SICHERHEITSUNTERWEISUNG

EINLEITUNG

Die Sicherheitsunterweisung ist ein vorgeschriebener Schritt im Verfahren für den Zugang zu Verschlusssachen der EU. Das Ziel der Unterweisung ist es, Sie über das Wesen und den Schutz von Verschlusssachen, die Zugangsbedingungen und über Ihre Verantwortung beim Schutz der Vertraulichkeit solcher Verschlusssachen zu informieren.

Diese schriftliche Sicherheitsunterweisung wurde ausschließlich für Mitglieder des Europäischen Parlaments erstellt. Als Mitglied des Europäischen Parlaments sollten Sie die Sicherheitsunterweisung lesen und die Empfangsbestätigung unterschreiben und persönlich beim Referat Verschlusssachen abgeben oder per Hauspost zurückschicken, um die Unterweisung zu bestätigen.

Nach dem Lesen und der Bestätigung des Empfangs dieser Unterweisung kann Mitgliedern nach Unterzeichnung einer förmlichen Erklärung Zugang zu an sie gerichteten Verschlusssachen bis zur Stufe EU-CONFIDENTIAL gewährt werden.

Mitglieder, die Zugang zu Verschlusssachen der Stufe EU-CONFIDENTIAL oder höher benötigen, müssen sich einer Sicherheitsüberprüfung unterziehen. Die EP-Sicherheitsermächtigung wird nach positivem Ergebnis einer Sicherheitsüberprüfung durch die nationale Sicherheitsbehörde im Heimatland des Mitglieds erteilt. In einigen Mitgliedstaaten kann Mitgliedern des Europäischen Parlaments Zugang zu diesen Verschlusssachen ohne vorherige nationale Sicherheitsüberprüfung gewährt werden. In diesen Fällen müssen sich die Mitglieder dennoch einer formellen mündlichen Sicherheitsunterweisung unterziehen und ihnen muss durch den Präsidenten des Europäischen Parlaments eine EP-Sicherheitsermächtigung (EP-PSC) erteilt werden.

Wenn der Zugang zu Verschlusssachen außerhalb der Räumlichkeiten des Parlaments stattfinden soll, benötigen Sie ein spezielles Zertifikat, das sie beim Referat Risikobewertung (DG SAFE) auf Anfrage erhalten können.

WAS SIND VERSCHLUSSSACHEN?

Verschlusssachen lassen sich anhand von drei Merkmalen von anderen Informationskategorien unterscheiden:

- Sie unterliegen Gesetzen und Vorschriften zu Staats- oder Amtsgeheimnissen

- Personen, die den Inhalt von Verschlusssachen an nicht berechtigte Dritte weitergeben, können strafrechtlich verfolgt werden
- Der Zugang zu ihnen wird, solange sie bestehen, streng kontrolliert und verwaltet durch Sicherheitsmaßnahmen, die dem Schutz ihrer Vertraulichkeit, Vollständigkeit und Verfügbarkeit dienen.

GEHEIMHALTUNGSGRADE

Die für den Schutz der Verschlusssachen angewandten Sicherheitsmaßnahmen richten sich nach der Geheimhaltungsstufe der Informationen. Auf europäischer Ebene gibt es vier Stufen für Verschlusssachen (EU-Verschlusssachen – EUCI):

EU-Informationen werden eingestuft als	**Wenn durch die Weitergabe der EU-Informationen oder der Materialien**
TRES SECRET UE/EU TOP SECRET	den wesentlichen Interessen der Union oder eines oder mehrerer ihrer Mitgliedstaaten außerordentlich schwerer Schaden zugefügt würde
SECRET UE/EU SECRET	den wesentlichen Interessen der Union oder eines oder mehrerer ihrer Mitgliedstaaten schwerer Schaden zugefügt würde
CONFIDENTIEL UE / EU CONFIDENTIAL	den wesentlichen Interessen der Union oder eines oder mehrerer ihrer Mitgliedstaaten Schaden zugefügt würde
RESTREINT UE / EU RESTRICTED	für die Interessen der EU oder eines oder mehrerer ihrer Mitgliedstaaten Nachteile entstehen könnten

„Gleichwertige Verschlusssachen“ sind Verschlusssachen, die von Mitgliedstaaten, Drittstaaten oder internationalen Organisationen erstellt wurden, deren Verschlusssachenkennzeichnung einer der Verschlusssachenkennzeichnungen für EUCI gleichwertig ist und die der Rat oder die Kommission dem Europäischen Parlament übermittelt hat.

Alle Verschlusssachen werden vom Ersteller des Materials gut sichtbar gekennzeichnet. Mit dieser Kennzeichnung werden die Empfänger über die Geheimhaltungsstufe und den erforderlichen Grad des Schutzes für das Material informiert. Bei einer Sicherheitseinstufung kann es sich um ein aufwendiges Verfahren handeln, und es gibt spezielle Anforderungen für verschiedene Arten von Material. Bei Dokumenten wird jeweils ein Sicherheitseinstufungs-Stempel für EUCI oben und unten auf jeder Seite des Dokuments angebracht. Bei Dokumenten des Rats werden Verschlusssachenkennzeichnungen auf EN oder FR verwendet. Die Kommission verwendet nur Stempel auf FR zur Angabe von Geheimhaltungsgraden.

REGELUNGSRAHMEN FÜR EU-VERSCHLUSSSACHEN (EUCI)

Der Umgang mit EUCI im Europäischen Parlament wird durch den *Beschluss des Präsidiums des Europäischen Parlaments vom 15. April 2013 über die Regeln zur Behandlung vertraulicher Informationen durch das Europäische Parlament*[1] geregelt, der am 1. April 2014 in Kraft trat.

In dem Beschluss des Präsidiums werden die Mindestsicherheitsanforderungen des Europäischen Parlaments für den Schutz von EUCI innerhalb seiner Räumlichkeiten geregelt. Sie sind den Sicherheitsanforderungen anderer EU-Organe gleichwertig. Ohne eine solche Gleichwertigkeit wäre der Austausch von EUCI zwischen EU-Organen nicht möglich.

Die Weitergabe von EUCI an das Parlament wird geregelt durch:

- die Interinstitutionelle Vereinbarung vom 20. November 2002 zwischen dem Europäischen Parlament und dem Rat über den Zugang des Europäischen Parlaments zu sensiblen Informationen des Rates im Bereich der Sicherheits- und Verteidigungspolitik [2], nach der die Einsichtnahme in vertrauliche Informationen über EU CONFIDENTIAL nur dem Präsidenten und Mitgliedern eines Sonderausschusses in den Räumlichkeiten des Rats genehmigt werden kann;

- Anhang II der Rahmenvereinbarung vom 20. Oktober 2010 über die Beziehungen zwischen dem Europäischen Parlament und der Europäischen Kommission[3], in dem der Zugang und besondere Vorkehrungen zum Schutz der Vertraulichkeit der Informationen vorgesehen sind, die im gegenseitigen Einvernehmen vor der Weitergabe der Informationen festgelegt werden sollen. Diese Vorkehrungen sind zwischen dem für den jeweiligen Politikbereich zuständigen Mitglied der Kommission und dem Vorsitzenden des parlamentarischen Gremiums/Amtsträger, der die Anfrage eingereicht hat, zu vereinbaren.

- die Interinstitutionelle Vereinbarung vom 12. März 2014 zwischen dem Europäischen Parlament und dem Rat über die Übermittlung an und die Bearbeitung durch das Europäische Parlament von im Besitz des Rates befindlichen Verschlusssachen in Bezug auf Angelegenheiten, die nicht unter die Gemeinsame Außen- und Sicherheitspolitik fallen[4].

WARUM MÜSSEN VERSCHLUSSSACHEN GESCHÜTZT WERDEN?

EU-Organe sind lohnende Ziele. Spionage kann zu schwerwiegenden Verletzungen der politischen und administrativen Integrität führen und schwerwiegende Folgen für die EU und/oder Mitgliedstaaten haben.

[1] ABl. C 96 vom 1.4.2014, S. 1-51.
[2] ABl. C 298 vom 30.11.2002, S. 1-3.
[3] ABl. L 304 vom 20.11.2011, S. 56-60.
[4] ABl. C 95 vom 1.4.2014, S. 1-7.

Geheim- und Nachrichtendienste wenden verschiedene Methoden zum Sammeln von Informationen an. Während das Sammeln von Informationen eine rechtmäßige Handlung von Regierungen, Organisationen und Individuen darstellt, beinhaltet Spionage das Sammeln von sensiblen und/oder vertraulichen Informationen ohne Einverständnis oder Kenntnis des Besitzers.

Was wollen Spione?

Alles, wodurch sie sich einen Vorteil verschaffen können, wie zum Beispiel:

- Politische, wirtschaftliche, kommerzielle, militärische, wissenschaftliche, technische, persönliche Informationen
- Energie und Forschung sind neben den traditionellen Bereichen Verteidigung und Militär ebenfalls lohnende Ziele
- Im Zusammenhang mit der EU suchen sie meist nach Informationen, um die Gestaltung der Politik oder Verhandlungen zu beeinflussen.

Wie gehen sie vor?

- Mit technischen Methoden, indem sie **Ihre Kommunikation (Telefon, soziale Medien usw.) abfangen, Schad-Software benutzen oder Informationen von Ihren elektronischen Geräten stehlen**
- Mit Operationen wie Undercover-Überwachung; Eindringen in Räume, in denen Informationen aufbewahrt werden; oder Ansprechen, Kultivieren und Rekrutieren **menschlicher Quellen**.

Im Anhang finden Sie einige bekannte Beispiele solcher Fälle von Spionage.

WIE WERDEN VERSCHLUSSSACHEN GESCHÜTZT?

Zugangsbedingungen

Bevor der Zugang gewährt wird, muss der Dienst, der den Zugang anbietet, prüfen, ob die betreffende Person befugt ist, ob sie die richtige Sicherheitsermächtigung für den Geheimhaltungsgrad der Verschlusssache mit EU-CONFIDENTIAL oder höher besitzt und ob es sich bei der Person um einen Adressaten der entsprechenden Informationen handelt.

Mitgliedern des Europäischen Parlaments kann der Zugang zu an sie gerichteten Verschlusssachen bis zum Geheimhaltungsgrad EU-CONFIDENTIAL gewährt werden, sofern sie einer gültigen Sicherheitsunterweisung unterzogen wurden und sie eine förmliche Erklärung über die Nicht-Weitergabe der Informationen unterzeichnet haben.

Formal gesehen kann der Zugang zu EUCI im Europäischen Parlament nur per Einsichtnahme gewährt werden. Der Zugang per Abgabe ist nur nach Genehmigung des Urhebers gestattet.

Der Zugang wird unterschiedlich organisiert, je nach Geheimhaltungsgrad der Informationen und je nachdem, von welchem Organ sie weitergegeben werden. In jedem Fall jedoch müssen alle Dokumente vor Gestattung der Einsichtnahme registriert und den Adressaten bekannt gegeben werden.

ZUSAMMENFASSUNG DER ANFORDERUNGEN FÜR DEN ZUGANG ZU EUCI

	Geheimhaltungsgrad	Genehmigung (EP-Sicherheits-ermächtigung)	Sicher-heitsüber-prüfung (Kontrolle)	Sicher-heits-unter-weisung	Kenntnis nur, wenn nötig
MdEP	EU RESTRICTED	nein	nein	ja	ja
	EU CONFIDENTIAL	ja oder förmliche Erklärung	ja oder förmliche Erklärung	ja	ja
	EU SECRET	ja	ja	ja	ja
	EU TOP SECRET	ja	ja	ja	ja
Beamte	EU RESTRICTED	nein	nein	ja	ja
	EU CONFIDENTIAL	ja	ja	ja	ja
	EU SECRET	ja	ja	ja	ja
	EU TOP SECRET	ja	ja	ja	ja

Schutz von Verschlusssachen

Es ist äußerst wichtig, dass Verschlusssachen jederzeit ordnungsgemäß geschützt oder aufbewahrt werden, und zwar in Übereinstimmung mit den Mindestsicherheitsanforderungen für den jeweiligen Geheimhaltungsgrad.

Aus diesem Grund werden alle mit EU CONFIDENTIAL oder höher eingestuften Verschlusssachen nur in sicheren Einrichtungen des Referats Verschlusssachen aufbewahrt.

Bei der Einsichtnahme

Es liegt in der Verantwortung der ermächtigten Personen, jederzeit den Schutz der Verschlusssache sicherzustellen. Bei der Benutzung soll die Verschlusssache ausreichend geschützt werden, um den Verlust oder eine Gefährdung zu verhindern. Zunächst müssen sich alle ermächtigten oder befugten Personen darüber im Klaren sein, dass die Verschlusssache nicht über ungesicherte Telefone, an öffentlichen Orten oder in sonst einer Weise, durch die eine Weitergabe an oder ein Abfangen durch unbefugte Personen ermöglicht würde, besprochen werden darf. Dies schließt auch ein, Verschlusssachen nicht an nicht genehmigten Computern zu bearbeiten. Verschlusssachen sollen niemals ungesichert oder unbewacht gelassen werden. Eine ständige Überwachung durch eine befugte Person, die über direkte Kontrolle über die Verschlusssache verfügt, bietet zusätzliche Sicherheit. Die befugte Person muss über die entsprechende Ermächtigung und Berechtigung zur Kenntnisnahme im Bedarfsfall verfügen und muss einschreiten, um den Zugang zum Material zu verhindern, wenn Personen ohne entsprechende Ermächtigung und Berechtigung zur Kenntnisnahme zugegen sind.

Das Arbeiten mit Verschlusssachen des Geheimhaltungsgrades EU CONFIDENTIAL außerhalb der sicheren Einrichtungen ist UNTERSAGT. Bei der Arbeit mit Verschlusssachen des Geheimhaltungsgrades EU-RESTRICTED auf einem zugelassenen Computer aber in einem ungeschützten Bereich sollten offene Vorhänge und Türen geschlossen werden. Sinnvoll ist auch das Anbringen eines Schildes mit der Aufschrift

„BITTE NICHT STÖREN“. Wenn ein Besucher oder eine nicht ermächtigte Person (einschließlich parlamentarischer Assistenten) zugegen ist, muss eine Verschlusssache geschützt werden, indem sie bedeckt, mit der Oberseite nach unten gelegt oder in einem genehmigten Behälter (Stahlbehälter) aufbewahrt wird.

Verschlusssachen sollten niemals mit nach Hause genommen werden. Generell sind Verschlusssachen nach der Nutzung wieder einzulagern.

Nach der Nutzung
Nach der Nutzung sind die Verschlusssachen wieder in einem genehmigten Behälter zu sichern, sofern sie nicht von einer anderen ordnungsgemäß ermächtigten Person mit Berechtigung zur Kenntnisnahme im Bedarfsfall bewacht werden. Die Aufbewahrung von Verschlusssachen in anderen als den genehmigten Behältnissen ist streng untersagt.

Genehmigte Aufbewahrungsbehälter sollten verschlossen bleiben.

Materialien, die als EU-RESTRICTED eingestuft sind, können von den Besitzern der Informationen in normalen Stahlschränken aufbewahrt werden. Materialien, die als EU-CONFIDENTIAL oder höher eingestuft sind, dürfen nicht außerhalb der gesicherten Einrichtungen des Referats Verschlusssachen aufbewahrt werden.

Reproduktion von Verschlusssachen
Kopien von Verschlusssachen unterliegen denselben Sicherheitskontrollen wie Original-Verschlusssachen. Im Europäischen Parlament dürfen Kopien von Verschlusssachen nur durch einen befugten Dienst zwecks Einsichtnahme bei Sitzungen unter Ausschluss der Öffentlichkeit reproduziert werden; dies gilt nur für Informationen, die als EU-CONFIDENTIAL oder darunter eingestuft sind.

Bei einer Sitzung unter Ausschluss der Öffentlichkeit mit Verschlusssachen mit dem Geheimhaltungsgrad EU-RESTRICTED ist das für die Sitzung zuständige Sekretariat zur strengen Einhaltung der folgenden Regeln verpflichtet:

- Erstellung und Registrierung der notwendigen Anzahl von Kopien,
- Verteilung von lediglich der benötigten Anzahl von Kopien, die der Anzahl der befugten Personen entspricht
- Einsammeln der Kopien am Ende der Sitzung, um eine ordnungsgemäße Aufbewahrung oder Vernichtung sicherzustellen

Bei einer Sitzung unter Ausschluss der Öffentlichkeit mit Informationen der Geheimhaltungsstufe EU CONFIDENTIAL übergibt das Referat Verschlusssachen dem zuständigen Sekretariat die registrierte und exakte Anzahl benötigter Kopien zusammen mit einer Nutzungs- und Empfangsliste dieser Kopien. Das für die Sitzung zuständige Sekretariat muss sicherstellen, dass alle Kopien vollständig sind und nach Ende der Sitzung an das Referat Verschlusssachen zurückgegeben werden.

In jedem Fall werden die Mitglieder des Europäischen Parlaments zu Beginn der Sitzung darauf hingewiesen, dass alle Kopien zurückgegeben werden müssen und den Raum nicht verlassen dürfen.

Das Kopieren von Verschlusssachen mit Büro-Fotokopierern ist verboten, es sei denn (im Fall von EU-RESTRICTED-Dokumenten), die Maschinen sind zertifiziert, vom EP-Netzwerk getrennt, haben keine Festplatte und ordnungsgemäße Kontrollen werden durchgeführt.

Jede andere Reproduktion ist UNTERSAGT, es sei denn, der Urheber erlaubt diese unter bestimmten Voraussetzungen nach Artikel 3.2 des Rahmenabkommens zwischen dem Europäischen Parlament und der Europäischen Kommission oder Artikel 5 (4b) der Interinstitutionelle Vereinbarung vom 12. März 2014 zwischen dem Europäischen Parlament und dem Rat.

BESONDERE HINWEISE UND WARNUNGEN

- ✓ Bitte denken Sie daran, dass nicht jeder über eine Sicherheitsermächtigung oder Zugangsberechtigung zu Informationen des Geheimhaltungsgrades EU RESTRICTED oder die Berechtigung zur Kenntnisnahme im Bedarfsfall verfügt. Treffen Sie die notwendigen Vorkehrungen und vermeiden Sie es, über Verschlusssachen in öffentlichen Bereichen zu sprechen, wo die Gefahr besteht, dass andere mithören können (also in Kantinen, Cafés, Restaurants, Taxis, öffentlichen oder privaten Verkehrsmitteln, Ihrem Hotelzimmer usw.). Gehen Sie nie davon aus, dass ein Telefon nicht abgehört werden könnte.

- ✓ Bei Computern von Regierungen und Institutionen sollte nicht von der Existenz von Privatsphäre ausgegangen werden. Computer, E-Mails und elektronische Daten können jederzeit und ohne Vorwarnung durchsucht und nachverfolgt werden. Es stehen im Europäischen Parlament noch keine Computerterminals für die Bearbeitung von Verschlusssachen zur Verfügung. Verschlusssachen sind derzeit nur als registrierte Hartkopie(n) verfügbar. **Denken Sie nach, bevor Sie damit beginnen, eine E-Mail oder ein Dokument zu verfassen, wenn sie Verschlusssachen verwenden oder wenn die Informationen zu EUCI werden sollen. Erstellen Sie keine Handouts für Verschlusssachen auf einem nicht genehmigten Computer, Laptop oder im INTRANET/Internet.**

- ✓ Die Nutzung elektronischer Geräte (Radios, Mobiltelefone, Kameras, iPods, persönliche Datenassistenten (Blackberrys), Laptops und Pager) ist **im sicheren Leseraum und in allen Räumen, in denen eine Sitzung unter Ausschluss der Öffentlichkeit zur Einsichtnahme in Verschlusssachen stattfindet, VERBOTEN.**

- ✓ Wenn Sie im Besitz von Verschlusssachen sind oder diese zur Einsichtnahme verwenden, **lassen Sie Ihre Kopie niemals unbeaufsichtigt**.

- ✓ Wenn Sie im offiziellen oder privaten Einsatz in Drittstaaten oder auf dem Gelände von nationalen Botschaften sind, sind Sie angehalten, Ihre SIM-Karte aus allen persönlichen oder offiziellen elektronischen Geräten, die Sie bei sich tragen, zu entfernen, um alle persönlichen, privaten und offiziellen Daten zu schützen.

- ✓ Verschlusssachen müssen in Räumen, die für den Umgang mit Verschlusssachen zertifiziert sind, benutzt, aufbewahrt, besprochen und bearbeitet werden. Verschlusssachen im Europäischen Parlament dürfen derzeit nur in Papierform

bearbeitet werden, solange noch kein zertifiziertes Informations- und Kommunikationssystem im Europäischen Parlament entwickelt wurde.

REGELUNGEN FÜR DIE EINSICHTNAHME

Allgemeine Regelungen des EP für die Einsichtnahme in EUCI

Dokumente mit dem Geheimhaltungsgrad EU-RESTRICTED können im sicheren Leseraum eingesehen werden, der vom Referat Verschlusssachen oder dem entsprechenden Sekretariat des Organs/Amtsträgers im Besitz dieser Informationen verwaltet wird. Informationen mit dem Geheimhaltungsgrad EU-CONFIDENTIAL oder höher dürfen nur im sicheren Leseraum des Referats Verschlusssachen (CIU) eingesehen werden.

Das zuständige Sekretariat des parlamentarischen Organs/Amtsträgers oder das CIU (je nach Fall) entscheidet, ob Zugang gewährt werden kann, indem geprüft wird, ob das Mitglied:

- die richtige Stufe der Befugnis oder Ermächtigung für EU-CONFIDENTIAL oder höher besitzt
- sich der verpflichtenden Sicherheitsunterweisung unterzogen hat
- auf der Zugangsliste aufgeführt wird.

Das zuständige Sekretariat erinnert das Mitglied dann an die geltenden Sicherheitsvorschriften und stellt sicher, dass die Person eine „Erklärung“ über die Nicht-Weitergabe der Informationen unterschreibt.

In Artikel 9 (5) des Beschlusses des Präsidiums vom 15. April 2013 wird betont:

> ***„Das zuständige Sekretariat des parlamentarischen Organs bzw. Amtsträgers oder das CIU ist befugt, allen Personen den Zutritt zu einem gesicherten Leseraum zu verwehren, die nicht zugangsberechtigt sind. Einsprüche gegen eine solche Zugangsverwehrung sind im Fall von Mitgliedern des Europäischen Parlaments, die Zugang beantragen, an den Präsidenten und in anderen Fällen an den Generalsekretär zu richten.“***

Modalitäten für individuelle Einsichtnahmen

Anfrage für individuelle Einsichtnahme

Eine Person, die Einsichtnahme in ein Dokument mit dem Geheimhaltungsgrad EU RESTRICTED wünscht, muss im Voraus dem zuständigen Mitglied des Ausschusssekretariats oder dem CIU ihren Namen mitteilen und einen Termin für die Einsichtnahme ausmachen, vorzugsweise per E-Mail. Die zutreffende E-Mail-Adresse wird in der Benachrichtigungs-E-Mail bzw. dem Benachrichtigungsschreiben mitgeteilt. Anfragen

für die Einsichtnahme in Material mit dem Geheimhaltungsgrad EU-CONFIDENTIAL und höher können nur an den CIU gerichtet werden (mailto:CIU@ep.europa.eu).

Alle Daten und Einsichtnahmen werden in einem Logbuch registriert. Alle persönlichen Daten werden unter Beachtung der Verordnung 45/2001 behandelt.

Verhalten während der individuellen Einsichtnahme:

- ✓ Ein befugter Mitarbeiter des zuständigen Dienstes, bei dem das Dokument aufbewahrt wird, ist während der gesamten Dauer der Einsichtnahme anwesend. Bei Ausschüssen trifft dies zu, wenn die Einsichtnahme in einem sicheren Leseraum oder im Büro des Referatsleiters stattfindet.

- ✓ Nur jeweils eine Person kann ermächtigt werden, in die Informationen Einsicht zu nehmen (außer in Ausnahmesituationen und mit Beschränkung auf Informationen mit dem Geheimhaltungsgrad EU-RESTRICTED).

- ✓ Der Kontakt nach außen (einschließlich mittels Telefon oder anderer technischer Geräte) und das Anfertigen von Notizen (außer, wenn dies vom Urheber erlaubt wurde), das Fotokopieren, Fotografieren oder eine andere Reproduktion der eingesehenen vertraulichen Informationen sind unzulässig.

- ✓ Wenn es gerade nicht benutzt wird, wird das Dokument in einem zugelassenen verschlossenen Stahlschrank aufbewahrt.

- ✓ Bevor die Person die Erlaubnis erhält, die sichere Einrichtung zu verlassen, kontrolliert der befugte Mitarbeiter, der während der gesamten Einsichtnahme zugegen ist, ob die vertraulichen Informationen noch vorhanden, unversehrt und vollständig sind.

Allgemeine Modalitäten für den Umgang mit EUCI in Sitzungen unter Ausschluss der Öffentlichkeit

Nur Dokumente mit dem Geheimhaltungsgrad EU-RESTRICTED dürfen bei einer Sitzung unter Ausschluss der Öffentlichkeit eingesehen werden, wobei unter 3.2.2 von Anhang II der Rahmenvereinbarung und Artikel 6(5) der Interinstitutionellen Vereinbarung vom 12. März 2014 festgelegt ist, dass diese Regelung in Ausnahmefällen auf Informationen mit dem Geheimhaltungsgrad EU CONFIDENTIAL erweitert werden kann.

Zu Beginn der Sitzung werden der Status und die Geheimhaltungsstufe des Dokuments durch den Vorsitzenden der Sitzung erklärt. Der Vorsitzende hebt außerdem hervor, dass Notizen, Fotokopien oder Fotografien nicht erlaubt sind, dass keine Dokumente den Raum verlassen darf und dass es am Ende der Sitzung dem Sekretariat zurückgegeben werden muss, mit Unterschrift des Adressaten bei Empfang und bei Abgabe des Dokuments.

Das zuständige Sekretariat hat sicherzustellen, dass nur befugte Personen im Raum zugegen sind, bevor es zur Einsichtnahme oder einem mündlichen Austausch vertraulicher Informationen kommt.

Nur die benötigte Anzahl von Kopien für alle ordnungsgemäß ermächtigten Personen, die an der Sitzung teilnehmen, ist im Raum verfügbar. Sie befinden sich in individuell versiegelten Umschlägen, die nummeriert sind, wenn es sich um Informationen mit dem Geheimhaltungsgrad EU-CONFIDENTIAL handelt. Jede Kopie ist mit einem Wasserzeichen versehen. Die Kopie-Nummer und der Name des Adressaten stehen auf jedem Umschlag.

Das Sekretariat verteilt die nummerierten Umschläge zu Beginn der Sitzung. Die Unterschrift jedes Adressaten im Fall von EU-CONFIDENTIAL-Kopien ist verpflichtend (in der vom CIU ausgegebenen Tabelle). Die Zeit der Übergabe wird ebenfalls in der Tabelle notiert.

Bei der Übergabe der Umschläge an die Adressaten bittet das Sekretariat jeden Adressaten, eine „förmliche Erklärung“ zu unterschreiben. Das Dokument wird nicht übergeben, solange diese Erklärung nicht unterschrieben wurde.

Am Ende der Sitzung geben die Mitglieder ihre Kopien an das zuständige Sekretariat und die zugewiesenen Mitarbeiter zurück, die alle Kopien einsammeln und jeden Adressaten um seine Unterschrift zur Bestätigung der Rückgabe bitten. Der Mitarbeiter überprüft auch, ob das Dokument vollständig ist, und notiert den Zeitpunkt der Abgabe des Dokuments.

Bei Informationen mit dem Geheimhaltungsgrad EU-CONFIDENTIAL gibt das Sekretariat die Dokumente direkt nach der Sitzung an das Referat Verschlusssachen (CIU) zurück, zusammen mit allen unterschriebenen „förmlichen Erklärungen“ und der ausgefüllten Tabelle für Registrierungszwecke.

Wenn Kopien nicht erneut verwendet werden sollen, vernichtet das zuständige Sekretariat sie in einem zugelassenen Schredder. Kopien mit dem Geheimhaltungsgrad EU-RESTRICTED können von dem zuständigen Sekretariat, das die Sitzung organisiert hat, vernichtet werden. Dokumente mit dem Geheimhaltungsgrad EU-CONFIDENTIAL dürfen nur durch das CIU vernichtet werden. Die Vernichtung von Kopien wird im Logbuch festgehalten.

Verhalten bei Sitzungen unter Ausschluss der Öffentlichkeit

- ✓ Es dürfen keine Aufzeichnungen der Dokumente und keine Fotokopien angefertigt werden.

- ✓ Im Sitzungsprotokoll wird nicht auf den Inhalt der Erörterung der betreffenden Informationen Bezug genommen. Nur der diesbezügliche Beschluss, sofern einer gefasst wurde, darf vermerkt werden.

- ✓ In den Sitzungssälen dürfen keine zusätzlichen Dokumentbestände bereitgehalten werden.

- ✓ **Die Teilnehmer dürfen keine Dokumente aus dem Sitzungsraum mitnehmen. Wenn Teilnehmer den Raum während der Einsichtnahme in Verschlusssachen verlassen, müssen sie ihre Kopie zurück in den entsprechenden Umschlag**

stecken und diesen während ihrer Abwesenheit bei den Mitarbeitern des zuständigen Sekretariats lassen.

- ✓ Wenn die Informationen nicht benutzt werden, müssen sie in dem ordnungsgemäß genehmigten und für den Geheimhaltungsgrad der entsprechenden Verschlusssache zugelassenen Tresor/Schließfach eingeschlossen werden.

VERSTÖSSE, VERLUST ODER KENNTNISNAHME DER EUCI DURCH UNBEFUGTE

Ein Verstoß gegen die Sicherheitsbestimmungen entsteht durch eine Handlung oder Unterlassung einer Person, die gegen die Sicherheitsvorschriften eines Organs gerichtet ist. Es kann zwischen unbeabsichtigten und vorsätzlichen Verstößen (oder zwischen Unterlassung und Verübung) unterschieden werden, wobei die relative Schwere Letzterer hervorgehoben werden sollte.

Eine Kenntnisnahme einer Verschlusssache durch Unbefugte liegt vor, wenn diese Verschlusssache gänzlich oder teilweise infolge eines Verstoßes gegen die Sicherheitsvorschriften an unbefugte Personen weitergegeben wurde oder wenn dies vermutet wird.

- Eine Verletzung der Geheimhaltungspflicht durch Mitglieder des Europäischen Parlaments hat die Anwendung entsprechender Strafmaßnahmen gemäß der Geschäftsordnung des Europäischen Parlaments zur Folge.

- Ein Verstoß durch einen Bediensteten des Europäischen Parlaments führt zur Anwendung der Verfahren und Sanktionen, die im Statut der Beamten der Europäischen Union und in den Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union, festgelegt durch die Verordnung (EWG, Euratom, EGKS) Nr. 259/68 („Beamtenstatut“) vorgesehen sind.

- Unbeschadet der anzuwendenden EU-Vorschriften unterliegt die Kenntnisnahme von Verschlusssachen durch unbefugte Personen dem nationalen Strafrecht. Der Präsident und/oder der Generalsekretär veranlasst alle notwendigen Ermittlungen im Falle eines Verstoßes.

Wurden die vertraulichen Informationen dem Europäischen Parlament durch ein Organ der EU oder einen Mitgliedstaat übermittelt, unterrichten der Präsident und/oder der Generalsekretär das Organ der Union oder den betroffenen Mitgliedstaat über einen erwiesenen oder mutmaßlichen Verlust einer Verschlusssache oder eine erwiesene oder mutmaßliche Kenntnisnahme von einer Verschlusssache durch Unbefugte sowie über die Ergebnisse der Untersuchung und die Maßnahmen gegen eine Wiederholung des Vorfalls.

Jede Kenntnisnahme der EUCI durch Unbefugte kann das Bild der Institution beschädigen und dazu führen, dass das Parlament keine Verschlusssachen mehr von Dritten erhalten wird.

EMPFANGSBESTÄTIGUNG

Ich, der/die Unterzeichnete, Herr/Frau _____,
(NAME, Vorname), geboren am _____**(Geburtsdatum)**, bestätige hiermit, dass ich die Mindestgrundsätze und -maßnahmen für die Sicherheit, die in der schriftlichen Sicherheitsunterweisung dargestellt werden, gelesen und zur Kenntnis genommen habe. Ich erkläre außerdem, dass ich über die im Europäischen Parlament anwendbaren Sicherheitsleitlinien unterrichtet wurde, die im Beschluss des Präsidiums des Europäischen Parlaments vom 15. April 2013 über die Regeln zur Behandlung vertraulicher Informationen durch das Europäische Parlament[1] enthalten sind, sowie über die darin beschriebenen Regeln zur Umsetzung (Behandlungsanweisungen[2]).

Hiermit nehme ich zur Kenntnis, dass eine Nichteinhaltung der Sicherheitsleitlinien und Behandlungsanweisungen administrative, disziplinarische und strafrechtliche Folgen haben kann.

Datum und Unterschrift:

……

BITTE MIT UNTERSCHRIFT UND DATUM PERSÖNLICH oder PER HAUSPOST ZURÜCKGEBEN AN:

REFERAT VERSCHLUSSSACHEN
BÜRO DES STELLVERTRETENDEN GENERALSEKRETÄRS
Ansprechpartner:
Daniela CARVALHO
Telefon: (+32.2.28) **43234** oder +32 (0) 473 864 898 (mobil)

Fernando SUAREZ
Telefon: (+32.2.28) **42439**

Standort:
PHS 04C005

[1] Abl. 96 vom 1.4.2014, S. 1-51
[2] Verfügbar unter http://www.intradsg.ep.parl.union.eu/intradsg/cms/welcome/classified_info

Anhang

Chronologie von Spionagefällen in Brüssel in der jüngeren Vergangenheit[1]

2014

Im März 2014 wurde ein Telefongespräch zwischen der Hohen Vertreterin der EU für Außen- und Sicherheitspolitik Catherine Ashton und dem estnischen Außenminister Urmas Paet auf YouTube veröffentlicht. Der Mitschnitt wurde in Brüssel – nicht in Tallinn – gemacht, es ist allerdings unklar, wer hinter der Operation steckt. Die belgische Staatsanwaltschaft hat kein Ermittlungsverfahren eröffnet, da keine offizielle Beschwerde vorlag.

In einer Presseerklärung vom März 2014 gab der frühere belgische Premierminister und Vorsitzende der ALDE-Fraktion im Europäischen Parlament Guy Verhofstadt an, dass sein Treffen mit dem russischen Oppositionsführer Alexei Nawalny abgehört wurde. Verhofstadt und Nawalny hatten sich im Mai 2013 in einem Moskauer Hotel getroffen, um über Fälle von Korruption und Geldwäsche in Russland und ihre Verbindungen zur Europäischen Union zu sprechen. Später wurde Material des privaten Treffens im russischen TV-Sender NTV gezeigt.

2013

Am 21. November 2013 wurden Mails von MdEP gehackt. Ziel der Hacker war es, den Gewinner des Sacharow-Preises herauszufinden.

2012

Ein europäischer Beamter wurde in Belgien zu 40 Monaten Haft verurteilt, weil er über einen französischen Lobbyisten vertrauliche Informationen über die Gemeinsame Agrarpolitik an Unternehmer weitergegeben hat, während er europäischer Beamter war. Der ehemalige Beamte Karel Brus, der mittlerweile die Kommission verlassen hat, wurde nach Angaben der Nachrichtenagentur Belga von einem Brüsseler Strafgericht zu einer Strafzahlung von 55 000 EUR und der Beschlagnahme von fast 140 000 EUR verurteilt.

2011

Eine Gruppe von Hackern mit den beiden Namen Comment und Byzantine Candor hat einige Tage vor dem EU-China-Gipfel E-Mails vom Computer des Präsidenten des Europäischen Rats Herman Van Rompuy gestohlen. Sie haben außerdem E-Mails und Anhänge des Anti-Terror-Koordinators der EU Gilles de Kerchove, von vier von Van Rompuys Beratern und vier anderen EU-Beamten gestohlen, in denen es um die

[1] Quellen:
- VSSE, belgischer Geheim- und Nachrichtendienst;
- EP GD SAFE Dienste
- euobserver.com und
- http://www.targetbrussels.be/

Handelsentwicklung ging. China bestritt eine Beteiligung, als der Hack ein Jahr später öffentlich wurde.

Kurz vor dem regelmäßigen Frühjahrsgipfel der EU gab die Europäische Kommission bekannt, dass sie Opfer einer ausgeklügelten Cyber-Attacke geworden war. Als Gegenmaßnahme wurden die Mitarbeiter der Kommission und des Europäischen Auswärtigen Diensts angewiesen, ihre Arbeits-E-Mails von zuhause aus abzurufen und ihre Passwörter zu ändern.

2010

Laut VSSE waren russische Geheimdienstaktivitäten in Belgien auf die euro-atlantische Verteidigungspolitik, politische Entscheidungen der EU und die EU-Wirtschaftspolitik sowie auf die russischsprachige Gemeinde in Belgien gerichtet.

Der VSSE ermittelte wegen Aktivitäten des kolumbianischen Geheimdiensts, dem Departamento Administrativo de Seguridad (DAS), die gegen „Institutionen und Nichtregierungsorganisation auf belgischem Boden“ gerichtet waren. Der DAS spionierte vermutlich das Europäische Parlament und Mitglieder der Nichtregierungsorganisation Broederlijk Delen und Oxfam Solidariteit aus.

2009

Der elektronische Angriff auf die Korrespondenz von Javier Solana, dem damaligen Hohen Vertreter für die Gemeinsame Außen- und Sicherheitspolitik der EU, konnte nach Südostasien zurückverfolgt werden.

Ein vertrauliches Memorandum von Stephen Hutchins, dem Sicherheitsdirektor der Europäischen Kommission, wurde der deutschen Frankfurter Allgemeinen Zeitung zugespielt. Hutchins warnte davor, dass die Bedrohung durch Spionage täglich zunehme. Viele Staaten, Informationssucher, Lobbyisten, Journalisten, private Agenturen und andere dritte Parteien seien weiterhin auf der Suche nach sensiblen und vertraulichen Informationen.

2008

13 Jahre lang leitete Herman Simm, der frühere Chef des Sicherheitsdienstes des estnischen Verteidigungsministeriums, Informationen an Russland weiter. Am Ende seiner Karriere war Simm Leiter der nationalen Sicherheitsbehörde in Estland. Er hatte auch Zugang zu Top-Secret-Dokumenten, die zwischen NATO-Mitgliedstaaten ausgetauscht wurden. **Simm besaß auch die Sicherheitsermächtigung für EU-Verschlusssachen, da er an Sitzungen der Beratenden Gruppe für das Sicherheitskonzept der Kommission und des Ausschusses des Sicherheitsrats teilnahm, zwei beratenden Ausschüssen der EU zu Sicherheit von Informationen. Die estnische Sicherheitspolizei Kapo sagte gegenüber EUobserver, dass Simm „mindestens“ 3294 estnische Dokumente an Russlands Auslandsgeheimdienst SWR weitergeleitet hat. Darunter waren 386 EU- und NATO-Papiere zu Kommunikationssystemen, Abwehr feindlicher Aufklärung und Verteidigungspolitik, von denen manche mit „CONFIDENTIEL UE“ oder „SECRET UE“ eingestuft waren. Simm wurde wegen Verrats angeklagt und später zu zwölfeinhalb Jahren Gefängnis verurteilt.**

Der VSSE unterrichtete den belgischen Justizminister Jo Vandeurzen über Hackingversuche gegen E-Mail-Accounts der Regierung, die wahrscheinlich aus China kamen; klare Beweise gab es jedoch keine. ***Die Angreifer benutzten „Social Engineering“ - das Herausfinden persönlicher Daten anhand von Informationen aus offen zugänglichen Quellen -, um belgische Beamte, die für Energie und europäische Angelegenheiten zuständig waren, dazu zu bringen, die an sie gesendeten schädlichen E-Mails zu öffnen.***

2003

Durch Störungen im Telefon des Justus-Lipsius-Gebäudes, dem Sitz des Rates der EU in Brüssel, wurde bemerkt, dass fünf schwarze Boxen mit Spionageausrüstung in den Betonwänden des Gebäudes versteckt waren und mit den Telefonleitungen der Delegationsräume von Deutschland, Spanien, Frankreich, Italien, Österreich und dem Vereinigten Königreich verbunden waren.