

**Verordnung der Bundesregierung über die Informationssicherheit
(Informationssicherheitsverordnung, InfoSiV)**

StF: [BGBl. II Nr. 548/2003](#)

Änderung

[BGBl. II Nr. 67/2012](#)

[BGBl. II Nr. 131/2018](#)

[BGBl. II Nr. 268/2022](#)

[BGBl. II Nr. 169/2025](#)

Inhaltsverzeichnis

- § 1. Geltungsbereich
- § 2. Klassifizierte Informationen
- § 3. Klassifizierungsstufen
- § 4. Informationssicherheitsbeauftragte
- § 5. Zugang zu klassifizierten Informationen
- § 6. Unterweisung
- § 7. Übermittlung klassifizierter Informationen
- § 8. Kennzeichnung
- § 9. Elektronische Verarbeitung und Übermittlung klassifizierter Informationen
- § 10. Dienstpflichten
- § 11. Administrative Behandlung
- § 12. Registrierung von klassifizierten Informationen
- § 13. Verwahrung von klassifizierten Informationen
- § 14. Kopien und Übersetzungen
- § 15. Vernichtung von klassifizierten Informationen
- § 16. Maßnahmen zum Schutz des Austausches klassifizierter Informationen für Galileo PRS
- § 17. Kontrolle

**Ordinance of the Federal Government on Information Security
(Information Security Ordinance (*Informationssicherheitsverordnung – InfoSiV*))**

← Original version

as amended by:

(list of amendments published in the Federal Law Gazette [F. L. G. = BGBl.])

← amendment entailing the latest update of the present translation

(the German version is updated to reflect also recent amendments; interim changes are highlighted as **deletions** and **insertions** respectively)

Click [here](#) for checking the up-to-date list of amendments in the Austrian Legal Information System.

Table of Contents

- § 1. Scope
- § 2. Classified information
- § 3. Classification levels
- § 4. Information Security Officers
- § 5. Access to classified information
- § 6. Instructions
- § 7. Transmission of classified information
- § 8. Marking
- § 9. Electronic processing and transmission of classified information
- § 10. Official duties
- § 11. Administrative management
- § 12. Registration of classified information
- § 13. Storage of classified information
- § 14. Copies and translations
- § 15. Destruction of classified information
- § 16. Measures for the protection of the exchange of classified information for Galileo PRS
- § 17. Control

§ 18. Inkrafttreten

Geltungsbereich

§ 1. Diese Verordnung gilt für die Dienststellen des Bundes mit Ausnahme der in § 1 Abs. 2 InfoSiG genannten Organe und Einrichtungen.

Klassifizierte Informationen

§ 2. (1) Klassifizierte Informationen im Sinne dieser Verordnung sind mit einem Klassifizierungsvermerk versehene Informationen und Materialien sowie Nachrichten, unabhängig von Darstellungsform und Datenträger, die aus den in § 2 Abs. 1 und 2 InfoSiG genannten Gründen eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen.

(2) Klassifizierte Informationen können insbesondere sein:

1. Schriftstücke;
2. Zeichnungen, Pläne, Karten, Lichtbildmaterial;
3. elektronisch verarbeitete Daten und deren Datenträger (z. B. E-Mail);
4. Ton- und Bildträger;
5. technische Geräte, technische Systeme und deren Teilkomponenten.

Klassifizierungsstufen

§ 3. (1) Klassifizierte Informationen sind zu qualifizieren als

1. EINGESCHRÄNKT (E), wenn die unbefugte Weitergabe der Informationen den in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 [Informationsfreiheitsgesetz, IFG, BGBl I Nr. 5/2024](#) genannten Interessen zuwiderlaufen würde,
2. VERTRAULICH (V), wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist,
3. GEHEIM (G), wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 [IFG](#) genannten Interessen schaffen würde,
4. STRENG GEHEIM (SG), wenn die Informationen geheim sind und überdies ihr bekannt werden eine schwere Schädigung der in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 [IFG](#) genannten Interessen wahrscheinlich machen würde.

(2) Die Klassifizierung, Deklassifizierung sowie die Herabstufung einer Information erfolgt durch ihren Urheber. Die Deklassifizierung ist schriftlich

§ 18. Entry into force

Scope

§ 1. This Ordinance shall apply to the services of the federal government with the exception of the bodies and institutions mentioned in § 1 para. 2 of the Information Security Act.

Classified information

§ 2. (1) Classified information within the meaning of this Ordinance is information and material designated as classified as well as news which – regardless of the format of presentation and data carrier – require special protection against disclosure and access by unauthorised persons for the reasons mentioned in § 2 paras. 1 and 2 of the Information Security Act.

(2) Classified information may consist particularly in:

1. written documents;
2. drawings, plans, maps, photographed material;
3. electronically processed data and the respective data carriers (e.g. e-mails);
4. sound and image recording media;
5. technical devices, technical systems and the respective components.

Classification levels

§ 3. (1) Classified information shall be qualified as

1. “EINGESCHRÄNKT” (E) [RESTRICTED] if unauthorised disclosure of the information would be contrary to the interests mentioned in Art. 20, para. 3 of the [Federal Constitutional Law](#)
2. “VERTRAULICH” (V) [CONFIDENTIAL] if information shall be kept secret under criminal law in accordance with other Federal Acts and if secrecy is in the public interest,
3. “GEHEIM” (G) [SECRET] if information is confidential and if, in addition, disclosure would entail the risk of severely damaging the interests mentioned in Art. 20, para. 3 of the [Federal Constitutional Law](#),
4. “STRENG GEHEIM” (SG) [TOP SECRET] if information is secret and if, in addition, disclosure would probably cause a severe damage to the interests mentioned in Art. 20, para. 3 of the [Federal Constitutional Law](#).

(2) The originator of the information is responsible for classifying, declassifying as well as downgrading information. Declassification shall be

festzuhalten. Empfänger einer klassifizierten Information sind von der Deklassifizierung zu informieren.

Informationssicherheitsbeauftragte

§ 4. (1) Als Informationssicherheitsbeauftragte und deren Stellvertreter dürfen ausschließlich Personen bestellt werden, die einer für die höchste im Ressortbereich angewendeten Klassifizierungsstufe erforderlichen Überprüfung gemäß § 3 Abs. 1 InfoSiG unterzogen wurden.

(2) Die Informationssicherheitsbeauftragten haben die Aufgabe, dafür Sorge zu tragen, dass in ihrem Wirkungsbereich

1. die Informationssicherheit durch organisatorische Maßnahmen gewährleistet ist,
2. die Überwachung der Einhaltung des InfoSiG, dieser Verordnung und der sonstigen Informationssicherheitsvorschriften sichergestellt ist,
3. die jährliche Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen gesichert ist,
4. die Unterweisungen gemäß § 6 nachweislich durchgeführt werden,
5. die erforderlichen Aufzeichnungen gemäß § 5 Abs. 1 und § 12 geführt werden,
6. die Regelungen für Zugang, Übermittlung und Verwahrung von klassifizierten Informationen umgesetzt werden,
7. der Verdacht strafbarer Handlungen im Zusammenhang mit der Informationssicherheit an die Ressortleitung gemeldet wird,
8. bei festgestellten Mängeln auf die unverzügliche Behebung des Mangels hingewirkt wird,
9. Verstöße gegen Sicherheitsvorschriften, deren Kenntnis über den eigenen Wirkungsbereich hinaus von Interesse sein kann, der Informationssicherheitskommission berichtet werden und
10. von der Informationssicherheitskommission verlangte Berichte erstattet werden.

Zugang zu klassifizierten Informationen

§ 5. (1) Der Zugang zu klassifizierten Informationen darf nur unter den Voraussetzungen des § 3 InfoSiG gewährt werden, wobei über die Personen, die tatsächlich Zugang zu Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM erhalten haben, über den Zeitpunkt des Zuganges

recorded in writing. The recipients of classified information shall be informed of declassification.

§ 4. (1) Only persons who were subject to a security clearance procedure in accordance with § 3 para. 1 of the Information Security Act, which is required for the highest qualification level applied in the respective unit of the department may be appointed as Information Security Officers and their deputies.

(2) The Information Security Officers have the task of ensuring that within their sphere of responsibility

1. information security is guaranteed through organisational measures,
2. monitoring of compliance with the Information Security Act, this Ordinance and other information security provisions is guaranteed,
3. an annual review of security arrangements for protecting classified information is conducted,
4. instructions in accordance with § 6 are given in a demonstrable way,
5. the required records are kept in accordance with § 5 para. 1 and § 12,
6. the rules concerning access, transmission and storage of classified information are complied with,
7. any suspicion of punishable offences relating to information security is reported to the head of the department,
8. measures are taken with a view to remedying immediately any defects identified,
9. any violations of security regulations knowledge of which might be relevant also outside the respective sphere of responsibility are reported to the Information Security Commission and
10. reports requested by the Information Security Commission are submitted.

Access to classified information

§ 5. (1) Access to classified information may not be granted unless the requirements of § 3 of the Information Security Act are met; a record shall be kept of the names of persons who actually had access to information classified as

und über die Bezeichnung der Information entsprechende Aufzeichnungen zu führen sind (Muster: **Anlage 1**).

- (2) Einem Bediensteten des Bundes darf der Zugang nur gewährt werden, wenn
1. dies für die Erfüllung seiner dienstlichen Aufgaben erforderlich ist,
 2. der Bedienstete nachweislich gemäß § 6 über den Umgang mit klassifizierten Informationen unterwiesen wurde und
 3. bei Informationen der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG oder eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG durchgeführt wurde.

- (3) Sonstigen Personen darf der Zugang nur gewährt werden, wenn
1. dies für die Ausübung einer im öffentlichen Interesse gelegenen Tätigkeit erforderlich ist,
 2. die Voraussetzungen des Abs. 2 Z 2 und 3 vorliegen und der von der zuständigen Dienststelle vorgesehene Schutzstandard gewährleistet wird und
 3. sie sich zur Geheimhaltung von klassifizierten Informationen auch nach Beendigung der Tätigkeit verpflichtet haben.

(4) In jedem Ressortbereich ist durch geeignete innerorganisatorische Maßnahmen sicherzustellen, dass der Zugang zu klassifizierten Informationen für Bedienstete nur im Rahmen der Erfüllung ihrer dienstlichen Aufgaben, nach nachweislicher Unterweisung und - soweit vorgesehen - nach Abschluss einer Sicherheitsüberprüfung bzw. Verlässlichkeitsprüfung möglich ist. Dies gilt sinngemäß auch für den Zugang sonstiger Personen.

(5) Ein Bediensteter des Bundes darf den Zugang zu klassifizierten Informationen nur dann suchen, wenn er sich vergewissert hat, dass die Voraussetzungen nach Abs. 2 gegeben sind.

Unterweisung

§ 6. (1) Die Unterweisung nach § 5 Abs. 4 hat jedenfalls über das InfoSiG, diese Verordnung, die jeweils gültigen völkerrechtlichen und unionsrechtlichen Verpflichtungen, allfällige schriftlich erlassene Durchführungsregelungen des Ressorts sowie über die Geheimhaltungspflichten und Sanktionen bei Verstößen gegen diese zu erfolgen.

CONFIDENTIAL, SECRET and TOP SECRET, the date and time of access as well as the level of classification (sample: **Annex 1**).

- (2) An employee of the federal civil service may not be granted access unless
1. this is necessary for fulfilling his official duties,
 2. the employee was provably instructed on managing classified information in accordance with § 6 and
 3. a security clearance procedure in accordance with §§ 55 to 55b of the Security Police Act (*Sicherheitspolizeigesetz*) or a reliability screening in accordance with §§ 23 and 24 of the Act on the Powers of the Military (*Militärbefugnisgesetz*) was conducted in respect of information classified as CONFIDENTIAL, SECRET and TOP SECRET.

- (3) Other persons may not be granted access unless
1. this is necessary for performing a task in the public interest,
 2. the requirements of para. 2 points 2 and 3 are met and the level of protection defined by the responsible service is ensured and
 3. they agreed to keep classified information secret even after the completion of their duties.

(4) By taking suitable measures of internal organisation, each unit of a department shall ensure that employees have access to classified information only when performing their official duties, after having received instructions in a demonstrable way and – if applicable – after being security cleared or reliability screened. This shall apply mutatis mutandis to access granted to other persons as well.

(5) An employee of the federal government may not seek access to classified information unless he has ensured that the requirements stipulated in para. 2 have been met.

Instructions

§ 6. (1) In accordance with § 5 para. 4, instructions shall in any event be given regarding the Information Security Act, this Ordinance, any applicable requirements under international law and European Union law, written implementing rules of the department as well as secrecy obligations and sanctions imposed in the event of violations of these requirements.

(2) Die Unterweisung dient der Sensibilisierung für Bedrohungen der Sicherheit von klassifizierten Informationen und soll sicherstellen, dass die vorgesehenen Sicherheitsstandards eingehalten und alle Sicherheitsverletzungen, selbst ein Verdacht auf solche, gemeldet werden. Sie hat vor der Eröffnung des Zugangs zu klassifizierten Informationen zu erfolgen und ist regelmäßig zu wiederholen. Der Nachweis der Unterweisung ist schriftlich festzuhalten (Muster: Anlage 2).

Übermittlung klassifizierter Informationen

§ 7. (1) Vor der Übermittlung von klassifizierten Informationen ist durch Prüfung im Einzelfall oder durch Einhaltung der hierfür vorgesehenen generellen Regelungen sicherzustellen, dass beim Empfänger die Voraussetzungen des InfoSiG und dieser Verordnung gegeben sind.

(2) Im Rahmen der Amtshilfe dürfen klassifizierte Informationen nur übermittelt werden, wenn das ersuchende Organ dies ausdrücklich begehrt und belegt, dass es den erforderlichen Schutzstandard und die vom Gesetz und von der Verordnung verlangten personellen Voraussetzungen zu gewährleisten vermag. Der Informationssicherheitsbeauftragte ist von der beabsichtigten Weitergabe in Kenntnis zu setzen.

(3) Dokumente der Klassifizierungsstufe **EINGESCHRÄNKT** sind im verschlossenen Kuvert und Dokumente der Klassifizierungsstufe **VERTRAULICH** oder höher in einem doppelten undurchsichtigen verschlossenen Kuvert zu übermitteln, wobei nur am inneren Kuvert die Klassifizierungsstufe einschließlich der Anschrift des Empfängers anzugeben und eine Empfangsbestätigung beizulegen ist (Muster: **Anlage 3**). Vermerke am äußeren Kuvert dürfen nicht auf den Inhalt schließen lassen.

(4) Für die Übermittlung von klassifizierten Informationen der Stufe **STRENG GEHEIM** ist die schriftliche Zustimmung des Urhebers erforderlich.

(5) Die Übermittlung von klassifizierten Informationen an Drittstaaten oder internationale Organisationen sowie an einen in einem Drittstaat niedergelassenen Auftragnehmer ist nur mit vorheriger schriftlicher Zustimmung des Urhebers erlaubt, sofern nicht völkerrechtliche oder unionsrechtliche Verpflichtungen die Weitergabe ohne eine solche Zustimmung vorsehen.

(6) Klassifizierte Informationen sind auf folgende Arten zu übermitteln:

1. Mündliche Übermittlung: Bei Besprechungen mit einem Inhalt ab der Klassifizierungsstufe **VERTRAULICH** hat der Besprechungsleiter dafür

(2) The purpose of instructions is to raise awareness of the security risks of classified information and to ensure that the security standards defined are complied with and that all security violations, or any suspicion thereof, are reported. Instructions shall be given before granting access to classified information and shall be repeated regularly. Evidence that these instructions were given shall be recorded in writing (sample: Annex 2).

Transmission of classified information

§ 7. (1) Before the transmission of classified information it is necessary to ensure that the recipient meets the requirements of the Information Security Act and of this Ordinance based on an examination of the individual case or by complying with the applicable general rules.

(2) Within the framework of mutual assistance between authorities, classified information may not be transmitted unless the body filing the request demands this explicitly and proves that it is capable of guaranteeing the necessary standard of protection and of meeting the personnel requirements laid down in the Ordinance. The Information Security Officer shall be informed of any intention to pass on information.

(3) Documents classified as **RESTRICTED** shall be transmitted in a sealed envelope. Documents classified as **CONFIDENTIAL** or having a higher classification level shall be transmitted in a double non-transparent envelope; the classification level – including the address of the recipient – shall be stated only on the inside of the envelope, and a receipt shall be attached (sample: **Annex 3**). It must not be possible to draw conclusions on the content from any notes on the outside of the envelope.

(4) The written consent of the originator is a prerequisite for transmitting information classified as **TOP SECRET**.

(5) Transmission of classified information to third countries or international organisations as well as to a contractor established in a third country is subject to the prior consent of the originator unless requirements laid down in international law or European Union law provide for transmission without consent.

(6) Classified information shall be transmitted in the following way:

1. Oral transmission: In meetings dealing with content classified as **CONFIDENTIAL** or above the chairperson of the meeting shall ensure that

Sorge zu tragen, dass die Teilnehmer entsprechend sicherheitsüberprüft oder verlässlichkeitsgeprüft und belehrt sind. Aufzeichnungen sind zu klassifizieren. Bei der mündlichen Darlegung von Informationen, die als GEHEIM oder STRENG GEHEIM klassifiziert sind, sind Maßnahmen gegen Abhören zu treffen.

2. Persönliche Übermittlung: Klassifizierte Informationen ab der Klassifizierungsstufe VERTRAULICH, die persönlich ausgehändigt werden, sind gegen Empfangsbestätigung zu übergeben. Die Übermittlung innerhalb eines Gebäudes hat durch Personen zu erfolgen, die für die betreffende Klassifizierungsstufe ermächtigt sind, und in einem verschlossenen Kuvert, auf dem nur der Name des Empfängers aufscheint; die Entgegennahme ist mit Empfangsbestätigung zu quittieren. Innerhalb eines Gebäudes oder einer geschlossenen Gebäudegruppe dürfen Informationen bis zur Stufe STRENG GEHEIM in einem verschlossenen undurchsichtigen Kuvert befördert werden.
3. Übermittlung durch Zustelldienste (Post oder private Kurierdienste), militärische und diplomatische Kuriere und diplomatisches Gepäck:
 - a) Klassifizierte Informationen der Stufe EINGESCHRÄNKT dürfen durch die Post oder private Kurierdienste, militärische und diplomatische Kuriere, diplomatisches Gepäck oder Handgepäck einer Person, die entsprechend unterwiesen ist, übermittelt werden. Über die Erfüllung der Schutzmaßnahmen entscheidet die Informationssicherheitskommission.
 - b) Klassifizierte Informationen der Stufe VERTRAULICH dürfen
 - durch die Post oder private Kurierdienste innerhalb der EU-Mitgliedsstaaten sowie in Staaten, mit denen ein bilaterales Abkommen gemäß § 14 InfoSiG oder eine sonstige völkerrechtliche Vereinbarung mit Regelungen über die Übermittlung von solchen Informationen auf diesem Wege besteht, übermittelt werden, sofern die Dienste über geeignete Schutzmaßnahmen verfügen, über deren Erfüllung die Informationssicherheitskommission entscheidet;
 - mit diplomatischem Gepäck oder durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte

a security clearance or a reliability screening was carried out on all participants and that all participants have received the instructions accordingly. Records shall be classified. If information classified as a SECRET or TOP SECRET is presented orally, measures shall be taken against unauthorised interception.

2. Personal transmission: Personally transmitted information classified as CONFIDENTIAL or above shall be delivered against receipt. Information shall be transmitted within a building by persons duly authorised for the respective classification level and in a sealed envelope stating merely the name of the recipient; receipt of the envelope shall be acknowledged with a receipt. Within a building or a closed group of buildings, information up to the classification level TOP SECRET may be handled in a sealed non-transparent envelope.
3. Transmission by delivery services (mail services or private courier services), military and diplomatic couriers and via diplomatic pouch:
 - a) Classified information of the level RESTRICTED may be delivered by mail services or private couriers, military and diplomatic couriers, via diplomatic pouch or in the hand luggage of a person who was instructed accordingly. The Information Security Commission is responsible for taking decisions on compliance with protective measures.
 - b) Classified information of the level CONFIDENTIAL
 - may be transmitted by mail services or private couriers within the EU Member States as well as in states with which a bilateral agreement in accordance with § 14 of the Information Security Act or another agreement under international law laying down requirements regarding the transmission of this type of information in the aforementioned way was entered into – provided that these services ensured adequate protective measures; the Information Security Commission is responsible for taking decisions on compliance with protective measures;
 - may be transmitted via diplomatic pouch or by military and diplomatic couriers as well as in hand luggage provided that the person (or courier) transmitting the classified information has been

Information übermittelt, zumindest bis VERTRAULICH überprüft und hierzu ermächtigt ist (Muster: **Anlage 4**).

- c) Klassifizierte Informationen der Stufe GEHEIM dürfen
- im Inland durch die Post oder private Kurierdienste übermittelt werden, sofern sie über geeignete Schutzmaßnahmen verfügen, über deren Erfüllung die Informationssicherheitskommission entscheidet;
 - durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte Information übermittelt, zumindest bis GEHEIM überprüft und ermächtigt ist (Muster: **Anlage 4**);
 - in Ausnahmefällen durch das diplomatische Gepäck übermittelt werden, wenn keine andere Übermittlungsmöglichkeit zur Verfügung steht.
- d) Klassifizierte Informationen der Stufe STRENG GEHEIM dürfen durch militärische und diplomatische Kuriere sowie als Handgepäck befördert werden, sofern die Person (bzw. der Kurier), die die klassifizierte Information übermittelt, bis STRENG GEHEIM überprüft und ermächtigt ist (Muster: **Anlage 4**).

Kennzeichnung

§ 8. (1) Klassifizierte Informationen sind eindeutig und gut erkennbar durch die in § 3 oder in völkerrechtlichen oder unionsrechtlichen Regelungen festgelegten Kennzeichnungen kenntlich zu machen.

(2) Bei Informationen in Papierform sind das Datum, die Geschäftszahl, der Urheber und auf jeder Seite die Kennzeichnung oben und unten und eine Seitennummerierung anzubringen. Falls erforderlich können weiters angebracht werden:

1. eine Urheberidentifikation;
2. weitere Informationen, wie z. B. Verteilungseinschränkungen (auf jeder Seite);
3. ein Zeitpunkt für die Herabstufung der Klassifizierung.

(3) Bei Informationen in elektronischer Form ist der Dateiname mit der betreffenden Klassifizierungsstufe zu versehen.

security cleared for the classification level of at least up to CONFIDENTIAL and was duly authorised (sample: Annex 4).

- c) Classified information of the level SECRET
- may be delivered in Austria by the mail services or private courier services provided that adequate protective measures were taken by them; the Information Security Commission is responsible for taking decisions on compliance with protective measures;
 - may be transported by military and diplomatic couriers as well as in hand luggage provided that the person (or the courier) transmitting the classified information has been security cleared for a classification level of at least up to SECRET and was duly authorised (sample: **Annex 4**);
 - may in exceptional cases be transmitted via diplomatic pouch provided that no other way of transmission is available.
- d) Information classified as TOP SECRET may be transported by military and diplomatic couriers as well as in hand luggage provided that the person (or courier) transmitting classified information has been security cleared for a classification level up to TOP SECRET and was duly authorised (sample: **Annex 4**).

Marking

§ 8. (1) Classified information shall be marked in a clear and easily visible manner in accordance with § 3 or the rules laid down in international law or European Union law.

(2) Hardcopy information shall be marked with the date, reference number, originator and on the top and bottom of each page the marking and page number. If required, the following data may be included:

1. identification of the originator,
2. other information, e.g. dissemination restrictions (on each page);
3. date for downgrading the classification level.

(3) As far as electronic information is concerned, the classification level shall be added to the name of the file.

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

Elektronische Verarbeitung und Übermittlung klassifizierter Informationen

§ 9. (1) Die Verarbeitung von klassifizierten Informationen in Informations- und Kommunikationssystemen bedarf besonderer Sicherungsmaßnahmen, die abhängig sind von

1. der Klassifizierungsstufe,
2. dem Grad der Abstrahlsicherheit der Geräte,
3. der Art und dem Ausmaß der Vernetzung,
4. den Speichermöglichkeiten und
5. den örtlichen Gegebenheiten.

(2) Informationen ab der Klassifizierungsstufe VERTRAULICH dürfen auf allen Informations- und Kommunikationssystemen verarbeitet werden, sofern eine Akkreditierung durch die Informationssicherheitskommission vorliegt. Die spezifischen Voraussetzungen (Anforderungen sowie Maßstab und Grad der Detaillierung) sind dabei in Abstimmung mit der Informationssicherheitskommission festzulegen. Für Informations- und Kommunikationssysteme, die Informationen der Klassifizierungsstufe EINGESCHRÄNKT verarbeiten, sind je nach Art und Umfang des Systems (Risikostufe bzw. Komplexität und Vernetzung) die Vorgaben der Informationssicherheitskommission zu beachten. In jedem Fall sind Maßnahmen zur Identifizierung und Protokollierung von Zugriffen vorzusehen. Bei Informations- und Kommunikationssystemen, die der Erfüllung von Aufgaben des Bundesheeres gemäß Art. 79 Abs. 1 B-VG dienen, nimmt diese Aufgaben die vom Bundesminister für Landesverteidigung und Sport für seinen Wirkungsbereich bestimmte Zertifizierungsstelle wahr.

(3) Informationen ab der Klassifizierungsstufe VERTRAULICH, die auf elektronischen Geräten verarbeitet werden, sind so zu schützen, dass von den Informationen über elektromagnetische Abstrahlung nicht unbefugt Kenntnis erlangt werden kann (TEMPEST-Sicherheitsvorkehrungen).

(4) Bei der Übermittlung von klassifizierten Informationen auf elektronischem Wege sind besondere Schutzvorkehrungen, insbesondere die der jeweiligen Klassifizierungsstufe entsprechende Verschlüsselung, sowie die Vorgaben der Informationssicherheitskommission zu beachten. Ungeachtet dieser Anforderung können in Notsituationen spezielle Verfahren oder spezielle technische

(4) Any annexes and attachments shall be listed on the first page of documents classified as CONFIDENTIAL or above.

Electronic processing and transmission of classified information

§ 9. (1) The processing of classified information in information and communication systems is subject to special security measures, which depend on

1. the level of classification,
2. the degree of shielding of devices,
3. the type and scope of networks,
4. storage facilities and
5. local circumstances.

(2) Information classified as CONFIDENTIAL or above may be processed in all information and communication systems provided that they have been accredited by the Information Security Commission. The specific prerequisites (requirements as well as the degree and level of detail) shall be laid down in cooperation with the Information Security Commission. For the use of information and communication systems that process information classified RESTRICTED, depending on the type and scope of the system (risk level or complexity and networking), the requirements laid down by the Information Security Commission shall be taken into account. Measures shall in any event be taken to identify and record access to these systems. As far as information and communication systems used to fulfil tasks of the Federal Army in accordance with Article 79 para. 1 of the Federal Constitutional Law are concerned, this task is performed by the certification body appointed by the Federal Minister of National Defence and Sports for his sphere of competence.

(3) Information classified as CONFIDENTIAL or above which is processed by electronic devices shall be protected in a way that prevents unauthorised access to the information through electromagnetic emissions (TEMPEST security arrangements).

(4) If classified information is transmitted electronically, it is necessary to comply with special security arrangements, in particular encryption commensurate with the respective level of classification, as well as the requirements laid down by the Information Security Commission. Irrespective of these requirements, special procedures or special technical configurations may be applied as deemed necessary

Konfigurationen nach Maßgabe der Informationssicherheitskommission angewendet werden. Die Übermittlung von klassifizierten Informationen ab der Klassifizierungsstufe VERTRAULICH ist gemäß den Vorgaben der Informationssicherheitskommission unter Einsatz qualifizierter Signatur bzw. bei automatischer Übermittlung mit technisch gleichwertigen Sicherheitsanforderungen zu protokollieren.

(5) Die Zusammenschaltung eines Informations- und Kommunikationssystems, in dem klassifizierte Informationen verarbeitet werden, mit anderen Systemen bedarf entsprechender Schutzmaßnahmen.

Dienstplichten

§ 10. (1) Die jeweiligen Dienstvorgesetzten haben die Pflicht, sich Kenntnis darüber zu verschaffen, welche Mitarbeiter Zugang zu klassifizierten Informationen haben. Sie haben weiters dafür Sorge zu tragen, dass dieser Zugang nur unter den Voraussetzungen der bezughabenden Vorschriften erfolgt.

(2) Personen, denen Zugang zu klassifizierten Informationen gewährt wird, sind zur Verschwiegenheit über die ihnen dadurch zur Kenntnis gelangten Informationen und zur Einhaltung der vorgesehenen Schutzstandards verpflichtet. Sie sind insbesondere dazu verpflichtet, jeden Verdacht einer Spionagetätigkeit und ungewöhnliche Umstände im Zusammenhang mit der Sicherheit von Informationen umgehend dem Informationssicherheitsbeauftragten zu melden. Andere gesetzliche Meldepflichten bleiben unberührt.

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

Administrative Behandlung

§ 11. (1) Klassifizierte Geschäftsstücke der Klassifizierungsstufen VERTRAULICH, GEHEIM und STRENG GEHEIM sind in einem hiefür vorgesehenen Register (Muster: Anlage 1) zu verbuchen. Dabei ist jedes Geschäftsstück mit einer eigenen Geschäftszahl zu versehen, der Name des Dokuments, die Ausfertigungsnummer, sein Datum und die jeweilige Klassifizierungsstufe anzugeben.

by the Information Security Commission in emergency situations. The transmission of information classified as CONFIDENTIAL or above shall be recorded in accordance with the requirements of the Information Security Commission by using qualified signature or, in the event of automatic transmission, based on technically equivalent security requirements.

(5) The interconnection of an information and communication system in which classified information is processed with other systems is subject to protective measures.

Official duties

§ 10. (1) The respective supervisors shall have the duty of knowing those of their staff members who have access to classified information. They shall also ensure that access is not granted unless the requirements laid down in the relevant provisions are met.

(2) Persons who are granted access to classified information shall maintain secrecy regarding the information obtained in this way and comply with the respective standards of protection. They shall in particular have the duty of reporting without delay any suspicion of espionage as well as any unusual circumstances affecting the security of information to the Information Security Officer. Other legal reporting duties shall remain unaffected thereby.

(3) The loss of classified information shall be reported without delay to the head of service and the Information Security Officer. They shall take all measures deemed necessary to find the respective piece of information, to avoid other disadvantages and to clear up the incident. These measures shall be recorded in the appropriate way. The entity which issued the information shall also be informed of this loss.

Administrative management

§ 11. (1) Classified official documents of the classification levels CONFIDENTIAL, SECRET and TOP SECRET shall be entered into a special register (sample: Annex 1). Each official document shall be marked with a specific reference number, the document name, the number of the copy, the date and respective classification level.

(2) Die auf klassifizierte Systeme bezogenen Verwaltungssysteme sind in geeigneter Weise gegen unbefugten Zugriff und Verlust zu schützen.

Registrierung von klassifizierten Informationen

§ 12. (1) Der Eingang und Ausgang jedes als VERTRAULICH oder höher klassifizierten Dokuments ist zu registrieren, wobei im Register neben den Angaben gemäß § 11 Abs. 1 der Urheber, der Zeitpunkt des Einlangens, der Zeitpunkt der Übermittlung und die Verwaltungseinheit festzuhalten sind (Muster: **Anlage 1**). Jede Phase des Umlaufs der klassifizierten Informationen ist in geeigneter Weise aufzuzeichnen.

(2) Registerbücher für die Klassifizierungsstufen VERTRAULICH und GEHEIM sind zumindest mit der Klassifizierungsstufe EINGESCHRÄNKT, Registerbücher für die Klassifizierungsstufe STRENG GEHEIM mit der Klassifizierungsstufe GEHEIM zu versehen.

(3) Abs. 1 und 2 sind sinngemäß auch bei elektronischer Registrierung zu erfüllen.

Verwahrung von klassifizierten Informationen

§ 13. (1) Informationen sind der jeweiligen Klassifizierungsstufe entsprechend in den Diensträumen gesichert zu verwahren und dürfen nur bei unabdingbaren dienstlichen Notwendigkeiten aus diesen verbracht werden.

(2) Zum physischen Schutz klassifizierter Informationen sind folgende entsprechend abgesicherte Bereiche einzurichten:

1. Verwaltungsbereiche: Bereiche mit sichtbarer äußerer Abgrenzung zur Ermöglichung der Kontrolle von Personen und Fahrzeugen, die nur von Personen betreten werden dürfen, die eine Ermächtigung erhalten haben. Bei allen anderen Personen ist eine ständige Begleitung bzw. gleichwertige Kontrolle sicherzustellen.
2. Besonders geschützte Bereiche: Bereiche mit sichtbarer und geschützter Abgrenzung mit vollständiger Eingangskontrolle (Ausweiskontrolle oder Kontrolle nach Identifikationsklasse 2 gemäß ÖNORM EN 50133-1:2003 „Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen“ vom 1.11.2003) und Ausgangskontrolle (Kontrolle nach Identifikationsklasse 0 gemäß ÖNORM EN 50133-1:2003), die nur von sicherheitsüberprüften, verlässlichkeitsgeprüften oder speziell ermächtigten Personen unbegleitet betreten werden dürfen. Bei allen

(2) The administrative systems relating to classified systems shall be protected against unauthorised access and loss in the appropriate way.

Registration of classified information

§ 12. (1) The receipt and dispatch of each document classified as CONFIDENTIAL or above shall be registered. Besides the information required by § 11 para. 1, the originator, time and date of receipt and of transmission as well as the administrative unit shall also be recorded in the register (sample: **Annex 1**). Each phase of the circulation of classified information shall be recorded in the appropriate way.

(2) Registries for the classification levels CONFIDENTIAL and SECRET shall have a classification level of at least RESTRICTED, registries for the classification level TOP SECRET shall be marked with the classification level SECRET.

(3) Paras. 1 and 2 shall be applicable mutatis mutandis to electronic registration.

Storage of classified information

§ 13. (1) Information shall be stored safely in the offices in accordance with the respective classification level and may not be retrieved unless this is absolutely necessary for official reasons.

(2) The following secure areas shall be established for the physical protection of classified information:

1. Administrative areas: areas which are clearly distinguishable from the exterior allowing checks to be made of persons and vehicles, which may be accessed only by authorised persons. All other persons shall be escorted or controlled by equivalent measures.
2. Highly protected areas: areas which are clearly distinguishable and protected with full access control (checking of identification cards or checks based on identification class 2 in accordance with ÖNORM EN 50133-1:2003 “Alarm Systems – Access Control Systems for Use in Security Applications” of 1 November 2003) and exit control (checks based on identification class 0 in accordance with ÖNORM EN 50133-1:2003), which may be accessed unescorted only by persons who are security cleared, reliability screened or by specially authorised persons. All other persons shall be escorted or controlled by equivalent measures.

anderen Personen ist eine ständige Begleitung bzw. gleichwertige Kontrolle sicherzustellen.

3. **Besonders geschützte Bereiche mit Abhörschutz:** Bereiche, die zusätzlich technisch abgesichert und mit Einbruchmeldeanlagen ausgestattet sind. Nicht zugelassene Kommunikationsverbindungen oder elektronische Ausrüstung oder Kommunikationsgeräte sind verboten. Im Zuge der Eingangskontrolle sind Personen, die den Bereich betreten, auf die Mitnahme verbotener Geräte zu kontrollieren. Regelmäßige Inspektionen und technische Überprüfungen sind durchzuführen.

(3) Die Auswahl geeigneter Maßnahmen zur physischen Absicherung der Räumlichkeiten erfolgt auf der Grundlage einer Einschätzung der Bedrohungslage durch die zuständigen Behörden, wobei Verwaltungsbereiche und besonders geschützte Bereiche zu unterscheiden sind. Derartige Maßnahmen oder eine Kombination von diesen können sein:

1. Zutrittssperre;
2. Einbruchmeldeanlage;
3. Zugangskontrolle;
4. Sicherheitspersonal;
5. Videoüberwachung;
6. Sicherheitsbeleuchtung;
7. sonstige geeignete physische Maßnahmen.

(4) Informationen gemäß § 2 Abs. 2 Z 1, 2 und 4 aller Klassifizierungsstufen sind in versperrten Behältnissen zu verwahren. Dabei sind für die Klassifizierungsstufe EINGESCHRÄNKT Büromöbel, für VERTRAULICH, GEHEIM bzw. STRENG GEHEIM Wertbehältnisse entsprechend der Zuordnung durch die Informationssicherheitskommission zu verwenden.

(5) Für Verwaltungsbereiche und besonders geschützte Bereiche sind entsprechende Dienstanweisungen festzulegen.

(6) Verfahren über die Verwaltung der Schlüssel und Codes sind vom zuständigen Informationssicherheitsbeauftragten festzulegen. Diese Verfahren müssen Schutz vor unbefugtem Zugang gewähren.

Kopien und Übersetzungen

§ 14. (1) Werden Kopien und/oder Übersetzungen von Dokumenten der Klassifizierungsstufe VERTRAULICH, GEHEIM oder STRENG GEHEIM

3. **Highly protected areas with interception protection:** areas with additional technical protection and equipped with intrusion detection systems. Unauthorised communication connections or electronic equipment or communication devices are prohibited. Persons entering this area shall be checked for carrying prohibited devices with them. Regular inspections and technical checks shall be performed.

(3) The selection of suitable measures to ensure the physical protection of premises is based on the assessment of the threat by the responsible authorities. In this process administrative and highly protected areas shall be distinguished. Such measures or a mix of measures may be as follows:

1. access barrier;
2. intrusion detection system;
3. access control;
4. security staff;
5. video surveillance;
6. security lighting;
7. other suitable physical measures.

(4) Information in accordance with § 2 para. 2 points. 1, 2 and 4 of all classification levels shall be stored in locked containers. Locked containers are defined as office furniture for the classification level RESTRICTED and as secure storage units for information of the classification levels CONFIDENTIAL, SECRET or TOP SECRET, which are used based on assignment by the Information Security Commission.

(5) Instructions shall be issued for administrative areas and highly protected areas.

(6) The responsible Information Security Officer shall define procedures for the administration of keys and codes. These procedures must protect against unauthorised access.

Copies and translations

§ 14. (1) Any copies and/or translations of documents of the classification level CONFIDENTIAL, SECRET or TOP SECRET shall be recorded in an appropriate

angefertigt, so ist dies in geeigneter Weise festzuhalten. Jede Kopie ist durch einen geeigneten Zusatz, der auf jeder Seite zu vermerken ist, zu individualisieren. Die Anfertigung von Kopien und Übersetzungen von Informationen der Klassifizierungsstufe STRENG GEHEIM durch Empfänger ist nur mit vorheriger schriftlicher Zustimmung des Urhebers erlaubt. Kopien dürfen ausschließlich unter der unmittelbaren Verantwortung des jeweiligen Leiters der Organisationseinheit und unter Kennzeichnung als Kopie angefertigt werden.

(2) Dokumente der Klassifizierungsstufe VERTRAULICH, GEHEIM oder STRENG GEHEIM dürfen nur von solchen Personen kopiert, abgeschrieben, übersetzt, gescannt, archiviert oder verarbeitet werden, die die Voraussetzungen des § 5 Abs. 2 erfüllen.

Vernichtung von klassifizierten Informationen

§ 15. (1) Der Bestand an klassifizierten Informationen ist möglichst gering zu halten. Werden Informationen nicht mehr benötigt, sind sie mittels geeigneter Verfahren unter Beachtung internationaler und nationaler Vorgaben zu vernichten. Registrierungspflichtige Dokumente werden von der zuständigen Registratur auf Anweisung des Leiters der aufbewahrenden Stelle vernichtet und die Registrierungsinformationen entsprechend aktualisiert. Die Vernichtung von Informationen der Klassifizierungsstufen GEHEIM oder höher hat unter Anwesenheit eines Zeugen zu erfolgen, der über eine Sicherheitsüberprüfung oder Verlässlichkeitsprüfung der entsprechenden Klassifizierungsstufe verfügen muss, und ist im Protokoll durch Unterschrift festzuhalten (Muster: **Anlage 5**). Die Vernichtung von Datenträgern hat nach den von der Informationssicherheitskommission genehmigten Verfahren zu erfolgen.

(2) Der Leiter der aufbewahrenden Stelle einer Information hat festzulegen, wann eine klassifizierte Information zu vernichten ist. Erfolgt keine Festlegung, so ist die Information nach sieben Jahren zu skartieren.

Maßnahmen zum Schutz des Austausches klassifizierter Informationen für Galileo PRS

§ 16. (1) In Österreich nimmt die Agenden der Galileo Public Regulated Service Behörde (PRS Behörde) gemäß Beschluss 1104/2011/EU über die Regelung des Zugangs zum öffentlichen regulierten Dienst, der von dem weltweiten Satellitennavigationssystem bereitgestellt wird, das durch das Programm Galileo eingerichtet wurde, ABl. Nr. L 287 vom 04.11.2011 S. 1, das Bundeskanzleramt wahr.

way. Each copy shall be individualised by making an appropriate annotation, which shall be recorded on each page. Copies and translations of information classified as TOP SECRET by recipients require the prior written consent of the originator. Copies may be produced exclusively under the supervision of the respective head of the organisational unit and by marking them as copies.

(2) Documents of the classification levels CONFIDENTIAL, SECRET or TOP SECRET may be photocopied, copied by hand, translated, scanned, archived or processed only by persons meeting the requirements of § 5 para. 2.

Destruction of classified information

§ 15. (1) The volume of classified information shall be kept as small as possible. Information, which is no longer required, shall be destroyed by using the appropriate procedures and by taking into account international and national requirements. Documents subject to registration are destroyed by the responsible registry following the instructions of the head of the unit responsible for storing them, and the registration information will be updated accordingly. Information of the classification levels SECRET or above shall be destroyed in the presence of a witness who is security cleared or reliability screened for the respective classification level. This shall be noted in the minutes and signed (sample: **Annex 5**). The destruction of data carriers shall conform to the procedures approved by the Information Security Commission.

(2) The head of the unit storing information shall determine when classified information shall be destroyed. If no deadline has been determined, the information shall be destroyed after seven years.

Measures for the protection of the exchange of classified information for Galileo PRS

§ 16. (1) In Austria, the Federal Chancellery performs all duties and responsibilities of the Galileo PRS Authority in accordance with Decision 1104/2011/EU on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme, OJ No. L 287 of 04.11.2011 p.1.

(2) Die gemäß § 8 InfoSiG beim Bundeskanzleramt eingerichtete Informationssicherheitskommission ist über alle Belange, die die Informationssicherheit in diesem Zusammenhang betreffen, regelmäßig zu informieren und zu hören.

Kontrolle

§ 17. Das System der Informationssicherheit ist durch den jeweiligen Informationssicherheitsbeauftragten einmal jährlich nachweislich zu überprüfen oder überprüfen zu lassen. Dabei ist insbesondere die Vollständigkeit der Aufzeichnungen, die Sicherheit der Behältnisse, das Schlüsselsystem und die Sicherungsmaßnahmen von Kommunikations- und Informationssystemen einer Überprüfung zu unterziehen. Liegen Informationen der Klassifizierungsstufe GEHEIM oder STRENG GEHEIM vor, so ist eine vollständige Überprüfung der Vorgänge des abgelaufenen Jahres vorzunehmen.

Inkrafttreten

§ 18. (1) § 16 in der Fassung BGBl. II Nr. 268/2022, tritt mit Ablauf des Tages der Kundmachung im Bundesgesetzblatt in Kraft.

[\(2\) § 3 in der Fassung des Bundesgesetzes BGBl. II Nr. 169/2025 tritt mit 1. September 2025 in Kraft.](#)

Anlage 1

Register

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

- Evidenzliste
- Dokumentenname
- Geschäftszahl (Fremdzahl)
- Ausfertigungsnummer
- Datum
- Seitenumfang
- Klassifizierungsstufe
- Urheber
- Eingang

.....
Datum Unterschrift

(2) The Information Security Commission established in accordance with § 8 Information Security Act shall be informed and heard regularly on all aspects concerning information security in this regard.

Control

§ 17. The Information Security Officer shall examine or have examined the information security system annually in a demonstrable way. In particular, the completeness of records, the safety of containers, the key management system and the security measures taken to protect communication and information systems shall be examined. In the event of information of the classification level SECRET or TOP SECRET, a complete review of the procedures of the preceding year shall be performed.

Entry into force

§ 18. § 16 as amended by the federal law promulgated in Federal Law Gazette II No. 268/2022 shall enter into force on the day following promulgation.

Annex 1

Registry

Registries shall in any case contain the information below. They may be kept in a centralised or decentralised way, as well as separately for the retrieval, forwarding and distribution of information.

- List of inventory
- Name of document
- Reference number(of the other party)
- Number of copy
- Date
- Number of pages
- Level of classification
- Originator
- Receipt

.....
Date Signature

Eigene Geschäftszahl
Übermittlung an

.....
Datum Unterschrift
oder Beilage der Empfangsbestätigung

Vernichtung

.....
Datum Unterschrift

Own reference number
Transmission to

.....
Date Signature
or attachment of receipt

Destruction

.....
Date Signature

Nachweis der Unterweisung

Hiemit wird bestätigt, dass

Herr/Frau

gemäß § 6 der Informationssicherheitsverordnung eine Ausgabe des geltenden Textes des InfoSiG, der Informationssicherheitsverordnung und der nachfolgend aufgelisteten Vorschriften erhalten hat, über die sich daraus ergebenden Pflichten und über die Folgen von Verstößen dagegen informiert wurde.

.....
(Datum)

.....
(Unterschrift des Unterweisenden)

.....
(Unterschrift des Unterwiesenen)

Liste:

.....

Annex 2

Proof of instructions

We hereby confirm that

Mr/Ms

has received according to § 6 Information Security Ordinance copies of the versions in force of the Information Security Act, the Information Security Ordinance and the regulations listed below and was informed on any obligations arising thereof as well as the consequences of any violations.

.....
(Date) (Signature of person giving instructions) (Signature of person receiving instructions)

List:

...

Empfangsbestätigung

Innerhalb von zehn Tagen zurück an den Absender!

Empfangsbestätigung

Der Empfänger bestätigt den Empfang von
Dienststempel

Stückzahl	Absender (Dienststempel)	GZ, Ausfertigungsnummer	Beilagen

..... am
Ort Datum Name in Druckschrift Unterschrift

Receipt

Return to sender within ten days!

Confirmation of Receipt

The recipient..... acknowledges the receipt of
(official stamp)

Number of items	Sender (official stamp)	Reference number, number of copy	Attachments

.....
Place date

.....
Name (in printed characters)

.....
Signature

Kurierbescheinigung

.....
(Dienststelle) (Datum)

Kurierbescheinigung

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

Ausweis Nr.:

ist berechtigt, vom (am) bis

Klassifizierte Informationen EINGESCHRÄNKT *)
VERTRAULICH *)
GEHEIM *)
STRENG GEHEIM *)

für
(Dienststelle)

anzunehmen bzw. zu übergeben.

Der Leiter:

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

*) Nichtzutreffendes streichen

Courier Certificate

.....
(Service) (Date)

Courier Certificate

.....
(Official title/rank) (First and second name)(Date of birth)

Identity card no.:

is entitled to receive/hand over

classified information RESTRICTED *)
CONFIDENTIAL *)
SECRET *)
TOP SECRET *)

for.....
(service)

from (on)..... to.....

The head:

.....
(Name, official title/grade)

*) Delete if not applicable

Anlage 5**Vernichtungsprotokoll**

Folgendes klassifiziertes Dokument wurde vernichtet:

Dokumentenname	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang	

Art der Vernichtung:

Name des Zeugen in Druckschrift:

Organisationseinheit:

.....
(Datum).....
(Unterschrift)

Annex 5**Destruction log**

The following classified documents were destroyed:

Name of document	
Reference number (of the other party)	
Number of copy	
Date	
Number of pages	
Level of classification	
Originator	
Receipt	

Mode of destruction:

Name of the witness in printed characters:

Organisational unit:

.....
(Date)

.....
(Signature)