

Verordnung der Präsidentin des Nationalrates über den Umgang mit klassifizierten und nicht-öffentlichen Informationen in Nationalrat und Bundesrat (Informationsverordnung – InfoV)

StF: [BGBl. II Nr. 58/2015](#)

Änderung

[BGBl. II Nr. 248/2017](#)

Auf Grund des Art. 30 Abs. 6 B-VG, BGBl. Nr. 1/1930, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 102/2014, sowie des § 26 des Informationsordnungsgesetzes – InfoOG, BGBl. I Nr. 102/2014, wird im Einvernehmen mit dem Vorsitzenden des Bundesrates verordnet:

Inhaltsverzeichnis

(Das Inhaltsverzeichnis ist nicht Bestandteil des Textes der Verordnung)

- § 1. Geltungsbereich
- § 2. Sicherheitsbelehrung
- § 3. Verzeichnis berechtigter Personen
- § 4. Kennzeichnung
- § 5. Geschützte Bereiche
- § 6. Aufbewahrung und Bearbeitung
- § 7. Verteilung und Beförderung
- § 8. Mündliche Übermittlung
- § 9. Elektronische Verarbeitung
- § 10. Registrierung
- § 11. Kopien und Übersetzungen
- § 12. Vernichtung
- § 13. Dienstanweisungen

Decree Issued by the President of the National Council concerning the Handling of Classified and Non-Public Information in the National Council and the Federal Council (Information Decree)

← Original version

as amended by:

(list of amendments published in the Federal Law Gazette)

← amendment entailing the latest update of the present translation

Click [here](#) for checking the up-to-date list of amendments

in the Austrian Legal Information System.

Be it decreed, in conjunction with the chairperson of the Federal Council, on the basis of Art. 30 (6) [Federal Constitutional Law](#), Federal Law Gazette No. 1/1930 as last amended by Federal Law Gazette I No. 102/2014, and of § 26 Information Rules Act, Federal Law Gazette I No. 102/2014, that

Contents

(The table of contents is not part of the text of the Decree)

- § 1. Scope of Application
- § 2. Security Briefing
- § 3. List of Authorised Persons
- § 4. Marking
- § 5. Secured Areas
- § 6. Storage and Handling
- § 7. Distribution and Carriage
- § 8. Oral Communication
- § 9. Electronic Processing
- § 10. Registration
- § 11. Copies and Translations
- § 12. Destruction
- § 13. Service Regulations

Geltungsbereich

§ 1. (1) Diese Verordnung gilt für den Bereich des Nationalrates und des Bundesrates.

(2) Soweit in dieser Verordnung auf bundesgesetzliche Bestimmungen verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Sicherheitsbelehrung

§ 2. (1) Jede Person, der auf Grund des InfOG Zugang zu klassifizierten Informationen gewährt wird, ist über den Umgang mit solchen Informationen zu belehren und für Bedrohungen der Sicherheit entsprechend der jeweiligen Klassifizierungsstufe zu sensibilisieren. Die Sicherheitsbelehrung soll sicherstellen, dass die vorgesehenen Sicherheitsstandards eingehalten werden, damit klassifizierte Informationen nicht an Personen gelangen, die über keine Berechtigung gemäß den §§ 13, 14 und 16 InfOG verfügen.

(2) Personen, denen Zugang zu EU-Verschlussachen gewährt wird, sind zudem über die Beachtung der EU-Vorschriften zu belehren.

(3) Die Sicherheitsbelehrung hat vor der Eröffnung des Zugangs zu klassifizierten Informationen schriftlich zu erfolgen und ist jedenfalls zu Beginn jeder Gesetzgebungsperiode des Nationalrates sowie im Fall einer Änderung oder Ergänzung der maßgeblichen Vorschriften und Verpflichtungen zu wiederholen. Der Nachweis der Sicherheitsbelehrung ist schriftlich festzuhalten.

(4) Die Sicherheitsbelehrung hat auch die Sanktionen bei der Verletzung von Geheimhaltungsvorschriften zu umfassen.

Verzeichnis berechtigter Personen

§ 3. Die Registraturen gemäß § 21 InfOG führen je ein ständiges Verzeichnis der Personen, denen auf Grund des InfOG Zugang zu klassifizierten oder nicht-öffentlichen Informationen gewährt wird.

Kennzeichnung

§ 4. (1) Klassifizierte Informationen sind eindeutig und gut erkennbar mit den in § 4 InfOG festgelegten Klassifizierungsstufen zu kennzeichnen.

(2) Folgende Informationen sind als „nicht-öffentlich“ zu kennzeichnen, wenn sie nicht zur Veröffentlichung geeignet sind (§ 3 Abs. 2 InfOG):

1. Vorlagen, Dokumente, Berichte, Informationen und Mitteilungen zu Vorhaben im Rahmen der Europäischen Union oder im Rahmen des

Scope of Application

§ 1. (1) This decree shall apply to the spheres of the National and Federal Councils.

(2) Whenever this decree refers to provisions of federal laws, they shall be applied as amended.

Security Briefing

§ 2. (1) Any person who under the Information Rules Act is granted access to classified information shall be briefed on the handling of such information, and their awareness of threats to the security of classified information shall be raised as appropriate to the respective classification level. The security briefing is to ensure that security standards are complied with to prevent classified information being disclosed to persons not authorised under §§ 13, 14 and 16 Information Rules Act.

(2) Persons granted access to EU Classified Information shall also be briefed on compliance with EU requirements.

(3) The security briefing shall be communicated in writing before access to classified information is granted and shall in any case be repeated at the beginning of each legislative period of the National Council and whenever the respective rules and obligations are amended or complemented. Evidence of the security briefing having been given shall be laid down in writing.

(4) The security briefing shall also pertain to the sanctions for violation of secrecy provisions.

List of Authorised Persons

§ 3. Each of the Registries under § 21 Information Rules Act shall keep a permanent list of persons who under the Information Rules Act are granted access to classified or non-public information.

Marking

§ 4. (1) Classified information shall be marked clearly and visibly with the classification levels defined in § 4 Information Rules Act.

(2) The following information shall be marked “non-public” if it is unsuitable for publication (§ 3 para 2 Information Rules Act):

1. Bills, Documents, Reports, Items of Information and Communications on projects within the framework of the European Union or within the

Europäischen Stabilitätsmechanismus, soweit sie nicht bereits eine entsprechende Kennzeichnung aufweisen;

2. Ersuchen und Mitteilungen im Zusammenhang mit der behördlichen Verfolgung von Abgeordneten gemäß § 10 Abs. 2, 3 und 5 des Geschäftsordnungsgesetzes 1975, BGBl. Nr. 410/1975, Anträge von Behörden gemäß Art. 63 Abs. 2 B-VG sowie Ersuchen um die Ermächtigung zur Verfolgung von Personen wegen Beleidigung des Nationalrates gemäß § 117 Abs. 1 des Strafgesetzbuches, BGBl. Nr. 60/1974;
3. Meldungen nach dem Unvereinbarkeits- und Transparenz-Gesetz, BGBl. Nr. 330/1983, über die der Unvereinbarkeitsausschuss des Nationalrates oder des Bundesrates zu entscheiden hat, unbeschadet der Bestimmungen des § 9 des Bundesverfassungsgesetzes über die Begrenzung von Bezügen öffentlicher Funktionäre, BGBl. I Nr. 64/1997;
4. Informationen, für die ein Ausschuss eine Beschränkung der Einsichtnahme und der Verteilung gemäß § 14 InfOG beschlossen hat, unter Beifügung der Bezeichnung des Ausschusses.

(3) Bei Informationen der Klassifizierungsstufen 2 oder höher sind das Datum, die Geschäftszahl und der Urheber sowie auf jeder Seite der Empfänger, die Klassifizierungsstufe, eine Seitennummerierung und gegebenenfalls die jeweilige Nummer der Kopie anzubringen. Ist eine solche Kennzeichnung im Einzelfall nicht möglich, werden nach Festlegung des zuständigen Registraturverantwortlichen andere geeignete Maßnahmen zur Kennzeichnung angewendet.

(4) Aufgrund einer Dienstanweisung gemäß § 13 Z 3 können unbeschadet des § 21 Abs. 5 der Anlage 1 zum Geschäftsordnungsgesetz 1975 zusätzliche Angaben etwa über den Empfänger angebracht werden.

Geschützte Bereiche

§ 5. (1) Als Verwaltungsbereiche im Sinne des § 20 Z 1 InfOG können Bürobereiche in den Parlamentsgebäuden, Ausschusslokale und speziell zur Bearbeitung und Aufbewahrung von klassifizierten Informationen vorgesehene Bereiche sowie die diese jeweils unmittelbar umgebenden Bereiche festgelegt werden.

(2) Als besonders geschützte Bereiche im Sinne des § 20 Z 2 und 3 InfOG können Bereiche innerhalb von Verwaltungsbereichen festgelegt werden, sofern

framework of the European Stability Mechanism insofar as they have not already been appropriately marked;

2. Requests and notifications in connection with the public prosecution of Members under § 10 paras 2, 3 and 5 Rules of Procedure Act 1975, Federal Law Gazette No. 410/1975, requests of authorities under Art. 63 para 2 [Federal Constitutional Law](#) as well as requests for the authority to prosecute persons for insulting the National Council under § 117 para 1 Criminal Code, Federal Law Gazette No. 60/1974;
3. Information provided under the Incompatibility and Transparency Act, Federal Law Gazette No. 330/1983, on which the Incompatibility Committee of the National or Federal Council has to decide, without prejudice to the provisions of § 9 of the Federal Constitutional Act on the Limitation of Emoluments of Holders of Public Offices, Federal Law Gazette I No. 64/1997;
4. Information whose inspection and distribution has been restricted by committee decision under § 14 Information Rules Act, in which case the marking shall include the committee name.

(3) Information classified at level 2 or higher shall bear the date, a reference number and the name of the originator and, on each page, the name of the recipient, the classification level, consecutive page number and, if appropriate, the serial number of the copy. If, in individual cases, such marking is impossible, other suitable methods of marking shall be used as determined by the person in charge of the Registry.

(4) § 21 para 5 of Annex 1 to the Rules of Procedure Act 1975 notwithstanding, further details, e.g. pertaining to the recipient, may be indicated if so provided by service regulations issued under § 13 [3].

Secured Areas

§ 5. (1) Office areas in the Parliament buildings, committee rooms and areas specifically designated for handling and storage of classified information, as well as the areas immediately surrounding such areas, may be established as administrative areas in terms of § 20 [1] Information Rules Act.

(2) Areas within administrative areas may be established as specially secured areas in terms of § 20 [2] and [3] Information Rules Act if they are fitted with

durch entsprechende Vorkehrungen, insbesondere durch Schließanlage oder elektronische Zutrittskontrolle sichergestellt ist, dass nur speziell ermächtigte Personen diesen Bereich selbständig betreten können.

Aufbewahrung und Bearbeitung

§ 6. (1) Klassifizierte Informationen sind der jeweiligen Klassifizierungsstufe entsprechend gesichert in versperrten Behältnissen aufzubewahren. Dabei erfolgt die Aufbewahrung klassifizierter Informationen

1. der Stufe 1 im Verwaltungsbereich in einem geeigneten, verschließbaren Büromöbel oder im besonders geschützten Bereich,
2. der Stufen 2 und 3 im besonders geschützten Bereich in einem Sicherheitsbehältnis oder Tresorraum,
3. der Stufe 4 im besonders geschützten Bereich in
 - a) einem Sicherheitsbehältnis mit ständiger Bewachung oder Kontrolle oder mit zugelassener Einbruchsmeldeanlage in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst oder
 - b) einem mit einer Einbruchsmeldeanlage ausgestatteten Tresorraum in Verbindung mit Bereitschaftspersonal im Sicherheitsdienst.

(2) Klassifizierte Informationen der Stufe 1 dürfen für einen begrenzten Zeitraum auch außerhalb der geschützten Bereiche aufbewahrt werden, wenn die Beförderung in einer Verpackung erfolgt, die keine Rückschlüsse auf den Inhalt ermöglicht, und der Besitzer entsprechend der Sicherheitsbelehrung gemäß § 2 einen vergleichbaren Sicherheitsstandard wie in den geschützten Bereichen garantiert.

(3) Die Bearbeitung klassifizierter Informationen erfolgt grundsätzlich in geschützten Bereichen, wobei die Bearbeitung klassifizierter Informationen

1. bis zur Stufe 2 im Verwaltungsbereich zulässig ist, sofern sie vor dem Zugang Unbefugter geschützt werden,
2. der Stufe 3 und 4 ausschließlich im besonders geschützten Bereich erfolgt.

(4) Klassifizierte Informationen bis zur Stufe 2 dürfen außerhalb der geschützten Bereiche bearbeitet werden, wenn

1. die Beförderung in einer Verpackung erfolgt, die keine Rückschlüsse auf den Inhalt ermöglicht, und der Besitzer entsprechend der Sicherheitsbelehrung gemäß § 2 einen vergleichbaren Sicherheitsstandard

appropriate devices, in particular a locking system or electronic access control system, ensuring that unescorted access is granted only to persons who are specifically authorised.

Storage and Handling

(1) Classified information shall be stored in locked containers in accordance with its respective classification level. Accordingly, storage shall be effected as follows:

1. classified information of level 1 in the administrative area in suitable, locked items of office furniture or in the specially secured area,
2. classified information of level 2 or 3 in the specially secured area in a security container or strong room,
3. classified information of level 4 in the specially secured area in
 - a) a security container with continuous protection or verification or an approved IDS in combination with response security personnel or
 - b) an IDS-equipped strong room in combination with response security personnel.

(2) Information classified at level 1 may temporarily be stored outside the secured areas if it is carried in a cover that prevents observation of its contents and the holder of that information has been duly briefed under § 2 and can warrant a security standard equal to that of the secured areas.

(3) Classified information shall in principle be handled in secured areas, the handling of

1. classified information up to level 2 being permitted in the administrative area on condition that it is secured from access by unauthorised persons, while
2. classified information of levels 3 and 4 shall be handled exclusively in the specially secured areas.

(4) Classified information up to level 2 may be handled outside the secured areas if

1. it is carried in a cover that prevents observation of its contents and the holder of that information has been duly briefed under § 2 and can warrant a security standard equal to that of the secured areas and

wie in den geschützten Bereichen garantiert, sowie

2. bei klassifizierten Informationen der Stufe 2 der Besitzer die klassifizierte Information jederzeit unter persönlicher Kontrolle hält.

(5) In der Öffentlichkeit sollen klassifizierte Informationen nicht gelesen oder erörtert werden.

Verteilung und Beförderung

§ 7. (1) Die Verteilung von EU-Verschlusssachen der Stufe 1 erfolgt durch die Datenbanken gemäß § 2 Abs. 2 und 3 des EU-Informationsgesetzes, BGBl. I Nr. 113/2011.

(2) Die Verteilung und Beförderung von klassifizierten Informationen erfolgt mit Ausnahme der Fälle des § 6 Abs. 2 und 4 ausschließlich durch die Registraturen gemäß § 21 InfOG.

(3) Klassifizierte Informationen der Stufe 2 oder höher sind gegen Empfangsbestätigung zu übergeben. Die Übermittlung hat durch Personen zu erfolgen, die für die betreffende Klassifizierungsstufe ermächtigt sind.

(4) Für die Beförderung innerhalb und zwischen der dem Parlament zugehörigen Gebäude sind klassifizierte Informationen der Stufen 1, 2 und 3 so zu verpacken, dass keine Rückschlüsse auf ihren Inhalt möglich sind. Klassifizierte Informationen der Stufe 4 sind in einem gesicherten Umschlag zu befördern.

Mündliche Übermittlung

§ 8. (1) Klassifizierte Informationen der Stufen 2 und 3 dürfen nur in geschützten Bereichen und in Anwesenheit von Personen, die für die jeweilige Stufe berechtigt sind, mündlich übermittelt werden.

(2) Telefongespräche über diese Informationen dürfen ohne Maßnahmen gegen Abhören nur in außergewöhnlichen und dringenden Fällen geführt werden. In diesen Fällen sind die Gespräche so vorsichtig zu führen, dass der Sachverhalt Dritten nicht verständlich wird.

(3) Bei der mündlichen Übermittlung von klassifizierten Informationen der Stufe 4 sind zusätzlich Maßnahmen gegen Abhören zu treffen.

Elektronische Verarbeitung

§ 9. (1) Bei der elektronischen Verarbeitung klassifizierter Informationen soll sichergestellt werden, dass die im InfOG und in der Maßnahmenbeschreibung gemäß Abs. 2 beschriebenen Sicherheitsstandards eingehalten werden, damit klassifizierte Informationen nicht an Personen gelangen, die über keine

2. in the case of classified information of level 2 the information is at all times under the holder's personal control.

(5) Classified information should not be read or discussed in public places.

Distribution and Carriage

§ 7. (1) Distribution of EUCI of level 1 shall be effected through the databases under § 2 paras 2 and 3 EU Information Act, Federal Law Gazette I No. 113/2011.

(2) Except for the cases of § 6 paras 2 and 4, distribution and carriage of classified information shall be strictly reserved to the registries under § 21 Information Rules Act.

(3) Delivery of classified information of level 2 or higher shall be acknowledged by a certificate of receipt. Carriage of such information shall be reserved to persons who are security cleared to the respective classification level.

(4) For carriage within and between Parliament buildings, classified information of levels 1, 2 and 3 shall be covered in such manner as to prevent observation of its contents. Classified information of level 4 shall be carried in a secured envelope.

Oral Communication

§ 8. (1) Classified information of levels 2 and 3 may be orally communicated only in secured areas and only in the presence of persons who are security cleared to the respective classification level.

(2) Such information may only in extraordinary and urgent cases be the subject of telephone conversations without anti-tapping protection. Such conversations shall be conducted with such discretion as to ensure that no third person can understand the facts.

(3) Oral communication of classified information of level 4 shall require additional measures protecting against eaves-dropping.

Electronic Processing

§ 9. (1) When electronically processing classified information, compliance with the security standards specified in the Information Rules Act and in the description of measures under para 2 below should be ensured in order to prevent classified information being disclosed to persons not authorised under §§ 12 to 16

Berechtigung gemäß den §§ 12 bis 16 InfOG verfügen. Dazu dienen entsprechende Belehrungen der berechtigten Personen. Klassifizierte Informationen der Stufe 2 oder höher dürfen – ausgenommen zum Zweck der Erstellung von Protokollen und auszugsweisen Darstellungen sowie zur Anfertigung von Kopien durch die Registratur – nicht elektronisch verarbeitet werden.

(2) Die Sicherungsmaßnahmen sind abhängig vom Ausmaß der Vernetzung, von den Speichermöglichkeiten und den örtlichen Gegebenheiten. Ihre konkrete Festlegung und Aktualisierung erfolgt anhand einer von der Parlamentsdirektion und den Klubs gemeinsam erarbeiteten Maßnahmenbeschreibung, die jedenfalls Folgendes zu beinhalten hat:

1. Es müssen entsprechende Vorkehrungen zur Erkennung von Schadsoftware getroffen werden. Jedes IKT-System muss geeignete Schutzmaßnahmen vor anderen, möglicherweise unsicheren Netzwerken oder verbundenen Computern treffen.
2. Die Übermittlung klassifizierter Informationen der Stufe 1 (elektronischer Transport oder Transport auf externen Datenträgern außerhalb geschützter Bereiche) hat grundsätzlich mittels kryptographischer Produkte und Verfahren zu erfolgen. Unverschlüsselte Dateinamen, Überschriften und Beschriftungen etc. dürfen dabei keine Rückschlüsse auf die klassifizierten Inhalte zulassen.
3. Findet die Übertragung innerhalb geschützter Bereiche statt, kann von einer Verschlüsselung abgesehen werden.
4. Findet die Übertragung außerhalb geschützter Bereiche statt, ist entweder eine Sicherung des Übertragungsweges mit kryptographischen Maßnahmen oder eine Ende-zu-Ende-Verschlüsselung vorzusehen. Beim Ausdruck klassifizierter Dokumente ist darauf zu achten, dass der Zugang zum Ausdruck nur für berechtigte Personen möglich sein darf und dass die Kennzeichnung gemäß § 4 erfolgt.

(3) In IKT-Systemen ist sicherzustellen, dass der Zugriff zu nicht-öffentlichen oder klassifizierten Informationen nur unter der Voraussetzung der §§ 12 bis 16 InfOG erfolgt. Für jedes IKT-System, in dem nicht-öffentliche oder klassifizierte Informationen verarbeitet werden, ist ein entsprechender Zugriffsschutz auf das System sicherzustellen. Jeder Benutzer muss eindeutig identifiziert werden.

Registrierung

§ 10. (1) Klassifizierte Informationen der Klassifizierungsstufen 2, 3 und 4

Information Rules Act. For this purpose, the authorised persons shall be given an appropriate briefing. Classified information of level 2 or higher may not be processed electronically – excluded for the purpose of funding records and in extracts presentations as well as for making copies by the registry.

(2) Security measures shall depend on the degree of interconnectivity, the storage capacity and the local conditions. Their final design and update shall be based on a description of measures, jointly prepared by the Parliamentary Administration and the parliamentary groups, which shall in any case provide that:

1. Appropriate provisions shall be made to ensure the detection of damaging software. Each ICT system must provide for adequate protection against other, potentially unsafe networks or connected computers.
2. Communication of classified information of level 1 (electronic transmission or transport on external storage devices outside secured areas) shall be effected by means of cryptographic products and processes. Unencrypted file names, headings, markings etc. must not betray the classified contents.
3. For transmission within secured areas, encryption may be dispensed with.
4. For transmission outside secured areas, a cryptographically secured transmission path or end-to-end-encryption shall be provided. When printing classified documents, it shall be ensured that access to the printout shall be restricted to authorised persons and that the printout is marked in accordance with § 4.

(3) It shall be ensured that access to non-public or classified information in ICT systems shall only be granted subject to the provisions of §§ 12 to 16 Information Rules Act. Each ICT system processing non-public or classified information shall be provided with appropriate access protection. Each user must be uniquely identified.

Registration

§ 10. (1) Classified information of levels 2, 3 and 4 shall be registered.

sind zu registrieren. Die Registrierung erfolgt in dafür vorgesehenen Geschäftsbüchern, die nach Klassifizierungsstufen zu unterscheiden sind. Jede Registratur gemäß § 21 InfOG führt eigene Geschäftsbücher, die ausschließlich für ihren Bereich verwendet werden.

(2) Die Geschäftsbücher gemäß Abs. 1 sind mit einer eigenen Klassifizierungsstufe zu versehen. Geschäftsbücher, in denen Informationen der Klassifizierungsstufen 2 oder 3 registriert werden, sind zumindest mit der Klassifizierungsstufe 1 zu versehen. Geschäftsbücher, in denen Informationen der Klassifizierungsstufe 4 registriert werden, sind mit der Klassifizierungsstufe 3 zu versehen.

(3) Zu registrieren sind die Erstellung oder der Empfang einer registrierungspflichtigen klassifizierten Information sowie deren Vervielfältigung, Übersetzung, Verteilung, Rückgabe, Umstufung, Freigabe und Vernichtung.

(4) Jede registrierungspflichtige klassifizierte Information ist mit einer eigenen Geschäftszahl zu versehen. Festzuhalten sind jedenfalls das Erstellungs- oder Eingangsdatum, der Urheber, der Gegenstand und die Klassifizierungsstufe, die jeweilige Nummer der Kopie, der Name des Empfängers sowie das Datum der Übermittlung, Rückgabe, Umstufung, Freigabe und Vernichtung.

(5) Bei einer Umstufung hat die Registrierung in den Geschäftsbüchern sowohl der bisherigen als auch der neuen Klassifizierungsstufe zu erfolgen. Empfänger einer registrierten klassifizierten Information sind von der Umstufung oder Freigabe zu informieren.

(6) Werden EU-Verschlussachen der Klassifizierungsstufe „Très Secret UE/EU Top Secret“ von einer anderen Stelle als der Zentralregistratur im Bundesministerium für europäische und internationale Angelegenheiten übermittelt, so ist diese davon unverzüglich nachweislich in Kenntnis zu setzen.

Kopien und Übersetzungen

§ 11. (1) Kopien und Übersetzungen von klassifizierten Informationen der Stufe 2 oder höher sind nur von der zuständigen Registratur in besonders geschützten Bereichen anzufertigen. Jede Kopie ist als solche zu kennzeichnen und durch die jeweilige Nummer der Kopie zu individualisieren.

(2) Die Anfertigung von Kopien oder Übersetzungen von klassifizierten Informationen der Stufe 4 ist nur mit vorheriger schriftlicher Zustimmung des Urhebers erlaubt.

(3) Die Anfertigung von Abschriften von klassifizierten Informationen der

Registration shall take the form of recording the classified information in dedicated journals for each of the classification levels. Each of the Registries under § 21 Information Rules Act shall keep its own journals which shall be exclusively used for the sphere of the respective Registry.

(2) The journals under para 1 shall themselves be assigned a classification level. Journals for the registration of information of classification level 2 or 3 shall at least be classified at level 1. Journals for the registration of information of classification level 4 shall be classified at level 3.

(3) Registration shall evidence the creation or receipt of registrable classified information, its reproduction (copying), translation, distribution, return, re-classification, declassification and destruction.

(4) Each classified information which shall be registered shall be marked with a reference number and shall indicate the date of creation or receipt, its originator, the subject matter, classification level, the serial number of the copy in question, the name of the recipient and the dates of communication, return, re-classification, declassification and destruction.

(5) If information is re-classified, it shall be recorded in the journal dedicated to the former classification level as well as in that dedicated to the new one. Recipients of registered classified information shall be informed of the re-classification or declassification.

(6) Whenever EUCI of classification level "Très Secret UE/EU Top Secret" is communicated by an agency other than the Central Registry in the Federal Ministry of European and International Affairs the latter shall demonstrably be informed of said communication without delay.

Copies and Translations

(1) Copies and translations of classified information of level 2 or higher shall only be produced by the responsible Registry in specially secured areas. Each copy shall be designated as such and individualised by serial numbers.

(2) Copies and translations of classified information of level 4 shall only be made with the approval in writing on the part of the originator.

(3) Except for the cases of § 21 para 1 (2) of Annex 1 to the Rules of

Stufe 2 oder höher und die Erstellung von Notizen über den die Klassifizierung begründenden Inhalt sind mit Ausnahme der Fälle des § 21 Abs. 1 Z 2 der Anlage 1 zum Geschäftsordnungsgesetz 1975 nicht zulässig.

(4) Die für das Original einer klassifizierten Information geltenden Bestimmungen finden auf Kopien, Notizen und Übersetzungen Anwendung.

Vernichtung

§ 12. (1) Klassifizierte Informationen sind mittels geeigneter Verfahren zu vernichten. Registrierungspflichtige klassifizierte Informationen werden ausschließlich von der zuständigen Registratur vernichtet.

(2) Über die Vernichtung registrierungspflichtiger klassifizierter Informationen ist ein Vernichtungsprotokoll anzulegen, das anstelle der vernichteten klassifizierten Information aufzubewahren ist. Vernichtungsprotokolle für klassifizierte Informationen der Stufen 2 und 3 sind mindestens fünf Jahre, Vernichtungsprotokolle für klassifizierte Informationen der Stufe 4 mindestens zehn Jahre aufzubewahren.

Dienstanweisungen

§ 13. Durch entsprechende Dienstanweisungen sind insbesondere festzulegen:

1. Verwaltungsbereiche und besonders geschützte Bereiche sowie die Verwaltung der jeweiligen Schlüssel und Codes in Absprache mit den über die jeweiligen Räume Verfügungsberechtigten,
2. Muster für den Nachweis der Sicherheitsbelehrung, die Registrierungsinformationen, die Empfangsbestätigung und das Vernichtungsprotokoll,
3. zusätzliche Angaben über den Empfänger, insbesondere die Bezeichnung des Klubs, der Fraktion oder der Parlamentsdirektion zur individuellen Kennzeichnung von Kopien gemäß § 4.

Procedure Act 1975, it shall not be permitted to make hand-written copies of classified information of level 2 or higher or to take notes of the content which was the cause of the document being classified.

(4) All provisions pertaining to the original of classified information shall likewise apply to all copies, notes and translations.

Destruction

§ 12. (1) Classified information shall be destroyed by appropriate processes. Registrable classified information shall be destroyed exclusively by the responsible Registry.

(2) Destruction of registrable classified information shall be evidenced in a destruction record that is to be kept on file in lieu of the classified information destroyed. Destruction records in respect of classified information of levels 2 and 3 shall be retained for at least five years, those of classified information of level 4 for a minimum of ten years.

Service Regulations

§ 13. Service regulations shall in particular define

1. Administrative areas and specially secured areas and, in coordination with the persons having authority over the respective rooms, the management of the respective keys and codes,
2. Samples of forms for evidencing security briefing, registration information, confirmation of receipt and the destruction record,
3. Further details pertaining to the recipient, such as in particular the name of the National Council group, Federal Council group or Parliamentary Administration, for individual marking of copies in accordance with § 4.