ausland** auf dem **Postweg oder persönlich** erfolgen.

134 Klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH und GEHEIM** dürfen **innerhalb des Bundesgebietes** durch **Post oder Zustelldienst** versendet werden.

Dabei ist ein **Rückschein (RSa)** oder eine gleichwertige nachweisliche Zustellart zu verwenden die eine Zustellung an Ersatzempfänger ausschließt.

Eine Verbringung in das **Ausland** hat durch **Kurier** zu erfolgen, wobei **multilateral klassifizierte Informationen** nur in und über die jeweiligen Mitgliedsländer verbracht werden dürfen.

135 In **Ausnahmefällen** kann der **persönliche Transport** (das Mitführen) klassifizierter Informationen **bis zur Klassifizierungsstufe GEHEIM in das Ausland** genehmigt werden.

Die **Genehmigung** für national klassifizierte Informationen erteilt der Kommandant/Dienststellenleiter, für multilateral klassifizierte Informationen der InfoSihB/BMLV (Ltr AbwA).

136 Klassifizierte Informationen der **Klassifizierungsstufe STRENG GEHEIM** sind **grundsätzlich** durch die **Militärpolizei,** sonst durch **zwei Kuriere** zu transportieren.

137 Die elektronische Übermittlung von klassifizierten Informationen hat auf **sicheren Übertragungswegen** auf dafür **zugelassenen Systemen** nach den vorgegebenen Methoden und Verfahren zu erfolgen.

Eine **offene fernmündliche Weitergabe** von klassifizierten Informationen ist nur in Ausnahmefällen bei Gefahr in Verzug zulässig und nach Identifikation des Empfängers so zu halten, dass der Sachverhalt gegenüber Dritten verschleiert wird. **138**

Für die **Mitnahme** von **multilateral klassifizierten Informationen** in das Ausland, einschließlich der Durchreisestaaten, ist **vor Reiseantritt die Zustimmung der Zentralregister BMLV** einzuholen. Die Verbringung in das Ausland ist im jeweiligen Register zu vermerken. Dabei sind die Bestimmungen der RdNr. 150 einzuhalten. **139**

Bedienstete, die **multilateral klassifizierte Informationen** auf Auslandsdienstreisen mitführen, sollen über einen **gültigen Dienst- oder Diplomatenpass** verfügen, jedenfalls ist eine **Kurierbescheinigung** (s. Beilage V) mitzuführen. **140**

Klassifizierte Informationen dürfen **nicht an öffentlichen Orten gelesen** und **keinesfalls unbeaufsichtigt gelagert** werden. Sie sind in entsprechenden **Behältnissen österreichischer Vertretungen** zu verwahren. Ist dies nicht möglich, so sind sie **ständig persönlich mitzuführen** und während der **Ruhezeit in versperrbaren Behältnissen** (zB Hotelzimmersafe) zu lagern. **141**

Nach **Beendigung** der **Dienstreise** ist den Zentralregistern BMLV fernmündlich die ordnungsgemäße Wiederverwahrung zu melden. **142**

Die **Mitnahme** von **IKT-Geräten** und **Systemen** gem. RdNr. 75 bis 78 in das Ausland ist im ADR-Auftrag bzw. in der Entsendeweisung anzuordnen. **143**

Der Transport und die Lagerung von klassifiziertem Gerät ist in den **fachdienstlichen Vorschriften** zu regeln. **144**

III. Kuriere

145 Als **Kuriere** sind militärische Organe (§ 1 Abs. 1 MBG) einzuteilen.

Diesen ist vom zuständigen Vorgesetzten ein **schriftlicher Wachauftrag** zu erteilen.

In **Ausnahmefällen** können auch **Zivilbedienstete** der Zentralstelle als Kurier eingeteilt werden, denen jedoch **keine Befugnisse nach MBG** zustehen.

146 Als **Kuriere** für klassifizierte Informationen sind nur Personen einzuteilen, die über eine **gültige Prüfbescheinigung** verfügen.

147 Den Kurieren ist von der Dienststelle eine **Kurierbescheinigung** (s. Beilage V) auszustellen, die sie in Verbindung mit ihrem Dienstausweis zur Übernahme sowie Übergabe von klassifizierten Informationen berechtigt.

148 Zur Durchführung des Kurierauftrages kann auch das Tragen von **Zivilkleidung** angeordnet werden.

149 Kuriere sind, sofern sie klassifizierte Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** befördern, **zu bewaffnen.** Die Art der Bewaffnung ist der Bedrohung anzupassen. Kuriere, die klassifizierte Informationen **in das Ausland** befördern, sind **nicht zu bewaffnen**, es sei denn, das Mitführen von Waffen ist durch internationale Abkommen oder im Rahmen von Auslandeinsätzen ausdrücklich gestattet.

150 Für **Personen**, die gem. RdNr. 135 klassifizierte Informationen der Klassifizierungsstufen **GEHEIM oder STRENG GEHEIM** aus anderen Gründen **außerhalb militärischer Liegenschaften mit sich führen**, gelten die gleichen **Bestimmungen wie für Kuriere.**

IV. Weitergabe innerhalb der Dienststelle

151 **Innerhalb der Dienststelle** erfolgt die auch nur vorübergehende Weitergabe der klassifizierten Informationen der **Klassifizierungsstufe VERTRAULICH und höher** mit **Zustellbuch** (s. Beilage VI) oder mittels Empfangsschein (s. Beilage II).

152 **Zustellbücher** sind mit der Bezeichnung der Dienststelle zu kennzeichnen. Zustellbücher enthalten keinen Hinweis auf den Inhalt der klassifizierten Information und unterliegen daher keiner Klassifizierung.

153 Bei **Übermittlung und Bearbeitung** von klassifizierten Informationen **auf zugelassenen IKT-Systemen** entfällt die Bestätigung des Empfanges, wenn durch das System die Zustellung dokumentiert wird.

V. Mündliche Weitergabe

154 Haben **Besprechungen** klassifizierte Informationen der **Klassifizierungsstufe VERTRAULICH oder höher zum Inhalt,** so ist dies in der Einberufung zur Besprechung unter Angabe der höchsten Klassifizierungsstufe bekannt zu geben.

Es dürfen nur **Personen** an o.a. Besprechungen **teilnehmen**, welche die Ermächtigung zum Zugang zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe besitzen (s. RdNr. 51).

155 Genehmigte Aufzeichnungen sind entsprechend zu klassifizieren. Die Mitnahme von nicht genehmigten **Kommunikationsmitteln** oder **Aufzeichnungsgeräten** ist verboten (zB Mobiltelefone).

156 Bei der **mündlichen Darlegung** von Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** sind, wenn vom AbwA zugelassene **abhörgeschützte oder abhörsichere Räume** nicht zur Verfügung stehen, entsprechende Maßnahmen (u.a. Ortswahl, Abgabe von Mobiltelefonen und ähnlichen Geräten, Bewachung/Sicherung des Raumes) für die **Abhörsicherheit** zu treffen.

G. VERWAHRUNG, VERNICHTUNG UND KONTROLLE

I. Verwahrung

Klassifizierte Informationen sind der jeweiligen Klassifizierungsstufe entsprechend **in den Diensträumen gesichert** zu **verwahren** und dürfen nur bei unabdingbaren dienstlichen Notwendigkeiten aus diesen verbracht werden. **157**

Klassifizierte Informationen der **Klassifizierungsstufe EINGESCHRÄNKT** sind in **Büromöbel versperrt** zu verwahren. **158**

Klassifizierte Informationen der **Klassifizierungsstufen VERTRAULICH oder höher** müssen in für die sichere Verwahrung von klassifizierten Informationen der entsprechenden Klassifizierungsstufe **zugelassenen Behältnissen** verwahrt werden. **159**

Eine Verwahrung in einem gemeinsamen Behältnis, welches für die jeweils höchste in Betracht kommende Klassifizierungsstufe zugelassen wurde, ist möglich (s. RdNr. 167). **160**

Den **Erstschlüssel** hat jene Person, die für die Benützung des Behältnisses verantwortlich ist, so zu verwahren, dass ein Zugriff durch Unbefugte ausgeschlossen ist. **161**

Zweit- bzw. Reserveschlüssel (ggf. Codes für elektronische Schlösser) verwahren **162**

- in der Zentralstelle die Sicherheitsbeauftragten,
- sonst
  - der Kommandant,
  - Chef des Stabes oder
  - Dienststellenleiter

in einem verklebten Umschlag mit der Unterschrift des Erstschlüsselverwahrers in ihrem Behältnis für klassifizierte Informationen.

163 Im Umschlag ist eine **Schlüsselausgabeliste** zu verwahren.

164 Das **Öffnen** des Behälters mit dem Zweitschlüssel hat **im Beisein einer zweiten Person**, die in der Schlüsselausgabeliste einzutragen ist, zu erfolgen.

165 Bei **Verlust eines Schlüssels** ist dies dem Vorgesetzten unverzüglich zu melden und sind bis zur Änderung/Erneuerung des Schlosses geeignete Maßnahmen zur Verhinderung unbefugter Zugriffe zu setzen.

166 Allenfalls in **Papierform** oder auf **Datenträgern** vorliegende national und/oder multilateral klassifizierte Informationen sind **getrennt für die jeweilige Organisation** und **getrennt nach Klassifizierungsstufen** zu **verwahren**.

BEACHTE:	National klassifizierte Informationen sind getrennt von multilateral klassifizierten Informationen zu verwahren.

167 Allenfalls in **Papierform** oder auf **Datenträgern** vorliegende **national und/oder multilateral klassifizierte Informationen** können in einem **gemeinsamen Behältnis verwahrt** werden. In diesem Fall müssen die **Behältnisse** den Anforderungen für die **höchste Klassifizierungsstufe** der gemeinsam verwahrten klassifizierten Informationen **entsprechen**. Dabei ist jedoch eine **organisatorische Trennung** (zB in getrennten Ordnern) nach Klassifizierungsstufen und Organisationen einzuhalten.

168 Im **Einsatz** und **bei Übungen** können klassifizierte Informationen entsprechend den Bedingungen im Einsatz- oder Übungsraum in einfachen versperrbaren Behältnissen verwahrt werden, sofern eine **durchgehende Bewachung** sichergestellt ist.

II. Vernichtung

Die **verfassende Stelle** hat auf den **Ausfertigungen** zu vermerken, **169**
ob die klassifizierte Information zu einem bestimmten Zeitpunkt, nach Zweckerfüllung oder auf Weisung zu vernichten ist.

Ist **kein Vermerk** angebracht, hat der **Kommandant (Dienststellenleiter)** der aufbewahrenden Stelle festzulegen, wann die klassifizierte Information zu vernichten ist.

MERKE:	Wurde **keinerlei Festlegung** getroffen, so ist die klassifizierte Information **nach 10 Jahren** zu vernichten.

Das **beim Verfasser abgelegte Original** der klassifizierten Informa- **170**
tion ist nach den Bestimmungen der Büroordnung für die Bundesministerien zu skartieren.

Eine Anbietung oder Abgabe von klassifiziertem Schriftgut ab der Klassifizierungsstufe **VERTRAULICH** an das Österreichische Staatsarchiv kommt erst nach erfolgter **Deklassifizierung** in Betracht.

Alle **Organisationseinheiten**, die klassifizierte Informationen **erstellen und Originale in Verwahrung halten**, haben regelmäßig, innerhalb eines Zeitraumes von längstens 10 Jahren, die **Angemessenheit der verfügten Klassifizierungsstufen** zu beurteilen und gegebenenfalls eine Herabsetzung der Klassifizierungsstufe oder eine Deklassifizierung zu veranlassen.

Diese Überprüfung kann auch im Zuge der periodischen Überprüfungen der Bestände klassifizierter Informationen im Einvernehmen mit dem Abwehramt durchgeführt werden.

Register, Geschäftsbücher, Bestandsverzeichnisse und Zustellbücher **171**
sind **unbegrenzt** aufzubewahren.

172 **Originale** von klassifizierten Informationen der Klassifizierungsstufen **VERTRAULICH**, **GEHEIM und STRENG GEHEIM** sowie **nicht mehr benötigte Register, Geschäftsbücher, Bestandsverzeichnisse und Zustellbücher** für klassifizierte Informationen dieser Klassifizierungsstufen der Zentralstelle des BMLV und der dem BMLV unmittelbar nachgeordneten Kommanden und Dienststellen, die gemäß RdNr. 170 zu skartieren wären, sind nicht zu vernichten sondern dem bei der **Abteilung Präsidiale eingerichteten Zwischenarchiv** für klassifizierte Informationen zuzuführen.

173 Dies gilt nicht für klassifizierte Informationen die beim **AbwA oder HNaA** anfallen.

174 Die **Vernichtung** von klassifizierten Informationen gem. RdNr. 22 hat mit einem für die jeweilige Klassifizierungsstufe freigegeben Verfahren so zu erfolgen, dass keine auswertbaren Reste der klassifizierten Information übrig bleiben.

Das **Löschen** von klassifizierten Informationen in **elektronischer/digitaler Form** hat mit den dafür **freigegeben Verfahren** zu erfolgen.

175 Die **Vernichtung** von klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH und GEHEIM** hat durch den **GehSchB** unter **Anwesenheit eines Zeugen** zu erfolgen.

176 Die **Vernichtung** von klassifizierten Informationen der **Klassifizierungsstufe STRENG GEHEIM** hat durch den **GehSchB** unter **Anwesenheit** von **zwei Zeugen** zu erfolgen.

Die **Zeugen** müssen über die Zugangsberechtigung zu klassifizierten Informationen der entsprechenden Klassifizierungsstufe verfügen.

177 **Multilateral klassifizierte Informationen,** welche den nationalen **Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG**

GEHEIM entsprechen, werden ausschließlich durch **die Zentralregister BMLV** vernichtet.

Klassifizierte Informationen der **Klassifizierungsstufe NATO RESTRICTED** sind durch den **GehSchB der verwahrenden Stelle** zu vernichten. **178**

Eine **Kopie** des Vernichtungsprotokolls ist dem **Zentralregister BMLV** zu übermitteln.

Bei der **Vernichtung** von klassifizierten Informationen **ab** der Klassifizierungsstufe VERTRAULICH ist ein **Vernichtungsprotokoll** (s. Beilage VII) anzulegen, welches **10 Jahre aufzubewahren** ist. **179**

Bei **Verwendung eines IKT-Systems** gem. RdNr. 75 bis 78 entfällt die Verpflichtung zur Führung eines Vernichtungsprotokolls dann, wenn für die Vernichtung freigegebene Verfahren verwendet werden, die eine ausreichende Dokumentation sicherstellen. **180**

Eintragungen über klassifizierte Informationen, die vernichtet wurden, sind in den (sofern in Papierform geführten) **Registern, Geschäftsbüchern und Bestandsverzeichnissen in roter Farbe zu streichen**; die Vernichtung ist mit Bezug auf das Vernichtungsprotokoll anzumerken. **181**

Besteht die **unmittelbar drohende Gefahr**, dass klassifizierte Informationen **durch Unbefugte in Besitz genommen werden** oder eine **Preisgabe** erfolgen könnte, ist der unverzügliche Abtransport oder, falls dies nicht möglich ist, die unverzügliche Vernichtung sicherzustellen. **182**

Grundsätzlich darf die Vernichtung von klassifizierten Informationen in diesem Fall **nur auf Weisung des Vorgesetzten** erfolgen. Kann die Weisung hiezu nicht rechtzeitig eingeholt werden, ist die Vernichtung selbständig durchzuführen. **183**

Die Vernichtung ist **schriftlich** zu **dokumentieren**. Entsprechende Vorkehrungen zur **raschen Vernichtung** sind vorzusehen.

184 **Kommandotagebücher und Einsatzjournale sind nicht zu vernichten.**

III. Kontrolle

Das **System** des Geheimschutzes ist durch den J2/S2/Sicherheitsbeauftragten in seinem Wirkungsbereich mindestens **1x jährlich** nachweislich zu **überprüfen**. **185**

Dabei sind insbesondere **186**
– die Vollständigkeit der Aufzeichnungen,
– die Sicherheit der Behältnisse und
– das Schlüsselsystem (Schlüsselordnung)
zu überprüfen.

Sind klassifizierte Informationen der **Klassifizierungsstufen GEHEIM oder STRENG GEHEIM** vorhanden, so ist eine **vollständige Überprüfung** der Vorgänge vorzunehmen. **187**

Bei klassifizierten Informationen der **Klassifizierungsstufen VERTRAULICH** ist eine **stichprobenartige Überprüfung** vorzunehmen. **188**

Das **Überprüfungsergebnis**, ab Ebene großer Verband aufwärts, ausgenommen HNaA, ist auf dem Dienstweg dem AbwA vorzulegen. **189**
Die durchgeführte Überprüfung ist in **den Registern zu vermerken**.

Davon unberührt bleiben zusätzliche Überprüfungen durch vorgesetzte Dienststellen. **190**

IV. Verlust oder Preisgabe

191 Der **Verlust** oder die **Preisgabe** von klassifizierten Informationen **bzw. ein entsprechender Verdacht** sind unverzüglich dem Kommandanten (Dienststellenleiter) sowie mittels BV-Meldung zu melden.

192 Der **Kommandant/Dienststellenleiter** hat alle erforderlichen Maßnahmen zur Wiederauffindung, Untersuchung des Vorfalles und Verhinderung von (weiteren) Schäden zu treffen.

193 Das **Untersuchungsergebnis** und die getroffenen Maßnahmen sind schriftlich zu dokumentieren und auf dem Dienstweg dem AbwA zu melden.

194 Beim **Verdacht einer gerichtlich strafbaren Handlung** ist überdies vom Disziplinarvorgesetzten Anzeige bei der zuständigen Staatsanwaltschaft zu erstatten.

195 Der Verlust oder die Preisgabe ist auch der Stelle zu melden, welche die klassifizierte Information ausgegeben hat (**Verfasser**). Diese hat zur Verhütung von (weiteren) Schäden alle nach dem Inhalt der klassifizierten Information zur **Schadensbegrenzung** erforderlichen Maßnahmen zu treffen.

196 Werden in Verlust geratene klassifizierte Informationen **innerhalb von 4 Wochen** nicht wiederaufgefunden, so ist unter Vorlage eines Berichtes über den Stand der Ermittlungen die Entscheidung über Fortführung oder Einstellung der Untersuchung bei der vorgesetzten Dienststelle einzuholen. Die getroffene Entscheidung ist dem AbwA zu melden.

Das **Auffinden** einer in Verlust geratenen klassifizierten Information ist ebenfalls dem Kommandanten/Dienststellenleiter zu melden. Dieser hat die Zustandebringung dem AbwA und dem Verfasser zu melden. **197**

Dabei ist anzugeben, **wann und wo** die klassifizierte Information gefunden wurde und ob **Unbefugte** dazu **Zugang** hatten.

Der Verlust, die Preisgabe und das Wiederauffinden von internationalen, aufgrund völkerrechtlicher Vereinbarungen klassifizierten Informationen ist unverzüglich dem Informationssicherheitsbeauftragten zu melden. **Die Untersuchung obliegt dem AbwA**. **198**

H. SONSTIGE BESTIMMUNGEN FÜR KLASSIFIZIERTE INFORMATIONEN

I. Weitergabe an ressortfremde Stellen

Vor der Übermittlung von klassifizierten Informationen ist durch Prüfung im Einzelfall sicherzustellen, dass beim Empfänger die Voraussetzungen für einen adäquaten Schutz gegeben sind. **199**

Klassifizierte Informationen sind von der **Informationspflicht** nach dem Informationsweiterverwendungsgesetz sowie nach dem Informationsfreiheitsgesetz (IFG) sowohl von der proaktiven Informationspflicht als auch von der Information auf Antrag **ausgenommen.** **200**

Auf § 6 Abs. 2 IFG wird hingewiesen.

II. Übergangsbestimmungen

201 entfällt

202 Für klassifizierte Informationen (VERSCHLUSS, DATENSCHUTZ, RESTREINT-UE und NATO-RESTRICTED), die vor Inkrafttreten dieser Dienstvorschrift angefallen sind und nicht mehr weiter bearbeitet werden, ergeben sich keine Änderungen.

203 Im Bedarfsfall bzw. bei einer Weiterbearbeitung hat durch den Ersteller eine **Neubeurteilung** der **Klassifizierungsstufe** nach den Bestimmungen dieser Dienstvorschrift (s. RdNr. 34ff) zu erfolgen.

204 Grundsätzlich sind bestehende klassifizierte Informationen wie folgt zu **behandeln:**

- „VERSCHLUSS“ wie „EINGESCHRÄNKT“.
- „GEHEIM“ und „STRENG GEHEIM“ unverändert.

205 Informationen der Klassifizierungsstufe VERTRAULICH und höher, ausgenommen multilateral klassifizierte Informationen, können weiterhin in den **bisher verwendeten Behältnissen** gelagert werden.

Bei **Neubeschaffungen** ist nach den Bestimmungen dieser Dienstvorschrift vorzugehen.

206 entfällt

III. Strafbestimmungen

Verstöße gegen die Bestimmungen dieser Dienstvorschrift sind ungeachtet einer allfälligen (verwaltungs-)strafrechtlichen Verfolgung dienstrechtlich zu ahnden. **207**

BEILAGE I

Nachweis der Geheimschutzverpflichtung

A: Identität der verpflichteten Person und Angaben zu deren Arbeitgeber[1]

Name, Vorname, akad. Grad, Dienstgrad, Nationalität	Geburtsdatum: Geburtsort:
Wohnadresse	Ausweis/Reisepass Nr.[2]: Ausstellungsbehörde: Ausstellungsdatum:
Bezeichnung der Dienststelle/Firma inkl. Adresse	

B: Grund der besonderen Verpflichtung zur Geheimhaltung sowie Bezeichnung der Klassifizierungsstufe

	Zugang zu klassifizierter nationaler Information	[3]
	Zugang zu völkerrechtlich klassifizierter Information	[4]
	Zutritt zu Objektschutzkategorie II oder höher	[5]

VERPFLICHTUNG
zum Schutz klassifizierter Information

Die verpflichtete Person wurde über folgende Punkte **unterwiesen**:

1. Art der klassifizierten Information.
2. Notwendige technische/organisatorische/personelle **Absicherungsmaßnahmen** gem. den nationalen und **völkerrechtlichen** Sicherheitsvorschriften.
3. **Verpflichtung** zur unverzüglichen Meldung von:
   - Annäherungsversuchen/Handlungsweisen, die auf Spionage hindeuten.
   - Allen ungewöhnlichen Umständen mit Bezug zum Geheimschutz.
4. **Strafrechtliche bzw. disziplinäre Folgen** von Verstößen gegen die Geheimhaltungspflicht.

---

[1] Falls zutreffend.

[2] Amtlicher Lichtbildausweis:
a. Bei der Ausstellung von Sicherheitsermächtigungen ist zwingend ein Reisepass vorzulegen.
b. In jedem Fall sind die Ausweisnummer, die Ausstellungsbehörde und das Ausstellungsdatum anzugeben.

[3] Angabe der jeweiligen höchsten Klassifizierungsstufe sowie Funktion bzw. Zweck für den Zugang (z.B.: GEHEIM, SB VSa II G4Abt/ KdoEU).

[4] Angabe des Staates oder der Organisation und der jeweiligen höchsten Klassifizierungsstufe sowie Funktion bzw. Zweck für den Zugang. Falls erforderlich auch Einschränkung auf konkrete klassifizierte Informationen.

[5] Konkrete Bezeichnung der zu betretenden Liegenschaft gemäß dem Erlass über die Festlegung von Objektschutzkategorien, GZ S93207/140-ndAbw/2023 (z.B.: FIH ZELTWEG, FlWft 2).

Die zur Kenntnis gelangten klassifizierten Informationen unterliegen der Geheimhaltung („need to know") und sind jederzeit vor der Kenntnisnahme durch unbefugte Personen zu schützen.
Der verpflichteten Person werden **folgende Dokumente** (auszugsweise) zur Verfügung gestellt bzw. wurde darauf hingewiesen, wo diese einzusehen sind (Intranet, Internet etc.):

- ☐ Geheimschutzvorschrift
  Richtlinien für den Geheimschutz von multilateralen Unterlagen
  - ☐ Sicherheitsbestimmungen der NATO (in der geltenden Fassung)
  - ☐ Sicherheitsbestimmungen der EU (in der geltenden Fassung)
- ☐ InfoSiG (Informationssicherheitsgesetz)
- ☐ InfoSiV (Informationssicherheitsverordnung)
- ☐ DSG (Datenschutzgesetz)
  Örtlich bedingte Absicherungsmaßnahmen[6]
  - ☐ Zutrittsbestimmungen
  - ☐ Verpflichtung zum Tragen der Identitätskarte
  - ☐ Verbot Fotografieren und Filmen
  - ☐ Verbot Mitnahme Mobiltelefon
  - ☐ Verbot Mitnahme IKT-Geräte (Laptop, Palm, Aufzeichnungsgeräte, udgl.)
  - ☐ Mitnahmeberechtigung
  - ☐ Schlüsselordnung
  - ☐ Brandschutz
- ☐ [7]
- ☐

(Zutreffendes ankreuzen)

Unterschriften

Ort und Datum	Die verpflichtete Person:	Der/Die Sicherheitsbeauftragte: Der/Die Geheimschutzbeauftragte:

[6] Z.B. für Bedienstete, die dauerhaft in einem Sicherheitsbereich Dienst versehen.
[7] Raum für allfällige weitere vor Ort erforderliche oder sonstige Verhaltensregeln.

BEILAGE II

Empfangsschein

EMPFANGSSCHEIN

Innerhalb von 14 Tagen zurück an den Absender!

EMPFÄNGER: _____ bestätigt den Empfang von:
(Dienststempel)

SkZl.	ABSENDER (Dienststempel)	Erl-GZ/Ausfertigung	Beilage	Ev. Nr.

_____, am _____ _____
(Ort) (Datum) (Unterschrift)

BEILAGE III

Bestandsverzeichnis für klassifizierte Informationen

Bestandsverzeichnis für klassifizierte Informationen

Dienststelle: _____ Blatt Nr.: _____

Erhalten				Gegenstandsbezeichnung	abgegeben		vernichtet	Ablagevermerk/ Anmerkung
Lfd. Nr.	am	von Fremdzl. Ausfertigung Nr.	eigene Zl. Ausfertigung Nr.		am	an	am gemäß	

BEILAGE IV

Geschäftsbuch für klassifizierte Informationen

Eigene GZ	des Schreibens: Datum	des Schreibens: Nr.	Eingangsdatum	von	Anzahl d. Beilagen	Gegenstand
612	*2. 6. 25*	*900-Geh/Präs/25*	*4. 6. 25*	*RevB*	*3*	*Kontrollbericht - 2. Ausf. -*
	6. 7. 25	*900-Geh/Abw4/25*	*5. 7. 25*	*Abw4*	*2*	*Informationsschutz Datensicherheit - Akt -*
613	*16. 6. 25*			*Präs*		*Information für FBM über besonderen Vorfall 11.6.2025 - Akt -*

Datum der: Genehmigung	Datum der: Abfertigung	Anzahl d. Beilagen	Erledigung	Hinterlegungsvermerk (Zahl .../...)	Anmerkung
			Oberst N.N. z.K. 10.6.2025		
			Einsichtsverkehr		*Weitergabe an S II 16.6.2025*
16. 6. 25	*17. 6. 25*		*Verteiler: KBM&GS 1. Ausf. S II 2. Ausf.*		

Kurierbescheinigung

.....

(Dienststelle)
(Unit / office / agency)

.....

(Ort, Datum)
(Place, date)

Kurierbescheinigung
Courier Pass

.....

(Amtstitel / Dienstgrad)
(Official title / rank)

(Name)

(Geburtsdatum)
(Date of birth)

Dienstausweis Nr.: */ ID card no.:* .....

Ist berechtigt, vom (am) ..... bis
Is authorised from (on) ..... *to* .....

klassifizierte Informationen folgender Klassifizierungsstufen anzunehmen bzw. zu übergeben:
to take over and to hand over classified information for classifications:

- **VERTRAULICH / CONFIDENTIAL** – national*) – international*)
- **GEHEIM / SECRET** – national*) – international*)
- **STRENG GEHEIM / TOP SECRET**– national*) – international*)

Der / *The* .....
(Dienststellung / *official function*)

.....
(Name, Amtstitel / Dgrd - *Name, official title / rank*)

*) Nichtzutreffendes streichen / *Delete as appropriate*

BEILAGE VI

Zustellbuch für klassifizierte Informationen

Datum	Zahl	Empfänger	Übernahme-bestätigung

BEILAGE VII

Vernichtungsprotokoll

_____ (Dienststelle)

_____ (Ort, Datum)

Vernichtungsprotokoll Nr. … / …

Nachstehende klassifizierte Information(-en) *)

- VERTRAULICH – national
- VERTRAULICH – international
- GEHEIM – national
- GEHEIM – international
- STRENG GEHEIM – national
- STRENG GEHEIM – international

lfd. Nr. von _____ bis _____ wurde(-n) nach erfolgter Überprüfung auf Vollzähligkeit vernichtet:

Lfd. Nr.	Eigene Zahl Fremdzahl	Nr. der Ausf. (Anzahl der Beilagen)	Vernichtet gemäß (Fremdzahl)

Geheimschutzbeauftragte/r:

_____ (Name, Amtstitel/Dienstgrad, Dienststelle)

Zeuge/Zeugin:

_____ (Name, Amtstitel/Dienstgrad, Dienststelle)

GESEHEN

Der Kommandant/Dienststellenleiter: *)
Die Kommandantin/Dienststellenleiterin: *)

_____ (Name, Amtstitel/Dienstgrad, Dienststelle)

*) Nichtzutreffendes streichen.

BEILAGE VIII

Muster für Schriftstück mit korrekten Bezeichnungen

GEHEIM
Seite 1 von 1

Bundesministerium
Landesverteidigung

bmlv.gv.at

[Bezeichnung]

[Sachbearbeiter]

An
Empfängerliste

[E-Mail]
[Telefon]
[Abgabenstelle], [Postleitzahl] [Ort]

Geschäftszahl: [Geschäftszahl inkl. Erledigungsnummer]

[Bezugszahlen der Erledigung (Textblock)]

[Gegenstand der Erledigung]

..... *Erledigungstext* .....

[Ort], am [Genehmigungsdatum]
Für die Bundesministerin:
[Genehmiger inkl. Titel]

Elektronisch gefertigt

Beilagen:
[Liste der Beilagen (Textblock)]

Ergeht an:
Empfängerliste + Ausfertigungsnummer
[Verteiler ohne E-Mail]

Diese klassifizierte Information ist nach Zweckerfüllung/Weisung zu vernichten!

(Erledigung – Original)

GEHEIM

Bundesministerium
Landesverteidigung

bmlv.gv.at

[Bezeichnung]

[Sachbearbeiter]

An
Empfängerliste

[E-Mail]
[Telefon]
[Abgabenstelle], [Postleitzahl] [Ort]

Geschäftszahl: [Geschäftszahl inkl. Erledigungsnummer]

[Bezugszahlen der Erledigung (Textblock)]

GenDatum
1. Ausfertigung für DSt

[Gegenstand der Erledigung]

..... *Erledigungstext* .....

[Ort], am [Genehmigungsdatum]
Für die Bundesministerin:
[Genehmiger inkl. Titel]

Elektronisch gefertigt

Beilagen:
[Liste der Beilagen (Textblock)]

Ergeht an:
Empfängerliste + Ausfertigungsnummer
[Verteiler ohne E-Mail]

Diese klassifizierte Information ist nach Zweckerfüllung/Weisung zu vernichten!

(Ausfertigung)

Bundesministerium
Landesverteidigung

Beilage xxx zu GZ xxx EvidNr.: xxx

Beilage

BEILAGE IX

AUT GEHEIM FREIGEGEBEN FÜR GBR
AUT SECRET RELEASABLE TO GBR
Page 1 of 1

Bundesministerium
Landesverteidigung

bmlv.gv.at

[Bezeichnung]

[Sachbearbeiter]

To
Empfängerliste

[E-Mail]
[Telefon]
[Abgabenstelle], [Postleitzahl] [Ort]

File number: [Geschäftszahl inkl. Erledigungsnummer]

Reference:
[Bezugszahlen der Erledigung (Textblock)]

GenDatum
xx. Copy

[Gegenstand der Erledigung]

..... *Erledigungstext* .....

[Ort], am [Genehmigungsdatum]
On behalf of the Federal Minister:
[Genehmiger inkl. Titel]

Signed electronically

Attachments:
[Liste der Beilagen (Textblock)]

Copy to / cc:
Empfängerliste + Ausfertigungsnummer
[Verteiler ohne E-Mail]

AUT GEHEIM FREIGEGEBEN FÜR GBR
AUT SECRET RELEASABLE TO GBR
- 1 -

BEILAGE X

AUT GEHEIM FREIGEGEBEN FÜR NATO
AUT SECRET RELEASABLE TO NATO
Page 1 of 1

Bundesministerium
Landesverteidigung

bmlv.gv.at

[Bezeichnung]

[Sachbearbeiter]

To
Empfängerliste

[E-Mail]
[Telefon]
[Abgabenstelle], [Postleitzahl] [Ort]

File number: [Geschäftszahl inkl. Erledigungsnummer]

Reference:
[Bezugszahlen der Erledigung (Textblock)]

GenDatum
xx. Copy

[Gegenstand der Erledigung]

..... *Erledigungstext* .....

[Ort], am [Genehmigungsdatum]
On behalf of the Federal Minister:
[Genehmiger inkl. Titel]

Signed electronically

Attachments:
[Liste der Beilagen (Textblock)]

Copy to / cc:
Empfängerliste + Ausfertigungsnummer
[Verteiler ohne E-Mail]

AUT GEHEIM FREIGEGEBEN FÜR NATO
AUT SECRET RELEASABLE TO NATO
- 1 -

STICHWORTVERZEICHNIS

Die Zahlen bezeichnen jene Randnummern,
in denen der Gegenstand behandelt ist.

W

Z