Öffentlich-rechtlicher Vertrag
(Geheimschutzverfahren)

zwischen der Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und

(Name und Anschrift des Unternehmens sowie die vom BMWK vergebene Betriebsnummer):

wird folgende Vereinbarung geschlossen:

1. (Name des Unternehmens):

   wird für den Fall des erfolgreichen Abschlusses des Prüfungsverfahrens gemäß den Vorschriften des Geheimschutzhandbuches (GHB) mit Ausstellung des Sicherheitsbescheides (Ziff. 2.4.1 GHB) in die Geheimschutzbetreuung durch das Bundesministerium für Wirtschaft und Klimaschutz nach Maßgabe des Sicherheitsüberprüfungsgesetzes (SÜG) und des GHB in der jeweils geltenden Fassung aufgenommen. BMWK macht die jeweils geltende Fassung dem Unternehmen zugänglich.

2. Das Unternehmen erkennt die Bestimmungen des Geheimschutzhandbuchs (GHB) einschließlich der Anlagen in der jeweils geltenden Fassung als rechtsverbindlich an und verpflichtet sich, alle erforderlichen organisatorischen, personellen und materiellen Geheimschutzmaßnahmen nach Maßgabe des GHB zu treffen.
   Dazu gehören insbesondere:
   - die Durchführung der vom Bundesministerium für Wirtschaft und Klimaschutz im Rahmen der Geheimschutzbetreuung verfügten Anordnungen und Maßnahmen,
   - die Beachtung des Grundsatzes „Kenntnis nur, wenn nötig“
     -- Alle Personen, die im Zusammenhang mit einem VS-Auftrag Verschlusssachen (VS) einsehen, bearbeiten, entwickeln oder schützen sollen, müssen entsprechend dem Geheimhaltungsgrad der VS überprüft und ermächtigt sein.
     -- Unbeschadet ihrer individuellen Ermächtigung sind Beschäftigte (eigenes und Fremdpersonal) zur Kenntnisnahme von VS nur berechtigt, wenn und soweit sie zur Ausübung ihrer Tätigkeit im Unternehmen hiervon Kenntnis benötigen.
     -- In regelmäßigen Zeitabständen von längstens fünf Jahren prüft das Unternehmen, ob eine VS noch benötigt wird. Andernfalls ist sie zu vernichten oder dem VS-Auftraggeber zurückzugeben.
   - die Bestellung eines/einer fachlich und persönlich geeigneten Sicherheitsbevollmächtigten als zentrales Sicherheitsorgan des Unternehmens sowie eines/einer ständige/n Vertreter/in vor Ort nach Zustimmung durch das Bundesministerium für Wirtschaft und Klimaschutz. Der/die Sicherheitsbevollmächtigte ist dem/der Vorsitzenden der Geschäftsleitung, wo

dies nicht möglich ist, dem nach der Geschäftsordnung zuständigen Mitglied der Geschäftsleitung in organisatorisch eindeutiger Weise unmittelbar zu unterstellen. Er/sie hat insoweit eine leitende Funktion und direktes Vortragsrecht in allen Geheimschutzangelegenheiten. Der/die Sicherheitsbevollmächtigte ist vom Unternehmen mit den notwendigen Befugnissen und allen erforderlichen personellen und materiellen Mitteln auszustatten und bei allen geheimschutzrelevanten Maßnahmen zu beteiligen und zu unterstützen. Er/sie ist an allen VS-relevanten Entscheidungen des Unternehmens zu beteiligen und im Vorfeld, beispielsweile über eine anstehende Änderung der Gesellschafterverhältnisse, zu informieren.
Ihm/ihr dürfen keine Aufgaben übertragen werden, die die Erfüllung seiner/ihrer vorrangigen sicherheitsrelevanten Aufgaben als Sicherheitsbevollmächtigte/r beeinträchtigen können. Er/sie darf wegen der Erfüllung der ihm/ihr übertragenen Aufgaben nicht benachteiligt werden.

3. Das Unternehmen wird mit jedem öffentlichen oder nichtöffentlichen VS-Auftraggeber und mit jedem eventuellen VS-Unterauftragnehmer eine Geheimschutzklausel als Bestandteil jedes Vertrages über geheimhaltungsbedürftige Lieferungen und Leistungen vereinbaren.

4. Das Unternehmen wird dem Bundesministerium für Wirtschaft und Klimaschutz jede Änderung der gemäß GHB relevanten Unternehmensangaben unverzüglich mitteilen. Bei der Beantragung des Insolvenzverfahrens wird das Unternehmen dem Bundesministerium für Wirtschaft und Klimaschutz unverzüglich den Insolvenzverwalter benennen und diesen über die Existenz von VS-Aufträgen sowie Rechte und Verpflichtungen aus dem Geheimschutzverfahren unterrichten.

Bonn, den , den

Für
die Bundesrepublik Deutschland,
vertreten durch das Bundesministerium
für Wirtschaft und Klimaschutz

Für
das Unternehmen

....
Name (Unterschrift) (Unterschrift der Geschäftsleitung)
Name in Druckbuchstaben wiederholen

Geheimschutzklausel

1. Der VS-Auftraggeber benennt dem VS-Auftragnehmer in einem Vertrag oder einem gesonderten Anhang alle Teile des VS-Auftrages, die auf amtliche Veranlassung geheim zu halten sind (VS-Einstufungsliste), und bestimmt die Dauer der Geheimhaltung. Diese Liste wird in ihrer jeweiligen Fassung Vertragsbestandteil. Unterschiedliche Auffassungen in der VS-Einstufung sind unverzüglich zwischen den Vertragspartnern auszuräumen. Bis zur endgültigen Klärung ist die VS-Einstufung des VS-Auftraggebers maßgebend.
2. Der VS-Auftragnehmer verpflichtet sich,

   a) im Rahmen der amtlich veranlassten Geheimhaltung alle nach Maßgabe des GHB notwendigen personellen und materiellen Geheimschutzmaßnahmen zu treffen.

   b) ergänzenden Forderungen des VS-Auftraggebers und des BMWK nachzukommen;

   c) Vertretern des BMWK und den durch ihn hinzugezogenen Behörden Besuche und Unternehmensbegehungen zu gestatten, um die Durchführung und die Wirksamkeit der amtlich veranlassten Geheimschutzmaßnahmen prüfen zu können;

   d) die VS-Unteraufträge, zu deren Durchführung gehe imhaltungsbedürftige Teile des VS-Auftrages an einen VS-Unterauftragnehmer weitergegeben werden sollen, dem VS-Auftraggeber zur Einwilligung vorzulegen, sofern diese nicht schon in allgemeiner Form vorliegt. In diese VS-Unteraufträge ist eine dieser Klausel entsprechende Vereinbarung aufzunehmen;

   e) nach Beendigung der VS-Arbeiten die vom VS-Auftraggeber erhaltenen und die während der Durchführung des VS-Auftrages bei ihm entstandene VS zu vernichten oder an den VS-Auftraggeber zurückzugeben. Hat der VS-Auftragnehmer am Ergebnis seiner Arbeiten Eigentümer- oder Urheberrechte, und kommt deshalb die Vernichtung oder Rückgabe dieser VS nicht in Betracht, hat er die Entscheidung des VS-Auftraggebers darüber herbeizuführen, in welchem Umfang und bis zu welchem Termin die bei ihm verbleibenden VS weiterhin geheimhaltungsbedürftig sind. Wird bei Forschungs- und Entwicklungsarbeiten ohne Zusammenhang mit einem VS-Auftrag auf VS aus früheren VS-Aufträgen zurückgegriffen, ist die Einwilligung des VS-Herausgebers, auf dessen Veranlassung die VS entstanden sind, einzuholen.

3. Die Übernahme der Kosten für erforderliche Geheimschutzmaßnahmen sind zwischen den Vertragsparteien zu regeln.

4. Hinsichtlich der VS-ermächtigten Unternehmensangehörigen entfällt - soweit es sich um die Pflicht zur Geheimhaltung aus Gründen der Staatssicherheit handelt - die Haftung des VS-Auftragnehmers nach §§ 280, 278 BGB. Die Haftung für eigenes Verschulden (§ 276 BGB) bleibt unberührt. Das gilt entsprechend für die Haftung des VS-Auftragnehmers hinsichtlich der Einschaltung von Zulieferern, soweit diese zulässig ist.

5. Die anwendbaren Bestimmungen des Bundesdatenschutzgesetzes sind zu beachten.

Leitfaden
für die Erstellung einer unternehmensinternen Anweisungen
für VS-Zwischenmaterial VS-VERTRAULICH oder höher

1. Allgemeines

Unternehmensinterne Anweisungen für VS-Zwischenmaterial müssen auf der Grundlage dieser Rahmenvorschrift erstellt werden und einen entsprechenden Hinweis enthalten. Sie sind dem Bundesministerium für Wirtschaft und Energie zur Einwilligung vorzulegen. Diese Rahmenvorschrift soll nur als Anhaltspunkt für die Erarbeitung eigener unternehmensinterner Anweisungen dienen. Wichtig ist, dass die unternehmensinternen Anweisungen den örtlichen Gegebenheiten des Unternehmens Rechnung tragen. Wenn im Unternehmen z.B. bestimmte Arten von VS-Zwischenmaterial gar nicht anfallen können, dann braucht dieser Tatbestand in der unternehmensinternen Anweisung auch nicht erwähnt zu werden. Wahrzunehmende Aufgaben sind nicht allgemein aufzuzählen, sondern bestimmten Personen oder Organisationseinheiten zuzuweisen.
Die unternehmensinterne Anweisung gilt grundsätzlich für das gesamte Unternehmen. Es ist jedoch zulässig, für einzelne Teile des Unternehmens gesonderte Anweisungen zu erstellen, in denen der Geltungsbereich dann anzugeben ist.

2. Definition des Begriffs VS-Zwischenmaterial

Vor- oder Teilinformationen (z.B. Vorentwürfe, Stenogramme, Tonträger, Schablonen, Folien, Fehldrucke, Ausdrucke der Datenverarbeitung), die ganz oder teilweise in eine VS einfließen und bereits auf amtliche Veranlassung zu schützende Informationen enthalten, sind VS-Zwischenmaterial.

3. Behandlung von VS-Zwischenmaterial

VS-Zwischenmaterial ist so zu behandeln und zu schützen wie die später daraus entstehende VS. Maßgebend ist in jedem Fall die VS-Einstufungsliste des amtlichen VS-Auftraggebers.

- Für VS-Zwischenmaterial, das unverzüglich (z.B. am Ende eines Arbeitstages) vernichtet oder der VS-Registratur zur Vernichtung übergeben wird, braucht eine Kennzeichnung und ein Nachweis nicht zu erfolgen.
- VS-Zwischenmaterial das nicht unverzüglich vernichtet wird, ist mit dem entsprechenden Geheimhaltungsgrad und dem Zusatz „VS-Zwischenmaterial“ zu kennzeichnen. Die Kennzeichnung kann handschriftlich erfolgen.
- Wenn eine Kennzeichnung auf der VS nicht möglich oder unzweckmäßig ist, kann die Kennzeichnung des VS-Zwischenmaterials auch in der Weise erfolgen, dass lediglich die Aufbewahrungsmappen/-behältnisse entsprechend gekennzeichnet werden.
  Dieses Verfahren kann immer dann zweckmäßig sein, wenn im Rahmen der Bearbeitung einzelne Seiten, Berechnungen, Skizzen usw. länger benötigt bzw. häufiger ausgetauscht werden müssen. Alle ausgetauschten Seiten sind ordnungsgemäß zu vernichten.
  Diese Kennzeichnung ist ausreichend, solange sich das VS-Zwischenmaterial im persönlichen Gewahrsam des Bearbeiters oder einer begrenzbaren Bearbeitergruppe befindet.

4. Weitergabe und Registrierung von VS-Zwischenmaterial

4.1 Weitergabe innerhalb desselben örtlichen Bereichs von Hand zu Hand

Wenn VS-Zwischenmaterial von Hand zu Hand an eine/n andere/n Bearbeiter/in oder an eine andere begrenzbare Bearbeitergruppe innerhalb desselben örtlichen Bereichs weitergegeben werden muss (d.h. es sich nicht mehr im persönlichen Gewahrsam/VS-Verwahrgelass des/der Bearbeiters/in der VS befindet), ist es in ein VS-Quittungsbuch für VS-Zwischenmaterial (Anlage 52) einzutragen. Der Empfänger des VS-Zwischenmaterials hat den Erhalt im VS-Quittungsbuch zu bestätigen.

4.2 Weitergabe an andere Stellen außerhalb desselben örtlichen Bereichs

Bei der Weitergabe von VS-Zwischenmaterial an andere Stellen außerhalb desselben örtlichen Bereichs ist die zentrale VS-Registratur einzuschalten, damit eine ordnungsgemäße Kennzeichnung und Registrierung des VS-Zwischenmaterials gewährleistet ist. In diesem Fall entfallen die Erleichterungen für VS-Zwischenmaterial und es gelten die allgemeinen Regeln für die Behandlung von VS.

4.3 Registrierung des VS-Zwischenmaterials nach Erstellung des Originals

Wenn nach der Erstellung der endgültigen VS (des sog. Originals) nicht das gesamte vorher entstandene VS-Zwischenmaterial vernichtet werden kann (z.B. noch benötigte Druckvorlagen, Bänder), ist dies im VS-Bestandsverzeichnis unter der VS-Tgb.-Nr. des sog. Originals nachzuweisen. Dieses VS-Zwischenmaterial ist mit dieser Tagebuchnummer zu versehen.

5. Vernichtung von VS-Zwischenmaterial

(1) In VS-Bestandsverzeichnissen nachgewiesenes VS-Zwischenmaterial darf nur durch den zuständigen VS-Verwalter/in oder die VS-Registratur vernichtet werden. Im „VS-Quittungsbuch“ für VS-Zwischenmaterial ist ein entsprechender Vermerk/Hinweis auf die Vernichtung einzutragen.

STRENG GEHEIM eingestuftes VS-Zwischenmaterial, das in VS-Bestandsverzeichnissen nicht nachgewiesen ist, ist durch den/die zuständige/n VS-Verwalter/in unter Aufsicht des/der Verfassers/in zu vernichten. GEHEIM oder VS-VERTRAULICH eingestuftes VS-Zwischenmaterial, das nicht in VS-Bestandsverzeichnissen nachgewiesen ist, ist grundsätzlich der zuständigen VS-Registratur zur Vernichtung zu übergeben.

(2) Bei VS-Zwischenmaterial, das auch nach der Erstellung des Originals aufbewahrt werden muss, ist gem. Nr. 4.3 zu verfahren.

6. Aufbewahrung von VS-Zwischenmaterial

VS-Zwischenmaterial, das nicht in der VS-Registratur aufbewahrt wird, ist am Arbeitsplatz des Bearbeiters oder der begrenzbaren Bearbeitergruppe in einem zugelassenen und ordnungsgemäß personell oder technisch überwachten VS-Verwahrgelass aufzubewahren. Die Vorschriften für die vorübergehende Aufbewahrung von VS sind sinngemäß anzuwenden.

7. Aufbewahrung und Vernichtung von VS-Zwischenmaterial mit dem Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH

Die Aufbewahrung und Vernichtung von VS-Zwischenmaterial mit dem Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (1.7) ist in einer „Unternehmensinternen Anweisung über die Behandlung von VS mit dem Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH“ zu regeln.

8. Kontrollen des Sicherheitsbevollmächtigten

Der/die SiBe oder ein/e von ihm beauftragte/r Mitarbeiter/in (z.B. der/die zuständige VS-Verwalter/in) führt nachweisbar in unregelmäßigen Zeitabständen Kontrollen am Arbeitsplatz der Bearbeiter/innen von VS durch, um die Einhaltung dieser Vorschriften zu gewährleisten.

Bundesministerium
für Wirtschaft
und Klimaschutz

Merkblatt für die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)

Inhalt

Stand: 07/2023

Über dieses Merkblatt - Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH: Rechte und Pflichten von öffentlichem VS-NfD-Auftraggeber und Unternehmen

1 VS-NfD-Auftrag

Vor der Weitergabe von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) an nichtöffentliche Stellen (Unternehmen[1]) muss mit diesen jeweils ein Vertrag geschlossen werden, in den die Bestimmungen dieses VS-NfD-Merkblatts (Anlage 4 zum Geheimschutzhandbuch - GHB) Eingang gefunden haben. Die konkreten geheimschutzrechtlichen Anforderungen eines VS-NfD-Auftrags sind zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer zu klären. Dazu gehört auch die Einbeziehung von VS-NfD-Unterauftragnehmern (s. Ziff. 3.2)

2 VS-NfD-Auftraggeber und VS-NfD-Herausgeber

VS-NfD-Auftraggeber im Sinne dieses Merkblatts sind öffentliche Stellen oder Unternehmen, die Unternehmen (VS-NfD-Auftragnehmer) Zugang oder Zugangsmöglichkeit zu VS-NfD ermöglichen müssen[2]. Bei Unternehmen erfolgt dies in Form eines VS-NfD-Unterauftrags.
Die Bundesbehörden und bundesunmittelbaren öffentlich-rechtlichen Einrichtungen (Dienststellen), die eine VS-NfD erstellen oder deren Erstellung veranlassen, oder der Rechtsnachfolger dieser Dienststelle, sind VS-NfD-Herausgeber.

3 Rechte und Pflichten des VS-NfD-Auftraggebers

3.1 Öffentlicher VS-NfD-Auftraggeber

Bei Weitergabe von VS-NfD an Unternehmen muss der öffentliche VS-NfD-Auftraggeber mit dem Unternehmen einen Vertrag schließen, in den die Bestimmungen dieses Merkblatts Eingang gefunden haben (gemäß Ziff. 6.6 Abs. 2 Anlage V der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz - Verschlusssachenanweisung – VSA). Die hierin enthaltenen Kontrollrechte werden grundsätzlich vom öffentlichen VS-NfD-Auftraggeber ausgeübt. Weitergehende Maßnahmen, wie ein Geheimschutzverfahren des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) oder Sicherheitsüberprüfungen, sind für eine Weitergabe von VS-NfD nicht erforderlich.

3.2 Nicht-öffentlicher VS-NfD-Auftraggeber

Verschafft der VS-NfD-Auftragnehmer anderen Unternehmen (VS-NfD-(Unter-) Auftragnehmern) Zugang oder Zugangsmöglichkeit zu VS-NfD, hat er den VS-NfD-Unterauftragnehmer auf dieses Merkblatt zu verpflichten. Er nimmt in diesem Verhältnis die Rolle des VS-NfD-Auftraggebers ein und die entsprechenden Kontrollrechte werden dann von ihm ausgeübt.

[1] Der Begriff „nicht-öffentliche Stelle“ im Sicherheitsüberprüfungsgesetz (SÜG) umfasst vor allem Unternehmen der Wirtschaft und privatrechtlich verfasste Institutionen. Er wurde als gebräuchlicher Terminus aus dem BDSG übernommen. Im GHB und in diesem Merkblatt wird im Folgenden der Begriff „Unternehmen“ verwendet.
[2] Ein „VS-Auftrag“ liegt erst ab VS des Geheimhaltungsgrades VS-VERTRAULICH vor.

4 Pflichten des VS-NfD-Auftragnehmers

4.1 Allgemein

Der VS-NfD-Auftragnehmer verpflichtet sich, die Vorgaben sämtlicher Teile dieses Merkblatts einzuhalten. Auf mögliche strafrechtliche und vertragliche Konsequenzen bei Zuwiderhandlung wird ausdrücklich hingewiesen.

4.2 Nachweisliche Belehrung und Verpflichtung

Bevor eine Person Zugang oder Zugangsmöglichkeit zu VS-NfD erhält, ist sie vom Unternehmen über Teil 2 dieses Merkblattes zu belehren und auf dessen Einhaltung zu verpflichten. Dabei ist ihr ein Exemplar von den Teilen 2 und 4 dieses Merkblattes zugänglich zu machen. Wenn die Person Zugang oder Zugangsmöglichkeit zu VS-NfD auf Informationstechnik (IT) erhält, gilt gleiches zusätzlich für Teil 3 dieses Merkblattes. Die Belehrung, die Verpflichtung und der Empfang der erforderlichen Teile des Merkblatts sind durch Unterzeichnung des „Nachweises über die Verpflichtung“ (VS-NfD-Merkblatt Teil 5) durch die Person nachzuweisen. Der Nachweis muss vom VS-NfD-Auftragnehmer aufbewahrt werden und ist auf Nachfrage dem VS-NfD-Auftraggeber vorzulegen. Der Nachweis muss spätestens fünf Jahre nach dem Ausscheiden der betroffenen Person aus der Tätigkeit mit Bezug zu VS-NfD vernichtet werden.

4.3 Kontrollmöglichkeiten

Der VS-NfD-Auftraggeber berät den VS-NfD-Auftragnehmer über die Vorgaben dieses Merkblatts und kann sich über deren Einhaltung vergewissern.

4.4 Benennung einer für VS des Geheimhaltungsgrades VS-NfD verantwortlichen Person

Der VS-NfD-Auftragnehmer benennt eine für die Einhaltung und Durchführung der erforderlichen Maßnahmen zum Schutz von VS-NfD verantwortliche Person sowie ggf. eine/n Vertreter/in unter Nutzung des Teils 1b) dieses Merkblattes.
Der VS-NfD-Auftraggeber und der VS-NfD-Auftragnehmer erhalten jeweils eine Ausfertigung des unterschriebenen Teils 1b) des NfD-Merkblattes.

5 Übergangsfrist

Dieses Merkblatt (Teil 1a), Teil 1b), Teil 2, Teil 3, Teil 4, Teil 5, Teil 6) tritt zum 01.09.2023 in Kraft. Die Selbstakkreditierung gem. Teil 3 dieses Merkblattes ist bis zum 01.09.2025 durchzuführen.

Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer

1. Der VS-NfD-Auftragnehmer verpflichtet sich, das VS-NfD-Merkblatt (Anlage 4 zum GHB) einzuhalten.

2. Der VS-NfD-Auftragnehmer benennt in Übereinstimmung mit datenschutzrechtlichen Vorschriften eine für die Einhaltung und Durchführung der erforderlichen Maßnahmen zum Schutz der Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) verantwortliche Person sowie ggf. ein/e Vertreter/in.

   Verantwortliche Person (geschäftliche Daten):

   ☐ Herr ☐ Frau Name, Vorname:

   Telefon-Nr. Mobilfunk-Nr.

   E-Mail-Adresse Anschrift

   Ggf. Vertreter/in der verantwortlichen Person (geschäftliche Daten):

   ☐ Herr ☐ Frau Name, Vorname:

   Telefon-Nr. Mobilfunk-Nr.

   E-Mail-Adresse Anschrift

3. Die Person ist im Auftrag des VS-NfD-Auftragnehmers dabei unter anderem für folgende Maßnahmen verantwortlich:

- Nachweisliche Belehrung und Verpflichtung der Mitarbeiter/innen des VS-NfD-Auftragnehmers, die Zugang oder Zugangsmöglichkeit zu VS-NfD erhalten, über bzw. auf VS-NfD-Merkblatt Teil 2, Teil 3 (sofern anwendbar) und Teil 4;
- Umsetzung der Vorgaben von Teil 3 dieses Merkblattes bei Verarbeitung von VS-NfD auf IT;
- Einholung der schriftlichen Einwilligung des VS-NfD-Auftraggebers zur Weitergabe von VS-NfD;
- Kontrolle der Einhaltung der erforderlichen Maßnahmen zum Schutz von VS-NfD im Unternehmen, ggf. auch bei VS-NfD-Unterauftragnehmern.

Ort, Datum

.....	.....
Unterschrift VS-NfD-Auftraggeber Dienststelle/Unternehmen:	Unterschrift VS-NfD-Auftragnehmer Unternehmen:

Allgemeine Hinweise zum Umgang mit Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

1 Allgemeines

1.1 Anwendbarkeit

Die Regelungen dieses VS-NfD-Merkblattes gelten für deutsche VS-NfD sowie für ausländische vergleichbar eingestufte VS, die einem Unternehmen in Deutschland zur Aufbewahrung oder Verarbeitung überlassen worden sind. Gleiches gilt für bilaterale Geheimschutzabkommen, soweit dort nichts anderes geregelt ist.
Die Regelungen dieses VS-NfD-Merkblattes gelten nicht für VS über- oder zwischenstaatlicher Einrichtungen und Stellen (wie z. B. NATO, EU, ESA, OCCAR) mit vergleichbarem Geheimhaltungsgrad. Beim Schutz solcher VS sind die jeweiligen Vorschriften dieser Einrichtungen/Stellen zu beachten.

1.2 Kenntnis nur, wenn nötig

Von einer VS-NfD dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung Kenntnis haben müssen. Keine Person darf über eine VS-NfD umfassender oder eher unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“.

1.3 Verstöße gegen die Geheimhaltungspflicht

Personen, die gegen die Vorschriften dieses VS-NfD-Merkblatts verstoßen, drohen Konsequenzen und eine strafrechtliche Ahndung des Verstoßes nach den §§ 93 bis 99, 203 Absatz 2 und 353b StGB.
Personen, die sich für den Umgang mit VS als ungeeignet erwiesen haben oder deren Geeignetheit nicht bewertet werden kann, werden von der für VS-NfD verantwortlichen Person von der Verarbeitung von VS-NfD ausgeschlossen.

1.4 Mitteilungspflichten bei Verlust von VS-NfD und Verstößen gegen Vorschriften dieses VS-NfD-Merkblatts

Der Verlust von VS-NfD sowie vermutete und festgestellte Verstöße gegen die Vorschriften dieses VS-NfD-Merkblatts sind unverzüglich der für VS-NfD verantwortlichen Person mitzuteilen. Diese informiert unverzüglich den VS-NfD-Auftraggeber. Mitteilungspflichten geheimschutzbetreuter Unternehmen nach GHB bleiben unberührt. Die erforderlichen Maßnahmen, um Schaden abzuwenden oder zu verringern und Wiederholungen zu vermeiden, werden unverzüglich getroffen. Die für VS-NfD verantwortliche Person bemüht sich um die Aufklärung des Sachverhalts.

1.5 VS-NfD auf IT

Bei Nutzung von IT beim Umgang mit VS-NfD ist zusätzlich Teil 3 dieses Merkblattes einzuhalten. Für die bearbeitenden Personen sind dort insbesondere die Vorgaben zur Verarbeitung in Ziff. 3 relevant.

2 Einstufung

Die Bundesbehörden und bundesunmittelbaren öffentlich-rechtlichen Einrichtungen (Dienststellen), die eine VS-NfD erstellen oder deren Erstellung veranlassen, oder der Rechtsnachfolger dieser Dienststelle, sind VS-NfD-Herausgeber.
Der VS-NfD-Herausgeber stuft eine VS in den Geheimhaltungsgrad VS-NfD ein, wenn deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann (§ 4 Absatz 2 Nummer 4 SÜG). Von einer Einstufung als VS-NfD ist nur Gebrauch zu machen, soweit dies notwendig ist.
Der VS-NfD-Herausgeber bestimmt, welche Informationen geheimhaltungsbedürftig sind. Das Unternehmen kann eine Einstufung nur auf Veranlassung des VS-NfD-Herausgebers vornehmen. Es ist stets nur deren Ersteller und nie selbst VS-NfD-Herausgeber. Das Unternehmen hat die erforderliche VS-NfD-Einstufung bei sich zu gewährleisten.

3 Befristung und Aufhebung der Einstufung

Die Einstufung einer VS-NfD ist auf 30 Jahre befristet. Der VS-NfD-Herausgeber kann, unter Berücksichtigung der Begründung für die Einstufung, eine kürzere Frist bestimmen. Die Einstufung endet mit Ablauf des Jahres, in welches das Fristende fällt. Die Frist kann nicht verlängert werden.
Entfällt die Geheimhaltungsbedürftigkeit einer VS-NfD, hat der VS-NfD-Herausgeber die Einstufung aufzuheben bzw. die Umsetzung durch das Unternehmen zu veranlassen. Die Aufhebung der Einstufung ist so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind.

4 Kennzeichnung

Bei der Erstellung ist eine VS-NfD so zu kennzeichnen, dass bei ihrer Handhabung während der gesamten Dauer ihrer Einstufung jederzeit der Geheimhaltungsgrad, das erstellende Unternehmen, der VS-NfD-Herausgeber, das Datum der Einstufung sowie das vom Herausgeber festgelegte Ende der Einstufung (falls die Regelfrist von 30 Jahren unterschritten wird) erkennbar sind.
Die verbindliche Gestaltung der Kennzeichnung von VS-NfD ist dem Teil 4 dieses Merkblattes zu entnehmen.
Lässt die Beschaffenheit einer VS-NfD eine solche Kennzeichnung nicht zu, ist sinngemäß zu verfahren. Geheimhaltungsgrade sind grundsätzlich auszuschreiben soweit die Beschaffenheit einer VS dies zulässt. Ist dies nicht möglich, wird der Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH mit VS-NfD abgekürzt.
Im Falle nichtdeutscher VS eines entsprechenden Geheimhaltungsgrades sind diese zusätzlich mit dem deutschen Geheimhaltungsgrad zu kennzeichnen, sofern dies in den anwendbaren Geheimschutzabkommen vorgesehen ist.

5 Aufbewahrung

VS-NfD sind bei Nichtgebrauch in verschlossenen Behältern oder Räumen zum Schutz vor Kenntnisnahme durch Unbefugte (Grundsatz: „Kenntnis nur, wenn nötig“) aufzubewahren. Außerhalb von solchen Räumen oder Behältern sind sie auch dort so zu behandeln, dass eine Kenntnisnahme durch Unbefugte ausgeschlossen ist. Können VS-NfD nach der Aufgabendurchführung nicht vernichtet oder vollständig zurückgegeben werden, sind diese bis zur Aufhebung der Einstufung gemäß den Vorgaben dieses Merkblatts zu verwahren.
VS-NfD-Zwischenmaterial (z. B. Vorentwürfe) ist in derselben Weise zu schützen wie das Bezugsdokument.

6 Weitergabe

Weitergabe ist eine Übergabe oder Bereitstellung, durch die eine andere Person Zugang zu VS-NfD hat oder ihn sich verschaffen kann.

6.1 Erforderlichkeit

Vor jeder Weitergabe ist zu prüfen, ob diese unter Berücksichtigung des Grundsatzes „Kenntnis nur, wenn nötig“ zur Aufgabenerfüllung tatsächlich erforderlich ist.

6.2 Weitergabe innerhalb eines Unternehmens

VS-NfD können innerhalb eines Unternehmens offen weitergegeben werden, wobei auch hier gilt, dass eine Kenntnisnahme von Unbefugten ausgeschlossen sein muss. Eine Quittierung der Weitergabe ist nicht vorgesehen.

6.3 Weitergabe an Dritte (öffentliche Stellen oder Unternehmen)

Durch eine Weitergabe an einen Dritten hat dieser Zugang zur VS-NfD oder kann ihn sich verschaffen. Eine Weitergabe kann auch erforderlich sein, wenn ein Dritter sich gelegentlich einer Tätigkeit (z. B. Wartung, Reparatur), die für die Aufgabenerfüllung erforderlich ist, Zugang verschaffen kann. In diesem Fall sind Maßnahmen zu ergreifen, die einen Zugang zu der Verschlusssache verhindern (z. B. Technische Maßnahmen, Abdecken, Begleiten). Die Weitergabe von VS-NfD an Dritte ist nur zulässig, wenn vor der Weitergabe die Einwilligung des VS-NfD-Herausgebers nachweislich vorliegt. Der VS-NfD-Herausgeber kann im Einzelfall einwilligen, aber auch vorab bestimmten oder sämtlichen Weitergaben von VS-NfD im Rahmen eines oder mehrerer VS-NfD-Aufträge und VS-NfD-Unteraufträge innerhalb eines bestimmten Programms einwilligen. Die Einwilligung kann auch für Tätigkeiten erfolgen, bei denen sich ein Dritter gelegentlich der Ausführung eines Auftrages Zugang zu VS-NfD verschaffen kann. Diese Einwilligung ist über den VS-NfD-Auftraggeber einzuholen. Unternehmen dürfen sich auf eine schriftliche Erklärung des jeweiligen VS-NfD-Auftraggebers, dass eine solche Einwilligung des VS-NfD-Herausgebers vorliegt, verlassen. Sie bewahren die Erklärung als Nachweis auf.

6.4 Weitergabe an nichtdeutsche öffentliche Stellen und Unternehmen mit Sitz im Ausland

Auch eine Weitergabe an nichtdeutsche öffentliche Stellen (ausländische öffentliche Stellen oder über- oder zwischenstaatliche Einrichtungen und Stellen) und Unternehmen[1] mit Sitz im Ausland ist mit Zustimmung des VS-Herausgebers möglich. Dabei sind über die vorstehend angeführten Aspekte hinaus zusätzliche Anforderungen zu beachten:
Die Weitergabe von deutschen VS-NfD an nichtdeutsche öffentliche Stellen setzt grundsätzlich ein bilaterales Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen (Geheimschutzabkommen) voraus, welches die Bedingungen für die Weitergabe und weitere Handhabung regelt.
Die Weitergabe von VS-NfD an Unternehmen mit Sitz im Ausland erfolgt auf der Grundlage vertraglicher Vereinbarungen und grundsätzlich unter der Voraussetzung, dass in einem Geheimschutzabkommen mit dem Empfängerland der Schutz deutscher VS-NfD vereinbart worden ist.[2] Auf das Geheimschutzabkommen ist in der vertraglichen Vereinbarung zu verweisen.
Liegt kein bilaterales Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen vor, legt der VS-Herausgeber entsprechend der

[1] s. Teil 1a), Ziff. 1.
[2] Ob mit dem jeweiligen Empfängerland ein Geheimschutzabkommen besteht und ob darin eine Vergleichbarkeit mit VS-NfD vereinbart wurde, ist beim BMWK zu erfragen.

VSA im Einzelfall die Modalitäten der Weitergabe an nichtdeutsche öffentliche Stellen oder Unternehmen mit Sitz im Ausland im Benehmen mit BMWK fest.

6.5 Weitergabe durch private Zustelldienste

VS des Geheimhaltungsgrades VS-NfD können durch private Zustelldienste als gewöhnliche Brief- beziehungsweise Paketsendungen versandt werden. Der Umschlag beziehungsweise das Paket erhält keine VS-Kennzeichnung.

Auch grenzüberschreitend können VS-NfD durch private Zustelldienste wie oben beschrieben weitergegeben werden, es sei denn, das spezifische bilaterale Geheimschutzabkommen lässt die Weitergabe auf diesem Weg nicht zu oder der VS-NfD-Auftraggeber oder der VS-NfD-Herausgeber hat einer solchen Weitergabe widersprochen.

7 Mitnahme und mobiles Arbeiten

VS-NfD können außerhalb von Unternehmen nur auf Geschäftsreisen und zu Besprechungen mitgenommen werden, soweit dies zur Aufgabenerfüllung notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme und unbefugten Zugriff gesichert werden. VS-NfD, u.a. Schriftstücke, können in diesem Fall in einem verschlossenen Umschlag unversiegelt mitgeführt werden.
Ihre Mitnahme zur Verarbeitung in der Privatwohnung ist grundsätzlich unzulässig. Die ausschließliche elektronische Verarbeitung von VS-NfD ist unter den Voraussetzungen von Teil 3, Ziff. 3.5 auch in der Privatwohnung zulässig. Der öffentliche VS-NfD-Auftraggeber kann weitere Ausnahmen zulassen. VS-NfD-Unterauftragnehmer dürfen sich auf eine schriftliche Erklärung ihres VS-NfD-Auftraggebers, dass eine solche Ausnahme zugelassen wurde, verlassen. Sie bewahren die Erklärung als Nachweis auf.
Zusätzlich zu der Ausnahmegenehmigung sind folgende Punkte einzuhalten:

- die Privatwohnung befindet sich innerhalb Deutschlands,
- die für VS-NfD verantwortliche Person erteilt die Zustimmung,
- der/die Mitarbeiter/in ist über spezifische Risiken des mobilen Arbeitens belehrt,
- Teil 6 dieses Merkblattes wurde von dem/der Mitarbeiter/in unterzeichnet und wird vom Unternehmen als Nachweis aufbewahrt.

8 Vernichtung

Um größere Bestände von VS-NfD zu vermeiden, sind nicht mehr benötigte VS-NfD zu vernichten oder an den VS-NfD-Auftraggeber zurückzugeben.
VS-NfD, auch VS-NfD-Zwischenmaterial, sind von den bearbeitenden Personen nur an den dafür vorgesehenen Orten so zu vernichten, dass der Inhalt weder erkennbar ist noch erkennbar gemacht werden kann.
Für die Vernichtung dürfen grundsätzlich nur Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllen.

Anforderungen an Informationstechnik zur Verarbeitung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1 Einleitung

1.1 Allgemeines

Wird Informationstechnik (IT) für die Verarbeitung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) genutzt, sind neben den allgemeinen Schutzmaßnahmen der Teile 1 und 2 dieses Merkblattes zum Schutz der VS-NfD geeignete technische sowie organisatorische Maßnahmen zu treffen und deren Einhaltung regelmäßig zu kontrollieren. Zu den geeigneten technischen Maßnahmen zählen unter anderem IT-Sicherheitsprodukte, die über eine Zulassungsaussage (Zulassung oder Einsatzerlaubnis) des BSI verfügen und im vorgesehenen Einsatzkontext verwendet werden. Sofern nicht durch den VS-NfD-Auftraggeber oder das BSI andere Vorgaben existieren, sind die technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen in Ziff. 2 geregelt. Unabhängig von dem eingesetzten IT-System sind die Anforderungen an die Verarbeitung von VS-NfD gem. Ziff. 3 einzuhalten.

1.2 VS internationaler Organisationen (NATO, EU u.a.)

Bei der Verarbeitung von VS über- oder zwischenstaatlicher Einrichtungen und Stellen eines mit VS-NfD vergleichbaren Geheimhaltungsgrades gelten die jeweiligen Vorschriften dieser Einrichtungen/Stellen.

2 IT-System

Die technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen hängen von der Ausprägung des IT-Systems ab. Es gibt zwei Ausprägungen:

1. ein IT-System, das technisch isoliert („air-gapped“) betrieben wird (Ziff. 2.1) oder
2. ein IT-System, das mit anderen Netzwerken verbunden wird, die ein niedrigeres Sicherheitsniveau als VS-NfD haben (Ziff. 2.2).

Ein technisch isoliertes IT-System („air-gapped“) kann ein Einzelplatz-PC (Ziff. 2.1.1) oder ein Verbund eines IT-Systems (2.1.2) sein. Letzteres kann auch standortübergreifend vorliegen. Hierbei ist für die Übertragung ein IT-Sicherheitsprodukt mit Zulassungsaussage des BSI einzusetzen.

Die Verarbeitung von VS-NfD auf einem eigenen IT-System im Unternehmen ist unter Einhaltung folgender Voraussetzungen zulässig:

2.1 VS-NfD auf einem technisch isolierten IT-System („air-gapped“)

2.1.1 Einzelplatz-PC

Folgende technischen und organisatorischen Sicherheitsmaßnahmen sind umzusetzen:

- Zugangs-/Zugriffskontrolle:
  - Benutzung der Geräte erfolgt nur durch zugriffsberechtigte, auf das VS-NfD Merkblatt verpflichtete Personen,

  - Einrichtung von Benutzerprofil / restriktiven[1] Zugriffrechten sowie Login / Passwort um den Grundsatz „Kenntnis nur, wenn nötig“ umzusetzen.
- IT-Systeme, die nicht über eine Festplattenverschlüsselung mit Zulassungsaussage verfügen, sind vor Arbeitsende auszuschalten und im ausgeschalteten Zustand gemäß Teil 2, Ziff. 5 aufzubewahren;
- Es sind entsprechende Maßnahmen beim Patch- und Änderungsmanagement sowie zum Schutz vor Schadprogrammen zu treffen, wobei ein unbemerkter Abfluss von VS-NfD zu verhindern ist.
- Die Nutzung drahtloser Schnittstellen ist nicht gestattet;
- Deaktivierung nicht freigegebener drahtgebundener Schnittstelle;
- Einsatz einer geeigneten Festplattenverschlüsselung für mobile IT-Systeme und
- Einsatz eines IT-Sicherheitsproduktes mit Zulassungsaussage des BSI zum Ver-/Entschlüsseln von VS-NfD; Der bidirektionale Transfer mittels eines mobilen Datenträgers zwischen offenem Arbeitsplatz-PC und Einzelplatz-PC hat ausschließlich in verschlüsselter Form zu erfolgen. Es ist sicherzustellen, dass die Klartextdaten nicht auf dem mobilen Datenträger gespeichert werden, auch nicht temporär beispielsweise im Rahmen des Ver-/ Entschlüsselungsvorganges.

Eine Anwendung des IT-Grundschutzes des BSI ist hier nicht erforderlich.

2.1.2 Verbund eines IT-Systems

Neben den Sicherheitsmaßnahmen gemäß Ziff. 2.1.1 sind folgende Sicherheitsmaßnahmen zusätzlich umzusetzen:

- Mindestanforderung Datenablage: Daten unterschiedlicher VS-NfD-Aufträge müssen jeweils in separaten und ausschließlich für die jeweiligen zugriffsberechtigten Nutzer freigegebenen Projektordnern abgelegt werden; Seitens des Auftraggebers können weitergehende Anforderungen, bspw. ausschließliche Verwendung des IT-Systems für das jeweilige Projekt gefordert werden.
- Zentrale VS-NfD Komponenten: Zentrale VS-NfD Komponenten müssen nach dem Grundsatz „Kenntnis nur, wenn nötig“ im Serverraum physisch abgesichert werden. Dies kann durch eine Abtrennung in Form eines Käfigs oder einer vergleichbaren Abkastung (abschließbare Serverracks mit Einzelschließung etc.) erfolgen und
- Kommunikationsbeziehungen: Sämtliche Kommunikationsbeziehungen, insbesondere standortübergreifende, werden in einem Informationssicherheitskonzept (siehe Ziff. 4.2) beschrieben und hinsichtlich einer erforderlichen Verschlüsselung der VS-NfD durch ein IT-Sicherheitsprodukt mit Zulassungsaussage bewertet (hierzu Ziff. 3.4.1).

Ein auf das IT-System konzentriertes Informationssicherheitskonzept nach den gültigen Standards des IT-Grundschutzes des BSI ist hier nur dann erforderlich, wenn ein standortübergreifendes IT-Systems eingesetzt wird. In diesem Fall sind mindestens die Basisanforderungen umzusetzen (Ziff. 4.1). Der VS-NfD Auftraggeber kann darüber hinausgehende Anforderungen vorgeben.

[1] In einem gewöhnlich konfigurierten Betriebssystem erhält jeder Nutzer automatisch Vollzugriff auf alle Inhalte des Datenträgers mit Ausnahme der persönlichen Ordner anderer Nutzer. Seine Berechtigung für einzelne Ordner muss explizit ausgeschlossen werden (Opt-OUT). Der Grundsatz „Kenntnis nur, wenn nötig“ hingegen fordert eine explizite Zugriffserlaubnis für Nutzer, die nicht Ersteller sind (Opt-IN). Sonderregelungen bspw. für Projektgruppenordner, bei denen alle Nutzer automatisch Zugriff auf die gespeicherten Daten erhalten, sind im Informationssicherheitskonzept zu dokumentieren.

2.2 VS-NfD-Netzwerk verbunden mit Netzwerksegmenten, die nicht die VS-NfD Anforderungen erfüllen

Neben den Sicherheitsmaßnahmen gem. Ziff. 2.1.2 sind folgende Sicherheitsmaßnahmen für das VS-NfD-Netzwerk zusätzlich umzusetzen:

- Segmenttrennung: Physische oder zugelassene Trennung des VS-NfD-Netzwerksegments von anderen Netzwerksegmenten beispielsweise durch ein mehrstufiges Firewall System entsprechend der PAP-Struktur nach IT-Grundschutz des BSI.
- Firewall: Für die Firewall (PAP-Struktur) ist ein Regelwerk zu erstellen und regelmäßig anzupassen und zu überprüfen. Gegenstand dieses Regelwerkes sind insb. auch nach außen gerichtete Kommunikationsverbindungen. Die Initiierung des Zugriffs darf nur aus dem VS-NfD-Netzwerk erfolgen. Weiterhin müssen Softwareaktualisierungen, Telemetriefunktionen oder Entsprechende Konfigurationsempfehlungen, die den Abfluss von oder die Einsichtnahme in VS-NfD verhindern, sind umzusetzen und regelmäßig, insbesondere nach jedem Update, auf Veränderung zu überprüfen. Bei Auffälligkeiten sind unverzüglich weitere Schutzmaßnahmen vorzunehmen.
- Externe Schnittstellen: Sämtliche Schnittstellen sind bezogen auf die Kommunikation mit dem VS-NfD Netzsegment zu definieren und im Informationssicherheitskonzept zu beschreiben sowie in die Risikoanalyse aufzunehmen (siehe Ziff. 4.2).
- Schutz vor Schadprogrammen: Die Inhaltsprüfung auf Schadcode muss für Datenverkehr, der aus externen Netzwerken kommt, auf dem ALG (Application Layer Gateway) durchgeführt werden. Weiterhin muss allen IT-Systemen eine Software zur Erkennung von Schadcode eingesetzt werden. Diese darf keine Schadcodeprüfung außerhalb des VS-NfD Netzes, beispielsweise in der Cloud, durchführen.

Eine Anwendung des IT-Grundschutzes des BSI ist hier erforderlich. Es sind Basis- und Standardanforderungen (Ziff. 4.1) umzusetzen.

3 Anforderungen an die Verarbeitung von VS-NfD

Nachstehend werden die spezifischen Anforderungen zur elektronischen Verarbeitung von VS-NfD dargestellt. Die Verarbeitung beginnt bereits mit dem Lesen von VS-NfD auf IT.

3.1 Zulässige IT-Systeme und Freigabe

IT-Systeme zur Verarbeitung von VS-NfD müssen vor der ersten Nutzung durch die VS-NfD-verantwortliche Person freigegeben werden. Gleiches gilt für räumliche Arbeitsbereiche, die für die Verarbeitung von VS-NfD vorgesehen sind.
Private IT, Software oder Datenträger dürfen nicht für die Verarbeitung von VS eingesetzt werden.

3.2 Kennzeichnung von Datenträgern und Geräten

Datenträger, auf denen VS-NfD unverschlüsselt gespeichert werden, sind gemäß Teil 2, Ziff. 4 dieses Merkblattes zu kennzeichnen. Gleiches gilt für Geräte, in denen sich diese Datenträger befinden.

3.3 Wartung und Instandhaltung

Auf Datenträgern, die VS-NfD unverschlüsselt enthalten, sind die VS-NfD gemäß Ziff. 3.6 komplett zu löschen, bevor die Datenträger im Rahmen von Wartungs- oder Reparaturarbeiten am IT-System den persönlichen Gewahrsam der zugriffsberechtigten Personen verlassen.
Ist eine Löschung nicht möglich, sind die Datenträger auszubauen und zurückzuhalten. Ist das nicht möglich, gilt Teil 2, Ziff. 6.3 dieses Merkblattes.

3.4 Weitergabe über technische Kommunikationsverbindungen

3.4.1 Notwendigkeit der Verschlüsselung bei elektronischer Übertragung

VS-NfD müssen bei der elektronischen Übertragung grundsätzlich verschlüsselt werden mit Ausnahme Ziff. 3.4.2. Dazu sind ausschließlich IT-Sicherheitsprodukte[2] mit Zulassungsaussage einzusetzen.

3.4.2 Anforderungen zur unverschlüsselten Übertragung innerhalb von Liegenschaften

Wenn die Übertragung innerhalb einer Liegenschaft ausschließlich leitungsgebunden erfolgt und sämtliche Übertragungseinrichtungen, -leitungen, -verteiler und Trassen gegen unbefugten Zugriff geschützt sind, kann eine Verschlüsselung unterbleiben.

3.4.3 Telefonie / Fax

Telefonie und Fax-Übertragung sind nach Vornahme einer Risikobewertung Ende-zu-Ende verschlüsselt gestattet. Es gilt Ziff. 1.1.

3.4.4 Mobile IT-Systeme

Werden für die Verarbeitung oder Speicherung von VS-NfD tragbare IT-Systeme verwendet, so sind die Verschlusssachen durch IT-Sicherheitsprodukte mit Zulassungsaussage zu verschlüsseln. Von einer Verschlüsselung kann abgesehen werden, wenn die IT-Systeme innerhalb der Liegenschaft verbleiben, entweder im persönlichen Gewahrsam oder unter physischem Schutz (Teil 2, Ziff. 5).

3.4.5 Weitergabe in Notfallsituationen

Abweichend von Ziff. 3.4.1 ff. dürfen VS-NfD ausnahmsweise über nicht für VS-NfD zugelassene Kommunikationsverbindungen übermittelt werden, wenn die Übermittlung über eine BSI-zugelassene verschlüsselte Kommunikationsverbindung in einen vertretbaren Zeitrahmen nicht bereitgestellt werden kann. Die Details zu den abweichenden Rahmenbedingungen und Anforderungen werden für die jeweilige Notfallsituation vom VS-NfD-Auftraggeber gesondert festgelegt.
Wenn die Einbeziehung des VS-NfD-Auftraggebers zu einer Verzögerung führen würde, bei welcher der entstehende Schaden den mit einer Preisgabe der VS-NfD verbundenen Schaden deutlich überwiegen würde, kann die für VS-NfD verantwortliche Person ausnahmsweise die Festlegung selbst vornehmen. Der VS-NfD-Auftraggeber ist dann unverzüglich zu informieren. Mitteilungspflichten geheimschutzbetreuter Unternehmen nach GHB bleiben unberührt. In jedem Einzelfall ist die Einwilligung der für VS-NfD verantwortlichen Person einzuholen und zu dokumentieren.
In den Ausnahmefällen sind folgende Vorsichtsmaßnahmen zu beachten, damit das Risiko eines Informationsabflusses möglichst reduziert wird:

- Die Identität des Kommunikationspartners soll vor Beginn der Kommunikation festgestellt werden;

[2] Die Liste aktuell zugelassener IT-Sicherheitsprodukte und Systeme (BSI-Schrift 7164) befindet sich auf der BSI Homepage unter https://www.bsi.bund.de. Die jeweiligen Einsatz- und Betriebsbedingungen (E&B) stehen im geschützten Bereich des BMWK-Sicherheitsforums zum Download zur Verfügung. Nicht geheimschutzbetreute Unternehmen erhalten diese von ihrem VS-NfD-Auftraggeber. Die in den E&B beschriebenen Vorgaben sind zwingend umzusetzen. Eine abweichende Installation bzw. Konfiguration ist unzulässig. Wenn es keine IT-Sicherheitsprodukte mit Zulassungsaussagegibt, darf die Kommunikationsverbindung nicht verwendet werden.

- Die Kommunikation ist so zu führen, dass der Sachverhalt Dritten nicht verständlich wird und ein unmittelbarer Rückschluss auf den VS-NfD-Charakter nicht möglich ist;
- Die übermittelten VS-NfD dürfen keine Kennzeichnungen oder Hinweise aufweisen, die sie von einer nicht eingestuften Information unterscheiden. Die Kennzeichnungspflicht ist in diesem Fall aufgehoben und
- die Kommunikationspartner sind auf anderem Wege (zum Beispiel über andere technische Kommunikationsverbindungen, durch Post oder Kurier) unverzüglich über die Einstufung der VS-NfD zu unterrichten, außer, dies ist im Einzelfall nicht möglich oder nicht zweckmäßig. Der Kommunikationspartner muss die Kennzeichnung der VS-NfD, sofern möglich, nachholen.

3.5 Mitnahme und mobiles Arbeiten

Die ausschließlich elektronische Verarbeitung von VS-NfD ist auch in der Privatwohnung zulässig, wenn

- die genutzte IT (z. B. Notebooks) hierfür von der für VS-NfD verantwortlichen Person freigegeben (Ziff. 3.1) ist,
- sich die Privatwohnung innerhalb Deutschlands befindet,
- die für VS-NfD verantwortliche Person ihre Zustimmung erteilt hat,
- der/die Mitarbeiter/in über spezifische Risiken des mobilen Arbeitens belehrt ist und
- Teil 6 dieses Merkblattes von dem/der Mitarbeiter/in unterzeichnet wurde und vom Unternehmen als Nachweis aufbewahrt wird.

3.6 Löschen und Vernichten von Speichermedien die VS-NfD enthalten

Bevor Speichermedien den VS-NfD-Arbeitsbereich dauerhaft verlassen, müssen diese mittels BSI zugelassener bzw. freigegebener IT-Sicherheitsprodukte gelöscht werden. Ist eine Löschung nicht möglich, sind die Speichermedien nach den jeweils gültigen BSI-Vorgaben physisch zu vernichten.

3.7 IT-Administration

Die IT-Administration ist grundsätzlich durch eigenes Personal auszuführen. Es gilt Teil 2, Ziff. 6.3 dieses Merkblattes.

4 IT-Grundschutz des BSI

Je nach gewählter Ausprägung des IT-Systems ist der IT-Grundschutz des BSI in der jeweils geltenden Fassung in verschiedenem Umfang anzuwenden (Ziff. 1.1 f.).

4.1 Sicherheitsanforderungen

Der IT-Grundschutz des BSI in der jeweils geltenden Fassung basiert auf einer modularen Struktur, unterteilt in prozess- und systemorientierte Bausteine. In jedem Baustein werden die Sicherheitsanforderungen, die für den Schutz des betrachteten Gegenstands relevant sind, aufgeführt. Sie beschreiben, was zu dessen Schutz zu tun ist. Die Anforderungen sind in verschiedene Kategorien unterteilt, insbesondere in

- Basis-Anforderungen und
- Standard-Anforderungen, die auf den Basis-Anforderungen aufbauen.

Der notwendige Umfang der Umsetzung für die jeweilige Ausprägung des IT-Systems ergibt sich aus Ziff. 2. Die Anforderungen aus Ziff. 3 stellen einen zusätzlichen Baustein bei der Anwendung des IT-Grundschutzes dar.

4.2 Informationssicherheitskonzept und Risikoanalyse

Für das IT-System ist ein Informationssicherheitskonzept zu erstellen, welches die Anwendung des IT-Grundschutzes des BSI mit allen relevanten Sicherheitsanforderungen behandelt. Vom Unternehmen ist zu definieren, welche der Bausteine, in die der IT-Grundschutz des BSI unterteilt ist, für das IT-System zum Tragen kommen. Des Weiteren müssen die Auflagen nach VS-NfD-Merkblatt sowie eine Risikoanalyse mit einfließen. Bei Änderungen ist das Informationssicherheitskonzept inkl. der Risikoanalyse fortzuschreiben.

5 Selbstakkreditierung

Die für VS-NfD verantwortliche Person im Unternehmen bestätigt der Geschäftsleitung spätestens alle drei Jahre schriftlich die Umsetzung der Anforderungen aus Teil 3 (IT-Anforderungen) dieses Merkblattes (Selbstakkreditierung). Auf Anforderung ist dem VS-NfD-Auftraggeber bzw. dem BMWK diese Bestätigung auszuhändigen.

In der Selbstakkreditierung erklärt das Unternehmen,

1. die Umsetzung der IT-Anforderungen dieses Merkblatts in der jeweils gültigen Fassung,
2. sofern erforderlich, die Umsetzung der Einsatz- und Betriebsbedingungen der IT-Sicherheitsprodukte mit Zulassungsaussage und
3. die Etablierung eines ISMS durch:
    - die Anwendung der jeweils gültigen Standards des IT-Grundschutzes des BSI mit Erstellung eines Informationssicherheitskonzepts inkl. IT-Grundschutz-Check, Risikoanalyse und Umsetzungsplanung oder
    - eine ISO 27001 Zertifizierung auf Basis IT-Grundschutz oder
    - eine ISO 27001 Zertifizierung auf Basis einer anderen Grundlage mit Differenz-Analyse zum IT-Grundschutz (Zuordnungstabelle), wenn mindestens ein gleichwertiges Sicherheitsniveau zu den Anforderungen des IT-Grundschutzes gewährleistet ist.

Hinweise zur Kennzeichnung einer Verschlusssache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

1. Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) sind am oberen Rand mit dem voll ausgeschriebenen Geheimhaltungsgrad in schwarzer oder blauer Farbe zu kennzeichnen. Sollte eine VS-NfD aus mehreren Seiten bestehen, ist die Kennzeichnung am oberen Rand jeder beschriebenen Seite durchzuführen. Entsprechendes gilt auch für eingestufte Anlagen.
   Zusätzlich muss die Angabe enthalten sein, wer der Ersteller bzw. der VS-NfD-Herausgeber der VS-NfD ist, und wann die Erstellung bzw. Einstufung erfolgte.
   Lässt die Beschaffenheit einer VS-NfD die Kennzeichnung nicht zu, ist sinngemäß zu verfahren (z. B. Kennzeichnung in der zugehörigen Dokumentation).

2. Die Einstufungsfrist ist nur anzugeben, sofern diese die Regelfrist von 30 Jahren unterschreitet. In diesem Fall ist die Einstufungsfrist auf der ersten Seite der VS-NfD mit folgenden Vermerk anzugeben: „Die VS-Einstufung endet mit Ablauf des Jahres … .“
   Die Einstufung von VS-NfD ist spätestens nach 30 Jahren aufgehoben und kann nicht verlängert werden. Die Frist endet mit Ablauf des Jahres, in welches das Fristende fällt.

Nachweis über die Verpflichtung

Zutreffendes ist angekreuzt

Herr/Frau

Name, Vorname Geburtsdatum

wurde heute im Hinblick auf den beabsichtigten Zugang zu Verschlusssachen des Geheimhaltungsgrades

VS-NUR FÜR DEN DIENSTGEBRAUCH

über die Bestimmungen der §§ 93 bis 99, 203 Absatz 2 und 353b StGB unterrichtet, über die besonderen Bestimmungen des VS-NfD-Schutzes belehrt und auf deren gewissenhafte Erfüllung verpflichtet. Diese Verpflichtung gilt auch für die Zeit nach dem Ausscheiden aus dem Beschäftigungsverhältnis. Ihm/Ihr ist bekannt, dass ihm/ihr bei Verstößen gegen die oben genannten Bestimmungen vertrags- oder arbeitsrechtliche Maßnahmen und eine strafrechtliche Ahndung des Verstoßes nach den §§ 93 bis 99, 203 Absatz 2 und 353b StGB drohen können. Er/Sie hat eine Abschrift dieser Verpflichtung erhalten. Ihm/Ihr wurde ein Exemplar des VS-NfD-Merkblatts

☐ Teil 2 (Allgemeine Hinweise)
☐ Teil 3 (Hinweise zur Nutzung von IT)
☐ Teil 4 (Hinweise zur Kennzeichnung)
☐ Teil 6 (Behandlung von VS-NfD in der Privatwohnung)

ausgehändigt.

Ort, Datum

.....
Unterschrift des/der Verpflichteten

Vereinbarung über die Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH in der Privatwohnung („Homeoffice“)

1 Aufrechterhaltung des Schutzniveaus

Bei der Behandlung von VS-NfD in der Privatwohnung ist das durch das VS-NfD-Merkblatt vorgegebene Schutzniveau umzusetzen. Der/die Beschäftigte verpflichtet sich, die hierfür nötigen Maßnahmen in seiner/ihrer Privatwohnung zu treffen. Die Privatwohnung meint den in der Bundesrepublik Deutschland belegenen Wohnsitz des Beschäftigten.

2 Grundsatz „Kenntnis nur, wenn nötig“

Der Grundsatz „Kenntnis nur, wenn nötig“ ist einzuhalten. VS-NfD sind insbesondere vor der Einsicht durch andere, sich in der Privatwohnung befindliche Personen zu schützen. Dies ist durch geeignete organisatorische oder technische Maßnahmen sicherzustellen (z. B. Nutzung eines separaten Raumes, einfacher Verschluss bei Papieren und Material, Einhaltung von Teil 3 dieses Merkblattes bei IT-Verarbeitung), die den spezifischen Gefahren der Behandlung von VS in der Privatwohnung gerecht werden.

3 Nutzung von Informationstechnik (IT)

Für die Verarbeitung von VS-NfD auf IT ist Teil 3 des VS-NfD-Merkblattes zu einzuhalten. Insbesondere hält der/die Beschäftigte folgende Maßnahmen ein:

- Die IT-gestützte Verarbeitung von VS-NfD in der Privatwohnung darf nur auf von der für VS-NfD verantwortlichen Person freigegebenen IT-Systemen (Hardware und Software) erfolgen.
- IT-Systeme, die nicht über eine Festplattenverschlüsselung mit Zulassungsaussage verfügen, sind vor Arbeitsende auszuschalten und im ausgeschalteten Zustand gemäß Teil 2, Ziff. 5 aufzubewahren.
- Die eingesetzten IT-Systeme dürfen nicht mit IT-Geräten in der Privatwohnung oder außerhalb verbunden sein (Ausnahme: private Internetzugangsrouter, die für eine von der VS-NfD verantwortlichen Person freigegebene VS-NfD-Kommunikationsverbindung genutzt werden).
- Wartungs- oder Reparaturarbeiten an IT-Systemkomponenten dürfen nur auf Veranlassung der für den Schutz von VS-NfD im Unternehmen zuständigen Person durchgeführt werden.
- Die IT-Systeme dürfen nicht für private Zwecke verwendet werden.
- Einhaltung der von der VS-NfD verantwortlichen Person ausgehändigten Nutzungsanweisung für die IT-Systeme.

Der/die Beschäftigte ist über spezifische Risiken im „Homeoffice“ belehrt worden und bestätigt, diese Vorgaben des VS-NfD-Merkblatts und dieser Vereinbarung umzusetzen.

Ort, Datum

.....	…….....
Unterschrift des/der Beschäftigten	Unterschrift der für VS-NfD verantwortlichen Person

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

All fields must be completed and the form communicated via Government-to-Government channels

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE TO:

(Country/international organization name)

Please complete the reply boxes, where applicable:

☐ Provide an FSC assurance at the level of. ☐TS ☐CTS ☐S ☐NS ☐C ☐NC

☐ other _____

for the facility listed below

☐ Including safeguarding of classified material/information

☐ Including Communication and Information Systems (CIS) for processing classified information

☐ Initiate an FSC up to and including the level of _____ with _____ level of safeguarding and _____ level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide correction/additions as required

	corrections /additions:
1. Full facility name	
2. Full facility address	
3. Mailing address(if different from 2)	
4. Zip/postal code/city/country	
5. Name of the Security Officer	
6. Telephone/Fax/E-mail of the Security Officer	

7. This request is made for the following reason(s): (indicate particulars of the pre-contractual stage, contract, sub-contract, programme/project etc.)

Requesting NSA/DSA: Name: _____ Date:(dd/mm/yyyy) ☐☐☐☐☐☐☐☐

REPLY (within 5 working days)

This is to certify that the above mentioned facility:

1. ☐ holds an FSC up to and including the level of ☐TS ☐CTS ☐S ☐NS ☐C ☐NC
   ☐ other _____
2. ☐ on the above mentioned request, the FSC process has been initiated. You will be informed when the FSC has been established or refused.
3. ☐ does not hold an FSC
4. has the capability to safeguard classified information/material:
   ☐ yes, level ☐ no
5. has Accredited/Authorized CIS:
   ☐ yes, level ☐ no
6. This FSC assurance expires on: _____ (dd/mm/yyyy), or as advised otherwise by the NSA/DSA. In case of an earlier invalidation or in case of any changes of the information listed above you will be informed.
7. Remarks:

Issuing NSA/DSA: Name: _____ Date:(dd/mm/yyyy) ☐☐☐☐☐☐☐☐

Muster – Formblatt nur in englischer Sprache benutzen

INFORMATIONSBLATT ZUR GEHEIMSCHUTZBETREUUNG EINES UNTERNEHMENS (FSCIS)

Es sind alle Felder auszufüllen und das Formular muss von Regierung zu Regierung kommuniziert werden.

ANTRAG AUF EINEN SICHERHEITSBESCHEID FÜR EIN UNTERNEHMEN

AN:_____

(Name des Landes / der internationalen Organisation)

Bitte kreuzen Sie die zutreffenden Kästchen an:

[ ] Antrag auf einen Sicherheitsbescheid des Geheimhaltungsgrades [ ] STRENG GEHEIM [ ] COSMIC TOP SECRET [ ] GEHEIM [ ] NATO SECRET [ ] VS-VERTRAULICH [ ] NATO CONFIDENTIAL

[ ] sonstige Geheimhaltungsgrade .....

für das unten genannte Unternehmen

[ ] einschließlich der Verwahrung von Verschlusssachen

[ ] einschließlich von Kommunikations- und Informationssystemen (CIS) für die Bearbeitung von Verschlusssachen

[ ] Antrag auf Aufnahme in die Geheimschutzbetreuung bis zum und einschließlich des Geheimhaltungsgrades ..... mit Verwahrungsmöglichkeiten für VS bis ..... und (CIS) bis ....., soweit das Unternehmen derzeit nicht über diese Voraussetzungen verfügt.

Bestätigen Sie bitte die Richtigkeit der zu dem Unternehmen im Folgenden gemachten Angaben und nehmen Sie die notwendigen Korrekturen / Ergänzungen vor.

1. Vollständiger Name des Unternehmens	Korrekturen / Ergänzungen:
2. Vollständige Anschrift des Unternehmens	
3. Postanschrift (falls abweichend von 2)	
4. Postleitzahl / Stadt / Land	
5. Name des Sicherheitsbevollmächtigten	
6. Telefon / Fax / E-Mail des Sicherheitsbevollmächtigten	

7. Dieser Antrag wird aus dem folgenden Grund / den folgenden Gründen gestellt:
(Nennen Sie bitte Details bezüglich Vorvertragsstadium, Vertrag, Unterauftrag, Programm / Projekt, etc.)

Antragstellende NSA/DSA: Name: ..... Datum:(TT/MM/JJJJ) .....

ANTWORT (innerhalb von 5 Arbeitstagen)

Hiermit wird bestätigt, dass das oben genannte Unternehmen:

1. [ ] über einen Sicherheitsbescheid verfügt bis zu und einschließlich der Geheimhaltungsgrade:
[ ] STRENG GEHEIM [ ] COSMIC TOP SECRET [ ] GEHEIM [ ] NATO SECRET
[ ] VS-VERTRAULICH [ ] NATO CONFIDENTIAL

   [ ] sonstiger Geheimhaltungsgrade: .....

2. [ ] Aufgrund des oben genannten Antrags wurde das Verfahren zur Aufnahme in die Geheimschutzbetreuung eingeleitet. Sie werden informiert, sobald der Sicherheitsbescheid erteilt beziehungsweise abgelehnt wurde.

3. [ ] nicht über einen Sicherheitsbescheid verfügt.

4. über Verwahrungsmöglichkeiten für Verschlusssachen verfügt:

   [ ] ja, bis einschließlich Geheimhaltungsgrad: ..... [ ] nein.

5. über akkreditierte/genehmigte CIS verfügt:

   [ ] ja, bis einschließlich Geheimhaltungsgrad: ..... [ ] nein.

6. Dieser Sicherheitsbescheid ist gültig bis: ..... (tt/mm/jjjj) oder bis zu einer anderslautenden Auskunft durch die nationale Sicherheitsbehörde / designierte Sicherheitsbehörde. Im Falle eines früheren Ablaufs oder bei Änderungen bezüglich der o.g. Angaben werden Sie informiert.

7. Anmerkungen:

.....

Ausstellende NSA/DSA Name: ..... Datum:(TT/MM/JJJJ) .....

AUFNAHMEANTRAG

in die Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Klimaschutz

Bundesministerium für Wirtschaft und Klimaschutz
- Referat RS3 -
53107 Bonn
Per E-Mail: buero-rs3@bmwk.bund.de

I. Angaben zum antragstellenden VS-Auftraggeber

1. Name und Anschrift des Antragstellers 1a. bei geheimschutzbetreuten Unternehmen: Betriebs-/Unternehmensnummer -
2. Name, Tel-Nr. E-Mail des/der Geheimschutzbeauftragten (bei Behörden) bzw. des/der SiBe (bei Unternehmen)

II. Angaben zum aufzunehmenden Unternehmen und zum VS-Auftrag

1. Name und Anschrift des aufzunehmenden Unternehmens / Unternehmensteils	
2. VS-Auftragsbezeichnung und Beschreibung des VS-Auftrags 2a. bei Beantragung durch ein geheimschutz-betreutes Unternehmen: lfd Nr. des entsprechenden VS-Auftrages laut letzter eigener VS-Auftragsmeldung	
3. voraussichtliche Projekt-/Auftragsdauer	

4. Herausgeber der VS	☐ Bundesbehörde[1] ☐ NATO ☐ EU ☐ OCCAR ☐ ESA ☐ sonstige:
5. höchster Einstufungsgrad der VS bzw. erforderlicher Ermächtigungsgrad	☐ VS-VERTRAULICH ☐ GEHEIM ☐ STRENG GEHEIM oder vergleichbarer nicht-deutscher Einstufungsgrad
6. Art des VS-Auftrages / der VS-Bearbeitung ☐ Bearbeitung und Aufbewahrung von VS in dem aufzunehmenden Unternehmen (BMWK wird hierzu ggf. weitere Informationen anfordern) ☐ Personalgestellung, d. h. Entsendung von ermächtigtem Personal in folgendes Unternehmen: Kurzbeschreibung der konkreten Tätigkeit[2]	
7. erforderliche materielle und/oder informationstechnische Geheimschutzvorkehrungen zu schaffende Kategorien gemäß Anlage 12 GHB (Aufbewahrung von VS, IT-Bearbeitung von VS, Abstrahlsicherheit, Abhörschutz u.a.)	

Ort, Datum, Unterschrift des/der Sicherheitsbevollmächtigten bzw. des/der Geheimschutzbeauftragten

[1] Ist der VS-Herausgeber ein Land der Bundesrepublik Deutschland, so wenden Sie sich bitte an die zuständige Landesstelle.
[2]Hinweis: Findet die sicherheitsempfindliche Tätigkeit nur in einer Behörde statt, so überprüft grundsätzlich die Behörde selbst die entsprechenden Unternehmensangehörigen (vgl. § 24 Abs. 2 SÜG). Davon abweichend wird das Unternehmen nur mit Zustimmung des BMWK in die Geheimschutzbetreuung aufgenommen. Ausnahmetatbestände für eine entsprechende Zustimmung können z.B. vorliegen, wenn aufgrund der besonderen Bedeutung oder besonderer Umstände der VS-Bearbeitung organisatorische Maßnahmen im Unternehmen erforderlich sind. Dies gilt auch für die Aufnahme von VS-Unterauftragnehmern, deren VS-Auftragsbearbeitung nur in Behörden stattfinden soll.

ANFORDERUNG eines SICHERHEITSBESCHEIDS

über ein/en geheimschutzbetreutes/n Unternehmen/Unternehmensteil

Bundesministerium für Wirtschaft und Klimaschutz
- Referat RS3 -
53107 Bonn
Per E-Mail: buero-rs3@bmwk.bund.de

I. Angaben zum anfordernden VS-Auftraggeber

1. Name und Anschrift des VS-Auftraggebers 1a. bei geheimschutzbetreuten Unternehmen: Betriebs-/Unternehmensnummer -
2. Name, Tel-Nr., E-Mail des/der Geheimschutzbeauftragten (bei Behörden) bzw. des/der SiBe (bei Unternehmen)

II. Angaben zum VS-Auftragnehmer und zum VS-Auftrag

1. Name und Anschrift des VS-Auftragnehmers sowie Betriebs-/Unternehmensnummer (falls bekannt)	
2. VS-Auftragsbezeichnung und Beschreibung des VS-Auftrags 2a. bei Anforderung durch ein geheimschutzbetreutes Unternehmen: lfd Nr. des entsprechenden VS-Auftrages laut letzter eigener VS-Auftragsmeldung	
3. voraussichtliche Projekt-/Auftragsdauer	

4. Herausgeber der VS	☐ Bundesbehörde ☐ Landesbehörde ☐ NATO ☐ EU ☐ OCCAR ☐ ESA ☐ sonstige:
5. höchster Einstufungsgrad der VS bzw. erforderlicher Ermächtigungsgrad	☐ VS-VERTRAULICH ☐ GEHEIM ☐ STRENG GEHEIM oder vergleichbarer nicht-deutscher Einstufungsgrad
6. Art des VS-Auftrages / der VS-Bearbeitung ☐ Bearbeitung und Aufbewahrung von VS beim VS-Auftragnehmer ☐ Personalgestellung, d. h. Entsendung von ermächtigtem Personal ☐ in folgenden Betrieb/Betriebsteil: ☐ in folgende Behörde: 6a. Kurzbeschreibung der konkreten VS-Tätigkeit	
7. erforderliche materielle und/oder informationstechnische Geheimschutzvorkehrungen bzw. erforderliche Kategorien gemäß Anlage 12 GHB (Aufbewahrung von VS, IT-Bearbeitung von VS, Abstrahlsicherheit, Abhörschutz u.a.)	

Ort, Datum, Unterschrift des/der Sicherheitsbevollmächtigten bzw. des/der Geheimschutzbeauftragten

VS–Auftragsmeldung

Unternehmen-/Unternehmensteil: **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**
Unternehmens-/Betriebs-Nr.: **XXXX-XXXX**
Anschrift/Telefon-Nr./E-Mail: **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX** **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX** **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**
Abgabetermin der VS-Auftragsmeldung: **XX.XX.XXXX**

Abgabe der VS-Auftragsmeldung nur Online möglich!

1. VS-V oder höher

a) Anzahl der im Unternehmen/Unternehmensteil aufbewahrten VS-V oder höher
☐ keine ☐ 1-10 ☐ bis 100 ☐ bis 1000 ☐ über 1000,
darunter internationale (z.B. NATO, EU, andere Staaten)?
☐ nein ☐ ja

b) Gibt es laufende VS-V oder höher eingestufte VS-Aufträge, die von dem Unternehmen/ Unternehmensteil durchgeführt werden?
☐ nein ☐ ja

c) Gibt es bei den VS-V oder höher eingestuften VS-Aufträgen Änderungen gegenüber der letzten VS-Auftragsmeldung?
☐ nein ☐ ja (Falls „ja“ ist die Liste der VS-V oder höher eingestuften VS-Aufträge auszufüllen.)

2. VS-NfD

a) Anzahl der laufenden VS-NfD-Aufträge des Unternehmens/Unternehmensteils
☐ keine ☐ 1-10 ☐ bis 50 ☐ über 50,
darunter internationale (z.B. NATO, EU, andere Staaten)?
☐ nein ☐ ja

b) Werden im Unternehmen/Unternehmensteil VS-NfD auf IT bearbeitet?
☐ nein ☐ ja

Ich versichere, dass die Angaben richtig und vollständig sind. Die vorhandenen Sicherheitsvorkehrungen für die Durchführung der VS-Aufträge sind ausreichend.

_____ _____

(Ort, Datum) Name in Druckschrift (Unterschrift Sicherheitsbevollmächtigte(r))

GHB – Anlage 6

Liste der VS-V oder höher eingestuften VS-Aufträge

Unternehmens-/Betriebs-Nr.:
-

Lauf-ende Nr.	Verfahrens-stand (L=Laufend, A=Abge-schlossen oder K=Nur nach Aufforderung durch BMWi)	VS-Auftragsbezeichnung oder Beschreibung des VS-Auftrags	amtliche VS-Auftrags-nummer (wenn vorhanden)	VS-Auftraggeber: Unternehmen: Betriebs-Nr.	VS-Auftraggeber: sonstiger VS-Auftraggeber (Behörden, ausländische VS-Auftraggeber): vollständiger Name und Anschrift	Höchste VS-Einstufung des VS-Auftrags	Ort der Auftrags-durchführung	Nr. der Kontrollzonne (falls Auftragsdurchführung in Kontrollzonen im eigenen Unternehmen/ Unternehmensteil)	Nr. der Sperrzone (falls Auftragsdurchführung in Sperrzonen im eigenen Unternehmen/ Unternehmensteil)	Nr. der ITGA (falls Bearbeitung von VS-V oder höher auf IT im eigenen Unternehmen/ Unternehmens-teil)	Art des VS-Auftrags (P = Personalgestellung, M = VS-V oder höher im eigenen Haus und/oder IT = VS-V oder höher auf IT im eigenen Haus)	Änderung gegen-über letzter Meldung
1	2	3a	3b	4a	4b	5	6	7a	7b	8	9	10

Abgabe der VS-Auftragsmeldung nur Online möglich!

 Bitte beachten Sie die Erläuterungen zum Ausfüllen der VS-Auftragsmeldung.

GHB – Anlage 6

Erläuterung zum Ausfüllen der VS-Auftragsmeldung

A. Vorbemerkungen

Der Begriff des VS-Auftrages gemäß 1.8.1 GHB ist weiter gefasst als der Begriff des kaufmännischen Auftrages. Ein VS-Auftrag liegt vor, wenn VS zur Kenntnis genommen, erstellt, verarbeitet, transportiert, verwahrt oder geschützt werden sollen oder die Möglichkeit besteht, sich im Zuge des VS-Auftrages Zugang zu VS zu verschaffen. Auch bei der Gestellung von überprüftem und VS-ermächtigtem Personal, für das SiBe-Bescheinigungen bzw. Personal Security Clearances angefordert werden, handelt es sich um einen VS-Auftrag. Es ist zu unterscheiden zwischen VS-NfD-Aufträgen und VS-V oder höher eingestuften VS-Aufträgen.

Die VS-Auftragsmeldung ist Teil des Geheimschutzes; dieser ist unabhängig vom vorbeugenden personellen Sabotageschutz und von der Satellitendatensicherheit.

B. Vorblatt

Alle Felder sind Pflichtfelder.

Abgabetermin der VS-Auftragsmeldung:
Anzugeben ist der halbjährliche Abgabetermin, der dem Unternehmen/Unternehmensteil im Sicherheitsbescheid mitgeteilt wurde.

1. a) Anzahl der im Unternehmen/Unternehmensteil aufbewahrten VS-V oder höher … darunter internationale (z.B. NATO, EU, andere Staaten)?
Anzugeben ist die Anzahl der VS-VERTRAULICH (VS-V), GEHEIM oder STRENG GEHEIM eingestuften VS, die in ihrem Unternehmen/Unternehmensteil aufbewahrt werden. Ferner ist anzugeben, ob darunter auch internationale VS (z.B. der NATO, der EU oder anderer Staaten) sind, die den deutschen Geheimhaltungsgraden VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM entsprechen.

1. c) Gibt es bei den VS-V oder höher eingestuften VS-Aufträgen Änderungen gegenüber der letzten VS-Auftragsmeldung?
Anzugeben ist, ob es Änderungen gegenüber der letzten VS-Auftragsmeldung gibt. Falls ja, ist die *Liste der VS-V und höher eingestuften VS-Aufträge* zu übersenden. Eine Änderung ist jede Änderung in den Spalten der *Liste der VS-V und höher eingestuften VS-Aufträge*, z.B. auch der Abschluss eines VS-Auftrags.

2. a) Anzahl der laufenden VS-NfD-Aufträge des Unternehmens/Unternehmensteils … darunter internationale (z.B. NATO, EU, andere Staaten)?
Anzugeben ist die Anzahl der reinen VS-NUR FÜR DEN DIENSTGEBRAUCH-Aufträge (VS-NfD). Das Führen von Sicherheitsakten stellt keinen VS-NfD Auftrag dar. Ferner ist anzugeben, ob unter den reinen VS-NfD-Aufträgen auch Aufträge von internationalen VS-Auftraggebern (z.B. der NATO, der EU oder anderer Staaten) sind.

2. b) Werden im Unternehmen/Unternehmensteil VS-NfD auf IT bearbeitet?
Anzugeben ist, ob im Unternehmen/Unternehmensteil VS-NfD auf IT bearbeitet werden unabhängig davon, ob dies im Rahmen von VS-V oder höher eingestuften Aufträgen oder reinen VS-NfD-Aufträgen erfolgt. Das Bearbeiten von ausgefüllten Sicherheitserklärungen auf IT ist ein Bearbeiten von VS-NfD auf IT.

Abgabe der VS-Auftragsmeldung nur Online möglich!

C. Liste der VS-V oder höher eingestuften VS-Aufträge

Die Betriebs-Nr. und die Spalten 1 bis 5 und 9 sind Pflichtfelder. Es sind alle laufenden VS-Aufträge aufzulisten und die VS-Aufträge, die seit der letzten VS-Auftragsmeldung abgeschlossen wurden.

Spalte 1: Laufende Nr.

Die VS-Aufträge werden fortlaufend nummeriert. Eine einmal vergebene laufende Nr. darf nicht nochmals vergeben werden, auch nicht nachdem der VS-Auftrag als abgeschlossen gemeldet wurde und in späteren VS-Auftragsmeldungen nicht mehr erscheint. Die Nummerierung ist fortlaufend weiterzuführen.

Spalte 2: Verfahrensstand (L=Laufend, A=Abgeschlossen und K=Nur nach Aufforderung durch BMWi)

Der Verfahrensstand K, d.h. kein VS-Auftrag, ist nur nach Aufforderung durch BMWi zu vergeben.

Spalte 3a/3b: VS-Auftragsbezeichung und VS-Auftragsnummer oder Beschreibung des VS-Auftrags

Einzutragen ist in Spalte *3a* die VS-Auftragsbezeichung. Falls keine VS-Auftragsbezeichung vorhanden ist, ist eine Beschreibung des VS-Auftrags einzutragen, die Beschreibung soll in wenigen Worten den Gegenstand des VS-Auftrags benennen. In Spalte *3b* ist die VS-Auftragsnummer einzutragen. Falls keine VS-Auftragsnummer vorhanden ist, ist keine einzutragen.

Spalte 4a/4b: VS-Auftraggeber (vollständiger Name und vollständige Anschrift) oder Betriebs-Nr.

Ist der Auftraggeber ein deutsches Unternehmen, so ist die Betriebs-Nr. des VS-Auftraggebers in Spalte *4a* einzutragen. Ist der VS-Auftraggeber eine Behörde, ein ausländisches Unternehmen, eine ausländische Behörde oder eine internationale Organisation, so ist in Spalte *4b* der vollständige Name und die Anschrift anzuführen. Bei VS-Aufträgen von Bundeswehrdienststellen ist das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAINBw) als VS-Auftraggeber einzutragen. Das Bundesministerium der Verteidigung (BMVg), das Amt für den militärischen Abschirmdienst (MAD), das Zentrum für Informationstechnik der Bundeswehr (IT-Zentrum Bw) bzw. die National Distribution Authority (NDA) Germany und das Kommando Strategische Aufklärung der Bundeswehr sind selbst als VS-Auftraggeber einzutragen.

Spalte 5: Höchste VS-Einstufung des VS-Auftrags

Einzutragen ist die höchste VS-Einstufung des VS-Auftrags. Bei VS-Aufträgen, die Personalgestellung umfassen, ist an dieser Stelle die höchste geforderte VS-Ermächtigung einzutragen.

Spalte 6: Ort der Auftragsdurchführung

Einzutragen ist die genaue Ortsangabe z.B. Raum oder Gebäude im Unternehmen/ Unternehmensteil; bei Gestellung von VS-ermächtigtem Personal beim VS-Auftraggeber dessen Anschrift. Bei verschiedenen Einsatzorten fremder VS-Auftraggeber, ist „beim Kunden“ einzutragen.

Spalte 7a/7b: Nr. der Sperr-/Kontrollzone (falls Auftragsdurchführung in Sperr-/Kontrollzonen im eigenen Unternehmen/Unternehmensteil)

Falls der VS-Auftrag in VS-Sperr-/Kontrollzonen im eigenen Unternehmen/Unternehmensteil durchgeführt wird, ist die von BMWi festgelegte Nr. der Sperr-/Kontrollzone anzugeben. Die Kontrollzone ist in Feld *7a* als Zahl und die Sperrzone in Feld *7b* als Zahl einzutragen. Zugelassen

Abgabe der VS-Auftragsmeldung nur Online möglich!

sind ausschliesslich nummerische Eingaben. Mehrfachnennungen sind durch Kommasetzung zu trennen.

Spalte 8: Nr. der ITGA (falls Bearbeitung von VS-V oder höher auf IT im eigenen Unternehmen/Unternehmensteil)
Falls zur Auftragsdruchführung VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM oder entsprechende internationale Geheimhaltungsgrade auf IT bearbeitet werden, ist die von BMWi festgelegte Nr. der IT-Geheimschutzanweisung (ITGA) anzugeben. Mehrfachnennungen sind durch Kommasetzung zu trennen.

Spalte 9: Art des VS-Auftrags (P=Personalgestellung, M=VS-V oder höher im eigenen Haus und/oder IT=VS-V oder höher auf IT im eigenen Haus)
Anzugeben ist die Art des VS-Auftrags. *Personalgestellung* steht für VS-Aufträge bei denen nur VS-ermächtigtes Personal zum VS-Auftraggeber entsandt wird.*VS-V oder höher im eigenen Haus* steht für VS-Aufträge bei denen im eigenen Unternehmen/Unternehmensteil VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM oder entsprechende internationale Geheimhaltungsgrade bearbeit werden. *VS-V oder höher auf IT im eigenen Haus* steht für VS-Aufträge bei denen im einen Unternehmen/ Unternehmensteil VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM oder entsprechende internationale Geheimhaltungsgrade auf IT bearbeit werden.

Spalte 10: Änderung gegenüber letzter Meldung
Bei einer Änderung gegenüber der letzten VS-Auftragsmeldung ist ein Haken zu setzen.

Abgabe der VS-Auftragsmeldung nur Online möglich!

VS-Einstufungsliste

Dieser Vordruck ist in zweifacher Ausfertigung zu übersenden.

Höchster Geheimhaltungsgrad:
VS-VERTRAULICH ☐ GEHEIM ☐ STRENG GEHEIM ☐
PROJECT SECURITY INSTRUCTION (PSI) ☐ JA ☐ NEIN
(Ob eine PSI besteht, ist beim zuständigen Vorhabenmanager zu erfragen.)

Auftragnehmer

Auftragsgegenstand

Auftragsnummer

Ausstellungsdatum	**Verlängert am**

Anmerkungen
1. Die VS-Einstufung ist durch ein Kreuz in der entsprechenden Spalte in der Rubrik "Geheimhaltungsgrade" festzulegen.
2. - Wenn die gesamte Position einem gleichen Geheimhaltungsgrad unterliegt, genügt das Kreuz in der jeweiligen Spalte.
   - Kommen innerhalb einer Position mehrere Geheimhaltungsgrade in Betracht, so ist ausschließlich der **höchste** Geheimhaltungsgrad anzukreuzen.
   - Abweichungen sind in den Anlagen aufzuschlüsseln und zu spezifizieren.
3. Hier nicht aufgeführte, jedoch einzustufende Positionen sind in ziffernmäßiger Fortsetzung anzufügen.

		Geheimhaltungsgrade				**Hinweise**			
	Die bei der Durchführung dieses Auftrages beim Auftragnehmer entstehenden Verschlusssachen sind auf Veranlassung des Bundesministers der Verteidigung geheimzuhalten und gemäß den Bestimmungen des Geheimschutzhandbuches des Bundesministeriums für Wirtschaft und Energie zu kennzeichnen.	STRENG GEHEIM	GE-HEIM	VS-VER-TRAU-LICH	VS-NfD	of-fen	KRYP-TO	Fm Auf kl	s. An-mer-kung bzw. Anlage
1.	**Bezeichnung des Auftragsgegenstandes** Ist eine VS-Einstufung unvermeidbar, so ist eine offene Deckbezeichnung zu wählen, bei deren Verwendung Schriftgut entsprechenden Inhalts offen behandelt werden kann.								
2.	**Angebot** Eine VS-Einstufung der rechtlichen und kaufmännischen Ausführungen ist zu vermeiden. Es sind nur die technischen Angaben einzustufen.								
3.	☐ **Vorvertrag** ☐ **Vertrag** Hinweis siehe Pos. 2								
4.	**Kalkulation** Hinweis siehe Pos. 2								
5.	☐ **Strukturpläne** ☐ **Netzpläne** ☐ **Balkenpläne** ☐ **Listen** ☐ **Beiträge zum AZF-Plan**								
6.	**Allgemeiner Schriftverkehr** Ist in der Regel offen zu führen.								
7.	☐ **Leistungsbeschreibung** ☐ **Lastenheft** In einer Erläuterung ist darzustellen, welche Angaben selbst und welche nur im Zusammenhang mit weiteren und welchen Angaben geheimzuhalten sind.								
8.	**Prüf-, Leistungsdaten, Meßwerte usw.** Hinweis siehe Pos. 7								
9.	**Skizzen, Zeichnungen, Pausen, Fotos usw.** Anzugeben sind die Voraussetzungen, unter denen der angekreuzte Geheimhaltungsgrad zutrifft (z.B.: Zusammenstellungsbezeichnungen u.ä.) und davon abweichende Gegebenheiten, die eine geringere VS-Einstufung zulassen und welche (z.B.: Zeichnungen von nicht spezifischen Einheiten, Zeichnungen ohne Rückschlüsse auf Funktion und Wirkungsweise bestimmter Teile)								
10.	**Konstruktionsberechnungen und -unterlagen** Hinweis siehe Pos. 9								
11.	**Modelle und Attrappen** Sinngemäß ist wie zu Pos. 9 zu verfahren. Zusätzlich sind Angaben erforderlich, die erkennen lassen, in welchem Bauzustand, ab welchem Zeitpunkt oder aufgrund sonstiger Merkmale eine VS-Einstufung erfolgen muß. Des weiteren ist - soweit zutreffend - der Zeitraum anzugeben, für den die VS-Einstufung gilt (z.B.: bis Beginn der Flug- oder Fahrerprobung). Zeitpunkt der Herabstufung ist wichtig für spätere Erprobung.								
12.	**Versuche** VS-Einstufung ist nach Möglichkeit zu beschränken auf Zielsetzung, Vorbereitung, Auswertung und Ergebnis des Versuchs.								
13.	**Analysen**								

		Geheimhaltungsgrade				Hinweise			
		STRENG GEHEIM	GE-HEIM	VS-VER-TRAU-LICH	VS-NfD	of-fen	KRYP-TO	Fm Aufkl	s. An-mer-kung bzw. Anlage
14.	☐ **Erprobungsergebnisse** ☐ **Berichte** ☐ **Dokumentation** Anzugeben sind die Voraussetzungen, unter denen der angekreuzte Geheimhaltungsgrad zutrifft. Gegebenheiten, die eine abweichende VS-Einstufung zulassen, sind unter Angabe des Geheimhaltungsgrades ebenfalls einzutragen. Für Teilergebnisse und -berichte ist der Hinweis zu Pos. 7. und 8. zu beachten.								
15.	☐ **Gerätebeschreibung** ☐ **Baubeschreibung**								
16.	☐ **Vollständiges Gerät** ☐ **Prototypen** Hinweis siehe Pos. 11.								
17.	**Äußere Form** Hinweis siehe Pos. 11.								
18.	**Baugruppen** Hinweis siehe Pos. 11.								
19.	**Unterbaugruppen** Hinweis siehe Pos. 11.								
20.	**Einzelteile** Hinweis siehe Pos. 11.								
21.	**Ersatzteilliste(n)**								
22.	**Sonderausrüstung** Soweit zutreffend und VS-Einstufung vorhanden, in gesonderter Anlage erläutern.								
23.	**Bewaffnung** Hinweis siehe Pos. 11.								
24.	☐ **Transport** ☐ **Versand** Entsprechend dem Geheimhaltungsgrad der zu versendenden Sache. Besonderheiten (z.B.: Transport mit Kraftfahrzeugen der Bundeswehr) sind zu vermerken.								
25.	**Erforderliche VS-Ermächtigung von Personen**								
26.	**ggf. Bemerkungen zur Sicherheitsüberprüfung von Personen (z.B.: FmAufkl)**								
27.									
28.									
29.									
30.									
31.	**Maßnahmen zur Abstrahlsicherheit sind zu treffen:** Bei “ja” ist die Notwendigkeit gesondert zu erläutern.	☐ **ja** ☐ **nein**							

Fachreferat	Ruf-Nr.	Datum	**Krypto (IT-AmtBw C 1)** Fachreferat	Ruf-Nr.	Datum
Unterschrift			Unterschrift		

VS-Einstufungsliste

Dieser Vordruck ist in zweifacher Ausfertigung zu übersenden

Höchster Geheimhaltungsgrad:
VS-VERTRAULICH ☐ **GEHEIM** ☐ **STRENG GEHEIM** ☐
PROJECT SECURITY INSTRUCTION (PSI) ☐ **JA** ☐ **NEIN**
(Ob eine PSI besteht, ist beim zuständigen Vorhabenmanager zu erfragen.)

Amtlicher Auftraggeber	.Herausgeber der amtlichen Einstufungsliste/Datum
Nichtamtlicher Auftraggeber	(Unter-) Auftragnehmer / (Unter-) Auftragsnummer
Auftragsnummer	Bezeichnung des (Unter-) Auftrags
Bezeichnung des öffentlichen Auftrags	

		Geheimhaltungsgrade				Hinweise			
	Die bei der Durchführung dieses Auftrages beim Auftragnehmer entstehenden Verschlusssachen sind auf Veranlassung des Bundesministers der Verteidigung geheimzuhalten und gemäß den Bestimmungen des Geheimschutzhandbuches des Bundesministeriums für Wirtschaft und Energie zu kennzeichnen.	STRENG GEHEIM	GE-HEIM	VS-VER-TRAU-LICH	VS-NfD	of-fen	KRYP-TO	Fm Auf kl	s. An-mer-kung bzw. Anlage
1.	**Bezeichnung des Auftragsgegenstandes** Ist eine VS-Einstufung unvermeidbar, so ist eine offene Deckbezeichnung zu wählen, bei deren Verwendung Schriftgut entsprechenden Inhalts offen behandelt werden kann.								
2.	**Angebot** Eine VS-Einstufung der rechtlichen und kaufmännischen Ausführungen ist zu vermeiden. Es sind nur die technischen Angaben einzustufen.								
3.	☐ **Vorvertrag** ☐ **Vertrag** Hinweis siehe Pos. 2								
4.	**Kalkulation** Hinweis siehe Pos. 2								
5.	☐ **Strukturpläne** ☐ **Netzpläne** ☐ **Balkenpläne** ☐ **Listen** ☐ **Beiträge zum AZF-Plan**								
6.	**Allgemeiner Schriftverkehr** Ist in der Regel offen zu führen.								
7.	☐ **Leistungsbeschreibung** ☐ **Lastenheft** In einer Erläuterung ist darzustellen, welche Angaben selbst und welche nur im Zusammenhang mit weiteren und welchen Angaben geheimzuhalten sind.								
8.	**Prüf-, Leistungsdaten, Meßwerte usw.** Hinweis siehe Pos. 7								
9.	**Skizzen, Zeichnungen, Pausen, Fotos usw.** Anzugeben sind die Voraussetzungen, unter denen der angekreuzte Geheimhaltungsgrad zutrifft (z.B.: Zusammenstellungsbezeichnungen u.ä.) und davon abweichende Gegebenheiten, die eine geringere VS-Einstufung zulassen und welche (z.B.: Zeichnungen von nicht spezifischen Einheiten, Zeichnungen ohne Rückschlüsse auf Funktion und Wirkungsweise bestimmter Teile)								
10.	**Konstruktionsberechnungen und -unterlagen** Hinweis siehe Pos. 9								
11.	**Modelle und Attrappen** Sinngemäß ist wie zu Pos. 9 zu verfahren. Zusätzlich sind Angaben erforderlich, die erkennen lassen, in welchem Bauzustand, ab welchem Zeitpunkt oder aufgrund sonstiger Merkmale eine VS-Einstufung erfolgen muß. Desweiteren ist - soweit zutreffend - der Zeitraum anzugeben, für den die VS-Einstufung gilt (z.B.: bis Beginn der Flug- oder Fahrerprobung). Zeitpunkt der Herabstufung ist wichtig für spätere Erprobung.								
12.	**Versuche** VS-Einstufung ist nach Möglichkeit zu beschränken auf Zielsetzung, Vorbereitung, Auswertung und Ergebnis des Versuchs.								
13.	**Analysen**								

BWB A 1443/01.03

		Geheimhaltungsgrade				Hinweise			
		STRENG GEHEIM	GE-HEIM	VS-VER-TRAU-LICH	VS-NfD	of-fen	KRYP-TO	Fm Aufkl	s. An-mer-kung bzw. Anlage
14.	☐ **Erprobungsergebnisse** ☐ **Berichte** ☐ **Dokumentation** Anzugeben sind die Voraussetzungen, unter denen der angekreuzte Geheimhaltungsgrad zutrifft. Gegebenheiten, die eine abweichende VS-Einstufung zulassen, sind unter Angabe des Geheimhaltungsgrades ebenfalls einzutragen. Für Teilergebnisse und -berichte ist der Hinweis zu Pos. 7. und 8. zu beachten.								
15.	☐ **Gerätebeschreibung** ☐ **Baubeschreibung**								
16.	☐ **Vollständiges Gerät** ☐ **Prototypen** Hinweis siehe Pos. 11.								
17.	**Äußere Form** Hinweis siehe Pos. 11.								
18.	**Baugruppen** Hinweis siehe Pos. 11.								
19.	**Unterbaugruppen** Hinweis siehe Pos. 11.								
20.	**Einzelteile** Hinweis siehe Pos. 11.								
21.	**Ersatzteilliste(n)**								
22.	**Sonderausrüstung** Soweit zutreffend und VS-Einstufung vorhanden, in gesonderter Anlage erläutern.								
23.	**Bewaffnung** Hinweis siehe Pos. 11.								
24.	☐ **Transport** ☐ **Versand** Entsprechend dem Geheimhaltungsgrad der zu versendenden Sache. Besonderheiten (z.B.: Transport mit Kraftfahrzeugen der Bundeswehr) sind zu vermerken.								
25.	**Erforderliche VS-Ermächtigung von Personen**								
26.	**ggf. Bemerkungen zur Sicherheitsüberprüfung von Personen (z.B.: FmAufkl)**								
27.									
28.									
29.									
30.									
31.	**Maßnahmen zur Abstrahlsicherheit sind gemäß den Vorgaben des amtlichen VS-Auftraggebers zu treffen:** **(vgl. ggfs. VS-Einstufungsliste des amtlichen VS-Auftraggebers, falls erforderlich ist die Notwendigkeit mit dem amtlichen VS-Auftraggebers abzustimmen.)**	☐ **ja** ☐ **nein**							

Unterschrift Projektleiter	Unterschrift

Anmerkungen

Die VS-Einstufung ist durch ein Kreuz in der entsprechenden Spalte in der Rubrik “Geheimhaltungsgrade” festzulegen.

- Wenn die gesamte Position einem gleichen Geheimhaltungsgrad unterliegt, genügt das Kreuz in der jeweiligen Spalte.
- Kommen innerhalb einer Position mehrere Geheimhaltungsgrade in Betracht, so ist ausschließlich der **höchste** Geheimhaltungsgrad anzukreuzen.
- Abweichungen sind in den Anlagen aufzuschlüsseln und zu spezifizieren.

Hier nicht aufgeführte, jedoch einzustufende Positionen sind in ziffernmäßiger Fortsetzung anzufügen.

Vorschlag zur Bestellung
des/der Sicherheitsbevollmächtigten (SiBe),
seiner/ihrer Vertretung und seine/r Mitarbeiter/innen

Bundesministerium
für Wirtschaft und Klimaschutz
Referat RS 3
53107 Bonn

1. Name und Anschrift des Betriebes bzw. des zu betreuenden Betriebsteils
   Name Betriebs-Nr. -

   Anschrift

2. In Kenntnis der Stellung und der Aufgaben der nachfolgend benannten Funktionsträger/innen schlage/n ich/wir vor,

a) als Sicherheitsbevollmächtigte/r (SiBe):

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

b) als ständige/n Vertreter/in des/der SiBe vor Ort (StVO):

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

c) gegebenenfalls[1] als Stellvertreter/in des/der StVO (Stv):

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

[1] ´Nur wenn der Umfang der Geheimschutzaufgaben und die Anzahl der VS-Ermächtigten eine solche Bestellung erforderlich machen (3.1.2 Abs. 2 S. 2 GHB); vorherige Abstimmung mit BMWK erforderlich

d) gegebenenfalls[2] als VS-Verwalter/in (VSV):

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

e) gegebenenfalls[3] als Vertreter/in des/der VS-Verwalter/in (VSVV):

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

f) gegebenenfalls[4] als IT-VS-Beauftragte/r:

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

g) gegebenenfalls[5] als Vertreter/in des/der IT-VS-Beauftragten:

☐ Herrn ☐ Frau Name, Vorname:	
Geburtsdatum	PK-Nr. (falls vorhanden)
Telefon-Nr. (geschäftlich)	Mobilfunk-Nr. (geschäftlich)
E-Mail-Adresse (geschäftlich)	Anschrift (geschäftlich) falls abweichend von 1.

zu bestellen.

[2] Nur bei Aufbewahrung von VS im Unternehmen; ggf kann SiBe/StVO selbst Funktion wahrnehmen
[3] Nur bei Aufbewahrung von VS im Unternehmen; ggf kann SiBe/StVO selbst Funktion wahrnehmen
[4] Nur bei Bearbeitung von VS auf IT im Unternehmen; ggf kann SiBe/StVO selbst Funktion wahrnehmen
[5] Nur bei Bearbeitung von VS auf IT im Unternehmen; ggf kann SiBe/StVO selbst Funktion wahrnehmen

3. Ich/wir bestätigen, dass:

   - der/die SiBe in Angelegenheiten des Geheimschutzes dem/der Vorsitzenden der Geschäftsleitung, wo dies nicht möglich ist, dem/der nach der Geschäftsordnung zuständigen Mitglied der Geschäftsleitung, in organisatorisch eindeutiger Weise unmittelbar unterstellt ist.
   - der/die SiBe mit allen Befugnissen ausgestattet ist, die für eine ordnungsgemäße Durchführung der von dem Unternehmen im öffentlich-rechtlichen Vertrag mit dem BMWK übernommenen Geheimschutzverpflichtungen erforderlich sind.
   - der/die SiBe mit den notwendigen personellen und materiellen Mitteln (Mitarbeiter, Räume, Einzelbüro für SiBe, technische Einrichtungen etc.) ausgestattet und bei allen geheimschutzrelevanten Maßnahmen beteiligt und unterstützt wird.
   - das Einverständnis der benannten Personen zur Weitergabe ihrer personenbezogenen Daten durch das BMWK an das Bundesamt für Verfassungsschutz, an die zuständigen Landesbehörden für Verfassungsschutz und die VS-Auftraggeber, vorliegt.

4. Der/die SiBe, der/die StVO und seine/ihre mit Aufgaben des Geheimschutzes befassten Mitarbeiter/innen nehmen keine Aufgaben des/der Datenschutzbeauftragten, der Gleichstellungsbeauftragten oder der Schwerbehindertenvertretung wahr. ☐ Trifft zu ☐ Trifft nicht zu

5. Der/die SiBe, der/die StVO und seine/ihre mit Aufgaben des Geheimschutzes befassten Mitarbeiter/innen üben keine anderen Aufgaben der Personalverwaltung (insb. Betriebsratsmitgliedschaft) oder die des Compliance Officer aus. ☐ Trifft zu ☐ Trifft nicht zu

   Falls **„Trifft nicht zu“** angekreuzt wurde und Sie einen Antrag für eine Ausnahme stellen wollen: Schildern Sie Gründe für diese Ausnahme auf einem Beiblatt (geringe Beschäftigtenanzahl oder Personalstruktur im Unternehmen, aufgrund derer die Trennung der genannten Person/en von Aufgaben der Personalverwaltung nicht möglich ist, siehe 3.2 Abs. 2 GHB)

6. Bitte beschreiben Sie (sofern zutreffend) die weiteren Tätigkeiten des/der SiBe und seiner/ihrer Stellvertreter/in im Unternehmen (insb. Tätigkeiten mit Bezug zu Staaten mit besonderem Sicherheitsrisiko - Anlage zur „Anleitung zum Ausfüllen der Sicherheitserklärung“ siehe Anlage 19b, 19c GHB).

7. Alle benannten Personen sind Angehörige des Unternehmens. ☐ Trifft zu ☐ Trifft nicht zu

8. Die benannten Personen werden nach Zustimmung des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) von der Geschäftsführung bestellt. Jede zukünftige Änderung wird unmittelbar mittels neuer komplett ausgefüllter Anlage beim Bundesministerium für Wirtschaft und Klimaschutz (BMWK) zu Händen Referat RS 3 angezeigt.

Ort, Datum

Unterschrift(en) Geschäftsleitung

GHB - Anlage 9

Unternehmensangaben

(Zweifach einsenden an das Bundesministerium für Wirtschaft und Klimaschutz)

1)	Unternehmen laut handelsgerichtlicher Eintragung / Beantragung:			***Bearbeitungsvermerke des BMWK***
	Betriebsnr.[1]:			
2)		Sitz und Anschrift des Unternehmens	Sitz und Anschrift des zu betreuenden unselbstständigen Unternehmensteils (Betriebsteil/Niederlassung)	
	PLZ / Ort			
	Straße / Hausnummer			
	Bundesland			
	Telefon / E-Mail			
	Internetadresse			
3)	Rechtsform / Handelsregisternr.			

4a)	Gesellschafter/Inhaber[2] (bei **juristischen** Personen genaue Bezeichnung lt. handelsgerichtlicher Eintragung und Postanschrift) (bei **natürlichen** Personen Name, Vorname(n) (Rufname unterstreichen), Geburtsdatum, Staatsangehörigkeit)	
	Anteile in %	
4b)	Falls unter 4a) juristische Personen angegeben sind, sind zusätzlich die Eigentumsverhältnisse dieser Gesellschafter einzutragen[2]	
	Anteile in % der unter 4a) genannten juristischen Personen	

[1] Vom BMWK vergebene Betriebsnr., 8-stellig angeben.
[2] Weitere Angaben, ggf. auf einem Ergänzungsblatt.

5)	Falls weitere übergeordnete Gesellschafter/Inhaber (juristische/natürliche Personen) bis zur obersten Ebene mit Sitz in Staaten mit besonderen Sicherheitsrisiken nach der Staatenliste gemäß § 13 Abs. 1 Nr. 17 SÜG existieren,[3] sind diese nachfolgend anzugeben Grafische Darstellung der Verbindung mit dem Unternehmen und der jeweiligen Anteile in % auf einem Ergänzungsblatt	

6) Geschäftsleitung (Inhaber, Vorstand, Geschäftsführer)[4]

Name	Vorname (n)	Geburts-datum	Staats-angehörig-keit	Aufgabengebiet/ Zuständigkeit Geheimschutz

7)	Branche (Fabrikations-programm, Arbeitsgebiet o.ä.)	
8)	Anzahl der im gesamten Unternehmen beschäftig-ten Personen	
9)	Welche unselbstständigen Unternehmensteile (Be-triebsteile / Niederlassun-gen) müssen geheim-schutzbetreut werden (2.3.2 Abs. 2 GHB)? Für jeden zu betreuenden unselbstständigen Unter-nehmensteil ist GHB-Anlage 8 (Vorschlag zur Bestellung des/der Sicher-heitsbevollmächtigten…) beizufügen.	

Die hier aufgeführten natürlichen Personen sind darüber unterrichtet, dass diese Daten gespeichert werden und sind damit einverstanden.

Ich/Wir verpflichte(n) mich/uns, jede Änderung (hierzu zählt auch die Beantragung des Insolvenzverfahrens) unverzüglich dem Bundesministerium für Wirtschaft und Klimaschutz - Referat ZC4 - 53107 Bonn mitzuteilen.

,

(Unterschrift Geschäftsleitung) (Ort, Datum)

[3] Die Liste findet sich als Anlage zur Sicherheitserklärung in Anlage 19b, 19c zum GHB; Beteiligungen (auch mittelbar) unter 10 % müssen nicht angegeben werden.

[4] Weitere Angaben, ggf. auf einem Ergänzungsblatt.

Verpflichtungserklärung (natürliche Person) gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz

Geheimschutzbetreutes Unternehmen:

(Name, Anschrift Sitz des betroffenen geheimschutzbetreuten Unternehmens)

1. Verpflichtungserklärung der betroffenen Person

Name:

Vorname:

Geburtsdatum:

Geburtsort:

Staatsangehörigkeit:

Als Inhaber/in / Gesellschafter/in / Geschäftsführer/in / Vorstand *(zutreffendes bitte unterstreichen)* des oben genannten, vom Bundesministerium für Wirtschaft und Klimaschutz geheimschutzbetreuten Unternehmens (im Folgenden „Unternehmen"), erkläre ich, dass

a) mir bewusst ist, dass ich nicht befugt bin, Kenntnis von Informationen zu nehmen, die im Sicherheitsinteresse der Bundesrepublik Deutschland, anderer Nationen oder internationaler Organisationen als Verschlusssachen eingestuft und als solche mit einem Geheimhaltungsgrad gekennzeichnet sind;

b) ich keine Kenntnis von solchen Informationen nehmen oder zu erlangen versuchen werde;

c) ich keine Anweisungen erteilen werde, welche die ordnungsgemäße Umsetzung der Geheimschutzbestimmungen beim Unternehmen beeinflussen und/oder sogar behindern könnten und

d) ich über diese Verpflichtung und meine fehlende VS-Ermächtigung die anderen Gesellschafter/innen / Mitglieder der Geschäftsleitung bzw. des Vorstands des Unternehmens unterrichten werde.

Ich bin mir bewusst, dass

a) Mitarbeiter/innen des Unternehmens arbeitsrechtliche oder vertragsrechtliche sowie strafrechtliche Konsequenzen drohen können, wenn sie Verschlusssachen Unbefugten offenbaren,

b) im Fall einer Nichteinhaltung dieser Verpflichtung dem Unternehmen der Sicherheitsbescheid entzogen und es aus der Geheimschutzbetreuung entlassen werden kann und mir selbst vertragsrechtliche und strafrechtliche Konsequenzen drohen können.

,

…….……..…… …….

Datum, Ort Unterschrift

2. Erklärung des/der Sicherheitsbevollmächtigte/n (SiBe) und des/der ständigen Vertreters/Vertreterin vor Ort

Als Sicherheitsbevollmächtigte/r und ständige/r Vertreter/in vor Ort des geheimschutzbetreuten Unternehmens haben wir von dieser Erklärung Kenntnis genommen.

Zur Erfüllung der Pflicht des Unternehmens zur Einhaltung der Vorgaben des Geheimschutzhandbuchs wirken wir darauf hin, dass die unterzeichnende Person keine Kenntnis von Verschlusssachen erhält. Wir werden die VS-Ermächtigten des Unternehmens entsprechend belehren.

Wir werden das Bundesministerium für Wirtschaft und Klimaschutz unverzüglich über alle Vorkommnisse informieren, welche auf eine Nichteinhaltung der vorstehenden Verpflichtung hindeuten könnten.

,

…….……

Datum, Ort

…… …….

Name (Sicherheitsbevollmächtigte/r) Unterschrift

…… …….

Name (ständige/r Vertreter/in vor Ort) Unterschrift

Verpflichtungserklärung der Gesellschafterin (juristische Person oder rechtsfähige Personengesellschaft) gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz

Geheimschutzbetreutes (Tochter)unternehmen:

(Name, Anschrift Sitz des betroffenen geheimschutzbetreuten Unternehmens)

1. Verpflichtungserklärung der Gesellschafterin

Gesellschafterin (umfasst auch Aktionärin):

(Name, Anschrift Sitz der Gesellschafterin)

Vertreten durch:

(Name, Funktion und Anschrift des/der Vertreter/in der Gesellschafterin)

Die Gesellschafterin

a) bestätigt die alleinige Verantwortung des geheimschutzbetreuten (Tochter)unternehmens (im Folgenden: „Unternehmen“) für die Durchführung von Verschlusssachenaufträgen,

b) bestätigt, nicht befugt zu sein, Kenntnis von Informationen zu nehmen, die im Sicherheitsinteresse der Bundesrepublik Deutschland, anderer Nationen oder internationaler Organisationen als Verschlusssachen eingestuft und als solche mit einem Geheimhaltungsgrad gekennzeichnet sind;

c) wird keine Kenntnis von solchen Informationen nehmen oder zu erlangen versuchen;

d) wird keine Anweisungen erteilen, welche die ordnungsgemäße Umsetzung der Geheimschutzbestimmungen beim Unternehmen beeinflussen und/oder sogar behindern könnten und

e) wird über diese Verpflichtung die anderen Gesellschafter/innen unterrichten.

Der Gesellschafterin ist bewusst, dass

a) Mitarbeiter/innen des Unternehmens arbeitsrechtliche oder vertragsrechtliche sowie strafrechtliche Konsequenzen drohen können, wenn sie Verschlusssachen Unbefugten offenbaren,

b) im Fall einer Nichteinhaltung dieser Verpflichtung dem geheimschutzbetreuten Unternehmen die Sicherheitsbescheide entzogen und es aus der Geheimschutzbetreuung entlassen werden kann sowie der Gesellschafterin vertragliche Konsequenzen drohen könnten,

,

…….……..…… ……
Datum, Ort Unterschrift

2. Erklärung des/der Sicherheitsbevollmächtigten (SiBe) und des/der ständigen Vertreter/s/in vor Ort beim geheimschutzbetreuten (Tochter)unternehmen

Als Sicherheitsbevollmächtigte/r und ständige/r Vertreter/in vor Ort des geheimschutzbetreuten (Tochter)unternehmens haben wir von dieser Erklärung Kenntnis genommen.
Zur Erfüllung der Pflicht des Unternehmens zur Einhaltung der Vorgaben des Geheimschutzhandbuchs wirken wir darauf hin, dass die Gesellschafterin keine Kenntnis von Verschlusssachen erhält. Wir werden die VS-Ermächtigten des Unternehmens entsprechend belehren.
Wir werden das Bundesministerium für Wirtschaft und Klimaschutz unverzüglich über alle Vorkommnisse informieren, welche auf eine Nichteinhaltung der vorstehenden Verpflichtung des beteiligten Unternehmens hindeuten können.

,

…….……
Datum, Ort

…… ……
Name (Sicherheitsbevollmächtigte/r) Unterschrift

…… ……
Name (ständige/r Vertreter/in vor Ort) Unterschrift

Geheimschutzmaßnahmen für die Behandlung von VS-Schriftgut bzw. VS-Material (Kategorien)

Die nach 2.4.1 Absatz 2 GHB im Sicherheitsbescheid aufzuführenden Kategorien werden wie folgt beschrieben:

Kategorie A - Personelle Geheimschutzmaßnahmen

VS-ermächtigtes Personal ist gemäß den folgenden Untergruppen vorhanden:

Kategorie A 1	Personal bis VS-VERTRAULICH ermächtigt
Kategorie A 2	Personal bis GEHEIM ermächtigt
Kategorie A 3	Personal bis STRENG GEHEIM ermächtigt
Kategorie A 4	Personal mit der Berechtigung zum Zugang zu Krypto-Informationen
Kategorie A 5	Personal mit Verpflichtung im Bereich der Fernmeldeaufklärung der Bundeswehr (FmAufkl Bw)

Kategorie B - Aufbewahrungsmöglichkeiten für VS

Im Unternehmen sind folgende Voraussetzungen für die Aufbewahrung von Verschlusssachen (VS) gegeben:

Kategorie B 1	Bankschließfach zur Aufbewahrung von VS-VERTRAULICH
Kategorie B 2	VS-Verwahrgelass zur vorübergehenden Aufbewahrung; Hinterlegung der VS im Bankschließfach
Kategorie B 3	VS-Verwahrgelass; ständig personell bewacht oder technisch überwacht
Kategorie B 4	Aktensicherungsraum, der besonderen Sicherheitsanforderungen entspricht, ständig personell bewacht oder technisch überwacht
Kategorie B 5	VS-Sperrzone zur Aufbewahrung von VS-Schriftgut/Kleinteilen; ständig personell bewacht oder technisch überwacht
Kategorie B 6	VS-Sperrzone zur Aufbewahrung von VS-Großteilen; ständig personell bewacht oder technisch überwacht

Kategorie C - Bearbeitungsmöglichkeiten für VS

Im Unternehmen sind folgende Voraussetzungen für die Bearbeitung von VS vorhanden:

Kategorie C 1	VS-Kontrollzone; vorübergehend aktiviert
Kategorie C 2	VS-Kontrollzone; ständig aktiviert
Kategorie C 3	VS-Kontrollzone; ständig personell bewacht oder technisch überwacht
Kategorie C 4	VS-Sperrzone zur Bearbeitung von VS-Schriftgut/Kleinteilen
Kategorie C 5	VS-Sperrzone zur Bearbeitung von VS-Großteilen

Kategorie D - Besondere Schutzvorkehrungen für VS

Im Unternehmen sind folgende besondere Schutzvorkehrungen für VS gegeben:

Kategorie D 1	Abhörgeschützter Raum
Kategorie D 2	Abhörsicherer Raum
Kategorie D 3	Abstrahlsichere(r) Kabine/Raum zur IT-VS-Bearbeitung
Kategorie D 4	Kryptobetriebsstelle

Kategorie E - IT-VS-Bearbeitung

Im Unternehmen wird VS auf IT-Systemen nach folgenden Grundsätzen bearbeitet:

Kategorie E 1	IT-Systeme für VS-VERTRAULICH ohne Maßnahmen zur Abstrahlsicherheit
Kategorie E 2	IT-Systeme für GEHEIM ohne Maßnahmen zur Abstrahlsicherheit
Kategorie E 3	IT-Systeme für VS-VERTRAULICH mit Maßnahmen zur Abstrahlsicherheit
Kategorie E 4	IT-Systeme für GEHEIM mit Maßnahmen zur Abstrahlsicherheit

GHB - Anlage 13

Notification of a Classified Subcontract (Auftragsanzeige Ausland)

Contractor: **BMWK RegistrationNumber:**

Bundesministerium für Wirtschaft und Klimaschutz
Referat RS 3 | 53107 Bonn

Subject: Notification of a classified subcontract

1	**Program/Project**	**name** **contract number** **(or other identification / number)** **date**	
1.1	**Prime Contractor**	**name** **prime contract number**	
1.2	**Previous Subcontractor (if any)**	**name** **sub-contract number**	
1.3	**Request for Proposal** **identification number**		
2	**Contractor**	**(to let the contract)**	
3	**Is this a follow-up contract?** **If yes, please complete the following:**	**preceding contractor name** **contract number** **(or other identification / number)** **date**	☐ yes ☐ no
4	**Prime contractor** **Subcontractor**	**name, address** **name, address**	
5	**Does a classification list exist?**		☐ yes ☐ no
6	**Highest level of classification**		☐ R ☐ C ☐ S
7	**Contracting officer (if known)**		
8	**Remarks:**		
9	**Please note: If the contract contains a Security Aspects Letter or a Security Requirements Clause please submit it to BMWK together with this notification.**		

Erklärung beim Erlöschen der Ermächtigung zum Zugang zu Verschlusssachen (VS)

1. Erklärung der/des betroffenen Person

Herr/Frau geb. am:

(Name, Vorname)

a) Mir ist eröffnet worden, dass die mir vom Bundesministerium für Wirtschaft und Klimaschutz erteilte Ermächtigung zum Zugang zu VS mit Wirkung vom erlischt/erloschen ist.
Ich bin erneut darüber unterrichtet worden, dass meine **Verpflichtung zur Geheimhaltung** der mir bekannt gewordenen VS **durch das Erlöschen meiner Ermächtigung** zum Zugang zu VS nicht berührt wird, sondern **fortbesteht**. Auch durch Veröffentlichungen in Presse, Rundfunk oder Fernsehen u. ä. werde ich von der Geheimhaltungspflicht nicht befreit, es sei denn, dass mir eine solche Befreiung ausdrücklich vom Herausgeber der VS schriftlich erteilt wird. Ich erkläre, dass ich weder VS oder damit zusammenhängendes geheimhaltungsbedürftiges Material irgendwelcher Art noch Schlüssel zu VS-Verwahrgelassen, in denen sich VS befinden, in Besitz oder Gewahrsam habe. Die Annahme neuer VS werde ich verweigern. Auf die Bestimmungen der §§ 93 ff und § 353 b Abs. 2 Strafgesetzbuch und die **Möglichkeit der Bestrafung bei Verletzung der Geheimhaltungspflicht** bin ich erneut hingewiesen worden.

b) Ich bin darüber informiert worden, dass ich gegenüber dem/der Sicherheitsbevollmächtigten und dem Bundesministerium für Wirtschaft und Klimaschutz eine **schriftliche Erklärung** abgeben muss, **falls ich eine verlängerte Aufbewahrung meiner Sicherheitsakten wünsche**.

Zusätzlich für Ü2 oder Ü3-ermächtigte Personen
[Bei Ü2/Ü3 ist Zutreffendes durch den/die SiBe anzukreuzen, bei Ü1 ist Punkt c durchzustreichen.]

c) Ich bin darüber unterrichtet worden, dass meine **Anzeige- und Berichtspflichten für Reisen in Staaten, für die Reisebeschränkungen gelten** (vgl. „Staatenliste Reisebeschränkungen“; primär Staaten im Einflussbereich der Russischen Föderation), auch **nach dem Erlöschen meiner Ermächtigung** zum Zugang zu VS (Ü2/Ü3) **fortbestehen** für einen Zeitraum

☐ von einem Jahr oder

☐ von drei Jahren.

Diese Pflichten erlöschen nur insoweit vorzeitig, als das z.B. im Falle eines Arbeitgeberwechsels erneut ein VS-Einsatz in einer sicherheitsempfindlichen Tätigkeit erfolgt und die o.g. Anzeige- und Berichtspflichten in gleichem Umfang auch dort bestehen.

, den

.....
Unterschrift der betroffenen Person

2. Erklärung des/der Sicherheitsbevollmächtigten

☐ Über die Bedeutung der vorstehenden Erklärung habe ich den/die Unterzeichner/in heute eingehend belehrt. Er/Sie hat die Erklärung in meiner Gegenwart unterschrieben.

☐ Dem/Der Betroffenen wurde die Erklärung per Einschreiben Rückschein mit der Bitte zugesandt, diese unterschrieben zurückzusenden.

, den

.....
Unterschrift des/der Sicherheitsbevollmächtigten

Veränderungsmeldung

Betriebs-Nr. (einzusetzen von dem/der Sicherheitsbevollmächtigten)	

Anschrift des Unternehmens

Bundesministerium für
Wirtschaft und Klimaschutz
- Referat ZC3 -
z.Hd.
53107 Bonn

Betreff: Geheimschutz in der Wirtschaft
hier: **Veränderungsmeldung**

Anlage:

Name	**Vorname**
Geburtsdatum	**Kenn-Nr.:**

I. Abmeldung

☐ Für die betroffene Person wurde ein VS-Ermächtigungsantrag gestellt, aber ein Zugang zu Verschlusssachen ist nicht mehr vorgesehen (z.B. beim Ausscheiden aus dem Projekt oder dem Unternehmen; Versterben des Mitarbeiters). Der Antrag auf VS-Ermächtigung vom wird daher zurückgenommen.

☐ Für die betroffene Person wurde dem Unternehmen bereits die Ermächtigungsurkunde zugesandt, aber die Ermächtigung ist noch nicht vollzogen worden, da künftig ein Zugang zu Verschlusssachen für den/die Betroffene/n nicht mehr vorgesehen ist.

☐ Die **nicht unterschriebene** Ermächtigungsbestätigung und die Ermächtigungsurkunde sind als Anlagen beigefügt.

☐ Die VS-Ermächtigung (Ermächtigungsurkunde des Bundesministeriums für Wirtschaft und Klimaschutz vom) ist erloschen, da

- ☐ die VS-ermächtigte Person im Unternehmen seit dem nicht mehr mit Verschlusssachen befasst ist.
  - ☐ Sie ist unterrichtet, dass die Verpflichtung zur Geheimhaltung bekannt gewordener Verschlusssachen trotz des Erlöschens der VS-Ermächtigung fortbesteht.
  - ☐ Die "Erklärung beim Erlöschen der Ermächtigung zum Zugang zu Verschlusssachen" wurde unterschrieben und zu der Sicherheitsakte des Unternehmens genommen.
- ☐ die VS-ermächtigte Person ist am verstorben.

☐ Die VS-Ermächtigungsurkunde ist beigefügt.

II. sicherheitserhebliche Erkenntnisse

☐ Bei dem/der Betroffenen bzw. der einzubeziehenden Person haben sich sicherheitserhebliche Erkenntnisse ergeben.
(Bitte unter Bemerkungen oder auf gesondertem Blatt mitteilen)

III. Bei dem/der Betroffenen haben sich folgende Änderungen ergeben

☐ Eheschließung/Begründung einer Lebenspartnerschaft

☐ Eingehen/Wechsel einer auf Dauer angelegten Gemeinschaft

Eine **neu** ausgefüllte und unterschriebene Sicherheitserklärung ist beigefügt.

☐ Scheidung/Aufhebung einer Lebenspartnerschaft

☐ Getrenntleben des/der Betroffenen

☐ Änderung der Staatsangehörigkeit
(Erläuterung unter Bemerkungen; Nachweise sind beizufügen)

☐ Sonstige (Erläuterung unter Bemerkungen)

☐ Namensänderung des/der Betroffenen (Nachweise sind beizufügen)

Neuer Name:

Neuer Vorname:

☐ Namensänderung des/der Ehegatten/in, des/der Lebenspartners/in, des/der Lebensgefährten/in

Neuer Name:

Neuer Vorname:

☐ Wohnsitzänderung des/der Betroffenen

Neu: PLZ/Wohnort:

Neu: Straße/Hausnr.:

Bemerkungen:

Ort, Datum

Unterschrift des/der Sicherheitsbevollmächtigten

Vereinbarung zum Direktionsrecht bezüglich des/der Sicherheitsbevollmächtigten und dessen/deren Mitarbeiter/innen für den Einsatz in einem verbundenen Unternehmen (kapitalmäßige Beteiligung, Konzernzugehörigkeit)

.....
(Beschäftigungsunternehmen)

Herrn/Frau.....

.....

.....

.....
(Sicherheitsbevollmächtigter/e und seine/ihre Mitarbeiter/innen)

Betr.: Ihr Arbeitsverhältnis

Sie sind eine arbeitsrechtliche Bindung[1] mit dem Unternehmen

.....
eingegangen.

Soweit Sie im Rahmen Ihrer Tätigkeit Aufgaben des Geheimschutzes in der Wirtschaft für dieses Unternehmen wahrnehmen, unterstehen Sie dem alleinigen Direktionsrecht dieses Unternehmens.

Im übrigen bleiben Ihre Rechte und Pflichten aus Ihrem Arbeitsverhältnis unberührt.

Ort, Datum

Unterschrift Geschäftsleitung des Beschäftigungsunternehmens

[1] oder Abordnung

Vereinbarung zwischen Beschäftigungsunternehmen und verbundenem Unternehmen

(kapitalmäßige Beteiligung/Konzernzugehörigkeit)

Zwischen:

.....

(Beschäftigungsunternehmen)

und

.....

(verbundenem Unternehmen)

1. Die Aufgaben des personellen Geheimschutzes bzw. der VS-Verwaltung werden von folgenden Mitarbeitern/innen des Beschäftigungsunternehmens wahrgenommen.

   Herrn/Frau.....

   .....

   .....

   .....

   (Sicherheitsbevollmächtigter/e und seine/ihre Mitarbeiter/innen)

2. Soweit die oben genannten Personen im Rahmen Ihrer Tätigkeit Aufgaben des Geheimschutzes in der Wirtschaft für dieses Unternehmen wahrnehmen, unterstehen Sie dem alleinigen Direktionsrecht der Geschäftsleitung des verbundenen Unternehmens.

Ort, Datum	Unterschrift Geschäftsleitung des Beschäftigungsunternehmens
Ort, Datum	Unterschrift Geschäftsleitung des verbundenen Unternehmens

Merkblatt zu § 25 Abs. 3 Satz 2 des
Sicherheitsüberprüfungsgesetzes (SÜG)

Im Zusammenhang mit meiner - beabsichtigten - Ermächtigung zum Zugang zu Verschlusssachen bin ich auf folgenden Sachverhalt hingewiesen worden:

Das Bundesministerium für Wirtschaft und Klimaschutz hat für das Unternehmen/die Niederlassung/die Betriebsstätte - in dem/der ich beschäftigt bin, eine Ausnahme gemäß § 25 Abs. 3 Satz 2 des SÜG zugelassen. Dies bedeutet, dass der/die – stellvertretende/örtliche - Sicherheitsbevollmächtigte zugleich Aufgaben der Personalverwaltung wahrnimmt. Mir ist bekannt, dass ich mich wegen dieses Sachverhaltes unmittelbar an die

Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

wenden kann.

_____

Datum Unterschrift

_____

§ 25 Abs. 2 SÜG:
Die Aufgaben der nicht-öffentlichen Stelle nach diesem Gesetz sind grundsätzlich von einer von der Personalverwaltung getrennten Organisationseinheit wahrzunehmen. Die zuständige Stelle kann Ausnahmen zulassen, wenn die nicht-öffentliche Stelle sich verpflichtet, Informationen, die ihr im Rahmen der Sicherheitsüberprüfung bekannt werden, nur für solche Zwecke zu gebrauchen, die mit der Sicherheitsüberprüfung verfolgt werden.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:
Tel.: 0228-997799-0, Fax: 0228-997799-550,
E-Mail: poststelle@bfdi.bund.de, Internet: www.bfdi.bund.de

GHB - Anlage 19a

Antrag auf VS-Ermächtigung

Betriebs-Nr. (von dem/der Sicherheitsbevollmächtigten einzusetzen)		Anschrift des antragstellenden Unternehmens

Bundesministerium für Wirtschaft und Klimaschutz
- Referat ZC3 -
z.Hd.
53107 Bonn

Die Sicherheitsüberprüfung soll durchgeführt werden aus Gründen

☐ des Schutzes von Verschlusssachen,
☐ des vorbeugenden personellen Sabotageschutzes,
☐ der Satellitendatensicherheit.

Personenangaben der betroffenen Person

Name:			
Vorname(n):			
Geburtsdatum:		**Geburtsort:**	
Kenn-Nr. (soweit bekannt):			

Die betroffene Person ist

☐ Mitarbeiter/in des antragstellenden Unternehmens.
☐ Fremdmitarbeiter/in (Ziff. 4.3.5 GHB) und beschäftigt als
  ☐ freier/e Mitarbeiter/in (es besteht eine vertragliche Vereinbarung mit dem antragstellenden Unternehmen, z.B. Werk- oder Dienstvertrag).
  ☐ Mitarbeiter/in des nachstehenden Unternehmens (bitte die genaue Unternehmensangabe einsetzen).

Begründung für die Sicherheitsüberprüfung

Bei der durchzuführenden Sicherheitsüberprüfung handelt es sich um eine

☐ Erstüberprüfung / erneute Überprüfung.	☐ Regelmäßige Aktualisierung / Wiederholungsüberprüfung. Akt./Wü-Nr.:	☐ Sicherheitsüberprüfung aus besonderem Anlass (bitte unter Bemerkungen erläutern).

Die betroffene Person soll im Rahmen ihrer Tätigkeit Zugang erhalten zu

☐ STRENG GEHEIM	☐ GEHEIM	☐ VS-VERTRAULICH
oder einer hohen Anzahl	☐ GEHEIM	☐ VS-VERTRAULICH

eingestuften/eingestufter Verschlusssachen oder kann sich Zugang dazu verschaffen.

☐ Die betroffene Person wird an folgendem/folgenden VS-Auftrag/VS-Aufträgen lt. VS-Auftragsmeldung (Ziff. 3.3.2 GHB) eingesetzt: (bitte die lfd. Nr./Nrn. der VS-Auftragsmeldung angeben oder die VS-Auftragsbezeichnung):

☐ Es handelt sich um eine Sicherheitsüberprüfung von Unternehmensorganen bzw. von sonstigem Funktionspersonal (z.B. Geschäftsführer, Sicherheitsbevollmächtigter bzw. dessen Stellvertreter, VS-Verwalter):

☐	Die Sicherheitsüberprüfung soll aus anderen Gründen erfolgen (z.B. besondere Anforderung einer amtlichen Stelle). Bitte ausführlich begründen und ggf. Anforderungsschreiben als Anlage beifügen.
☐	Die betroffene Person soll in besonderen sicherheitsempfindlichen Programmen (z.B. Fernmeldeaufklärung) eingesetzt werden. Bezeichnung des Programms:

Vorgeschlagene Art der Überprüfung (Ziff. 4.2.1 GHB)	☐	Ü1	☐	Ü2	☐ Ü3

Antrag für besondere Ermächtigungen

☐	**Vorläufige Ermächtigung** (Ziff. 4.3.2 GHB): Es wird eine vorläufige Ermächtigung beantragt. Die besondere Dringlichkeit ist ausführlich unter sonstige Bemerkungen begründet worden.
☐	**Mehrfachermächtigung** (Ziff. 4.3.3 GHB): Die betroffene Person ist bereits VS-ermächtigt für (Unternehmen) Betriebs-Nr.: | Kenn-Nr.: | Geheimhaltungsgrad: und soll für das antragstellende Unternehmen eine zusätzliche VS-Ermächtigung erhalten (Begründung auf besonderem Blatt bzw. unter sonstigen Bemerkungen)
☐	**Sofortermächtigung** (Ziff. 4.3.4 GHB): Es wird eine Sofortermächtigung beantragt. ☐ Es wurde eine neue Sicherheitserklärung von der betroffenen Person ausgefüllt und diesem Antrag beigefügt.

Frühere Sicherheitsüberprüfungen (soweit bekannt)

Zuständige Behörde für eine frühere Sicherheitsüberprüfung war:		
Die Sicherheitsüberprüfung ist für folgendes Unternehmen bzw. öffentliche Stelle durchgeführt worden:		
ggf. Betriebs-Nr.:	ggf. Kenn-Nr.:	Geheimhaltungsgrad:

Bestätigungen des Sicherheitsbevollmächtigten

☐	Die Notwendigkeit der VS-Ermächtigung ist geprüft worden und wird bejaht. Die betroffene Person ist für den Zugang zu VS geeignet und nach hiesiger Einschätzung überprüfbar. Die Sicherheitserklärung wurde geprüft.
☐	Das Einverständnis der betroffenen Person und ggf. der in die Sicherheitsüberprüfung einzubeziehenden Person (mitbetroffene Person) liegt durch persönliche Unterschrift in der Sicherheitserklärung vor.
☐	Die Kopie der Sicherheitserklärung wurde zur Sicherheitsakte genommen.

Sonstige Bemerkungen (z.B. Feststellung sicherheitserheblicher Erkenntnisse bei der betroffenen oder mitbetroffenen Person):

,

Ort, Datum

Name des/der Sicherheitsbevollmächtigten

Tel.-Nr.

Unterschrift des/der Sicherheitsbevollmächtigten

Anlage:

GHB - Anlage 19b

Az (wird vom BMWK eingetragen)

vorgesehene Verwendung (wird vom SiBe eingetragen)

Wichtiger Hinweis!

1. Beachten Sie bitte die „Anleitung zum Ausfüllen der Sicherheitserklärung für eine einfache Sicherheitsüberprüfung (Ü1)“ und lesen Sie erst die jeweiligen Erläuterungen zu den nachstehenden Fragen bevor Sie diese beantworten.
2. Machen Sie Ihre Angaben bitte
   - mittels **PC** oder
   - in **gut lesbaren Druckbuchstaben in schwarzer Farbe (nur im Ausnahmefall).**
3. Alle Felder sind verpflichtend auszufüllen! "Keine“ oder „entfällt“ dürfen nur angekreuzt werden, wenn tatsächlich keine Informationen vorliegen.

Anders ausgefüllte Vordrucke können aus Gründen der Datenverarbeitung nicht angenommen werden.

Sicherheitserklärung für die einfache Sicherheitsüberprüfung (Ü1)

Zutreffendes bitte ankreuzen bzw. ausfüllen [X]

1. Angaben zu Ihrer Person			aktuelles Lichtbild ***verpflichtend***
1.1 Personalien			
Name			
ggf. früherer Name (z.B. Geburtsname, frühere Ehenamen etc.)	☐ keine		
Vorname(n)			
ggf. frühere(r) Vorname(n)	☐ keine	**Jahr der Aufnahme:**	
Geburtsdatum (TT/MM/JJJJ)			
Geburtsort, Kreis, Bundesland, Staat			
gegenwärtige Staatsangehörigkeit(en)			
frühere Staatsangehörigkeit(en)	☐ keine	☐ ja, bitte angeben: (bitte Nachweis beifügen)	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers
Familienstand/auf Dauer angelegte Gemeinschaft	☐ ledig ☐ getrennt lebend ☐ verheiratet ☐ verwitwet	☐ Lebenspartnerschaft ☐ geschieden/aufgehobene Lebenspartnerschaft ☐ Lebenspartner/in verstorben	☐ auf Dauer angelegte Gemeinschaft
ausgeübter Beruf			
Arbeitgeberin/Arbeitgeber (Anschrift, Vorwahl, Rufnummer oder E-Mail-Adresse)			

1.2 Wohnsitze/Aufenthalte in Deutschland

- von längerer Dauer als zwei Monaten in den letzten **fünf Jahren** (in zeitlicher Reihenfolge)
- **einschließlich derzeitiger Anschrift, sofern sie in Deutschland liegt (ansonsten siehe Nr. 1.3)**

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Bundesland)	**Hauptwohnsitz**	
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**

1.3 Wohnsitze/Aufenthalte im Ausland

- von längerer Dauer als zwei Monaten seit Vollendung des 18. Lebensjahres, in jedem Fall aber in den vergangenen fünf Jahren
- soweit nicht unter Nr. 6.1, 6.2 – Wohnsitze in Staaten gemäß §13 Abs. 1 Nr. 17 SÜG – anzugeben

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Staat)	**Anlass des Aufenthalts**

2. Angaben zu Ihrer Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihrem Ehegatten/Lebenspartner/Lebensgefährten			
☐ **entfällt**			
Name			
ggf. frühere(r) Name(n) (z.B. Geburtsname, frühere Ehenamen, etc.)	☐ keine		
Vorname(n)			
ggf. frühere(r) Vorname(n)	☐ keine		
Geburtsdatum (TT/MM/JJJJ)			
Geburtsort, Kreis, Bundesland, Staat			
gegenwärtige Staatsangehörigkeit(en)			
frühere Staatsangehörigkeit(en)	☐ keine	☐ ja, bitte angeben: (bitte Nachweis beifügen)	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers

3. Angaben zu weiteren Personen über 18 Jahren, die mit Ihnen in einem Haushalt leben						
☐ **entfällt**						
	Person 1			**Person 2**		
Name (ggf. auch frühere Namen, z.B. Geburtsname, frühere Ehenamen)						
Vorname(n)						
Beziehung (z.B. Kind)						
Geburtsdatum (TT/MM/JJJJ)						
Geburtsort, Kreis, Bundesland, Staat						
gegenwärtige Staatsangehörigkeit(en)						
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers	☐ weiblich	☐ männlich	☐ divers

	Person 3			**Person 4**		
Name (ggf. auch frühere Namen, z.B. Geburtsname, frühere Ehenamen)						
Vorname(n)						
Beziehung (z.B. Kind)						
Geburtsdatum (TT/MM/JJJJ)						
Geburtsort, Kreis, Bundesland, Staat						
gegenwärtige Staatsangehörigkeit						
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers	☐ weiblich	☐ männlich	☐ divers

4. Angaben zur finanziellen Situation	
4.1 Sind Sie in der Lage, Ihren finanziellen Verpflichtungen nachzukommen und sind auch keine Veränderungen absehbar, die dies in Frage stellen?	
☐ ja	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 11)
4.2 Sind in den letzten fünf Jahren Zwangsvollstreckungsmaßnahmen gegen Sie erfolgt? Laufen oder liefen in den letzten fünf Jahren Insolvenzverfahren für Sie?	
☐ ja, ggf. nähere Angaben (bitte entsprechende Unterlagen beifügen)	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 11)

5. Kontakte zu ausländischen Nachrichtendiensten oder zu Nachrichtendiensten der ehemaligen DDR, die auf einen Anbahnungs- oder Werbungsversuch hindeuten können	
Sind Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte in irgendeiner Form angesprochen, angeschrieben oder sonst kontaktiert worden, die vermuten lässt, dass durch einen ausländischen Nachrichtendienst oder einen Nachrichtendienst der ehemaligen DDR eine nachrichtendienstliche Beziehung angeknüpft werden sollte?	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 11)
☐ siehe nähere Angaben:	

6. Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG (s. beigefügte Staatenliste)

6.1 Wohnsitze/Aufenthalte in diesen Staaten

Haben oder hatten Sie Wohnsitz(e) oder Aufenthalt(e) in einem dieser Staaten?

☐ nein ☐ ja, bitte nähere Angaben:

Dauer von bis (Monat/Jahr)	(Monat/Jahr)	Wohnsitze/Aufenthalte (Straße, Hausnummer, PLZ, Ort, Staat)	Anlass

6.2 Reisen/Sonstige Aufenthalte

Haben Sie Reisen in oder durch diese Staaten unternommen oder sich aus anderen Gründen dort aufgehalten?

☐ nein	☐ ja, bitte nähere Angaben:	
Dauer von bis (Datum) (Datum)	Ziel (Ort, Staat)	Anlass der Reise/des Aufenthaltes (z.B. Urlaub, Verwandtenbesuch, Dienstgeschäft, Montageaufenthalt, etc.)

6.3 Nahe Angehörige

Haben Sie nahe Angehörige in einem dieser Staaten?
(ausgenommen sind Personen, die sich im amtlichen Auftrag der Bundesrepublik Deutschland dort aufhalten)

☐ nein	☐ ja, bitte nähere Angaben:

6.4 Sonstige Beziehungen

Haben Sie sonstige Beziehungen in einen dieser Staaten **oder zu außerhalb des Gebietes dieser Staaten lebenden** Vertreterinnen/Vertretern eines solchen Staates?

☐ nein	☐ ja, bitte nähere Angaben:

7. Beziehungen zu verfassungsfeindlichen Organisationen

Sind oder waren Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte Mitglied in einer für verfassungswidrig erklärten oder anderen verfassungsfeindlichen Organisation? Besteht oder bestand eine anderweitige Beziehung zu einer solchen Organisation?

☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 11)

8. Anhängige Strafverfahren einschließlich Ermittlungsverfahren und Disziplinarverfahren, strafrechtliche Verurteilungen im Ausland

8.1 Anhängige Verfahren

Ist zurzeit ein Strafverfahren und/oder ein Ermittlungsverfahren und/oder Disziplinarverfahren gegen Sie anhängig?

☐ nein	☐ ja, bitte nähere Angaben:

8.2 Verurteilungen im Ausland

Wurden Sie im Ausland strafrechtlich verurteilt?

☐ nein	☐ ja, bitte nähere Angaben:

9. Sonstiges		
9.1 Sind Ihnen sonstige Umstände bekannt, die für die Sicherheitsüberprüfung von Bedeutung sein können?		
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 11)	
9.2 Wurde für Sie bereits früher eine Zuverlässigkeits- bzw. Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz durchgeführt?		
☐ nein	☐ ja, (soweit Ihnen bekannt)	
am (Datum)	**von, Anlass der Überprüfung** (Behörde oder Stelle, die die Überprüfung durchgeführt hat)	**Überprüfungsart**

10. Ergänzende Angaben	
☐ keine	
zu Nr.	

11. Gewünschtes persönliches Gespräch	
☐ nein	
Ich möchte ein Gespräch mit	
☐ der/dem Sicherheitsbevollmächtigten	☐ einer Vertreterin/einem Vertreter des Bundesamtes für Verfassungsschutz (BfV)

12. Erreichbarkeit		
Ich bin erreichbar: **(diese Felder bitte immer ausfüllen)**		
beruflich: (Uhrzeit von - bis)	Telefon: (Vorwahl, Rufnummer)	E-Mail-Adresse:
privat: (Uhrzeit von - bis)	Telefon: (Vorwahl, Rufnummer)	E-Mail-Adresse:

Ich habe die vorstehenden Angaben unter Berücksichtigung der "Anleitung zum Ausfüllen der einfachen Sicherheitserklärung" gemacht. Sie erfolgten nach bestem Wissen wahrheitsgemäß und vollständig.

Meiner Sicherheitsüberprüfung stimme ich zu.

Sollten mir künftig Umstände bekannt werden, die auf einen Anbahnungs- oder Werbungsversuch eines ausländischen Nachrichtendienstes (insbesondere von Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG) hindeuten, ist mir bewusst, dass ich diese unverzüglich mitteilen sollte, da eine unterlassene oder verspätete Mitteilung im Zweifel das Vorliegen eines Sicherheitsrisikos begründen kann. Gleiches gilt für neue Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG (s. beigefügte Staatenliste) und sonstige sicherheitsrelevante Umstände, die Gegenstand dieser Sicherheitserklärung sind.

Änderungen des Familienstandes, zu einer auf Dauer angelegten Gemeinschaft, des Namens, des Vornamens, des Geschlechtseintrages, des Wohnsitzes und der Staatsangehörigkeit werde ich unverzüglich mitteilen.

Ich bin mir bewusst, dass ich im Falle meiner Betrauung mit einer sicherheitsempfindlichen Tätigkeit als Geheimnisträger/in wegen meiner evt in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG lebenden nahen Angehörigen im Hinblick auf die dortigen Nachrichtendienste einer Gefährdung ausgesetzt sein könnte. Dies gilt gleichermaßen für die evtl. dort lebenden Angehörigen. Mir ist bekannt, dass meine evtl. sonstigen Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG u.U. gleiche Gefährdungen zur Folge haben könnten. Ich bin dennoch bereit, mich mit einer sicherheitsempfindlichen Tätigkeit betrauen zu lassen.

Ich bin mir bewusst, dass im Falle meiner Betrauung mit einer sicherheitsempfindlichen Tätigkeit jede private und dienstliche Reise, insbesondere in oder durch Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG, mit einer nachrichtendienstlichen Gefährdung verbunden sein kann.

Ort, Datum, Unterschrift der zu überprüfenden Person

Anfragen an ausländische Sicherheitsbehörden bei unter Nr. 1.3 angegebenen Auslandsaufenthalten von ununterbrochen längerer Dauer als sechs Monaten in den vergangenen fünf Jahren stimme ich zu.

zusätzlich bei früheren und jetzigen Wohnsitzen im Ausland:
Ort, Datum, Unterschrift der zu überprüfenden Person

Einverständniserklärung der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/Lebensgefährten zu den Angaben zu ihrer oder seiner Person:

Die Angaben zu meiner Person wurden mit meinem Einverständnis gemacht.

Ort, Datum, Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/ Lebensgefährten

Ergänzung der Angaben nach fünf Jahren bzw. auf besondere Anforderung

Ich habe meine Angaben im Vordruck „Sicherheitserklärung für die einfache Sicherheitsüberprüfung (Ü1)“ überprüft und ergänzt, soweit sich Änderungen ergeben haben. Ergänzungen zu Ziffer(n):

habe ich am Rand farblich gekennzeichnet.

Ggf. weitere Anmerkungen:

Persönliches Gespräch

☐ Ich benötige kein persönliches Gespräch.

☐ Ich wünsche ein Gespräch mit

- der/dem Sicherheitsbevollmächtigten
- einer Vertreterin/einem Vertreter des Bundesamtes für Verfassungsschutz (BfV)

Ort/Datum/Unterschrift der zu überprüfenden Person

Anfragen an ausländische Sicherheitsbehörden bei unter Ziffer 1.3 ergänzten Auslandsaufenthalten von ununterbrochen längerer Dauer als <u>sechs Monaten</u> in den vergangenen <u>fünf Jahren</u> stimme ich zu.

Ort/Datum/Unterschrift der zu überprüfenden Person -zusätzlich bei früheren und aktuellen Wohnsitzen im Ausland-

<u>Einverständniserklärung der Ehegattin/Lebenspartnerin/Lebensgefährtin bzw. des Ehegatten/Lebenspartners/Lebensgefährten:</u>

Die Angaben zu meiner Person wurden überprüft. Ergänzungen, soweit sie sich ergeben haben, erfolgten mit meinem Einverständnis.

Ort/Datum/Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin bzw. des Ehegatten/Lebenspartners/Lebensgefährten

GHB - Anlage 19c

Az (wird vom BMWK eingetragen)

vorgesehene Verwendung (wird vom SiBe eingetragen)

Wichtiger Hinweis!

1. Beachten Sie bitte die „Anleitung zum Ausfüllen der Sicherheitserklärung für die erweiterte Sicherheitsüberprüfung (Ü2) und für die erweiterte Sicherheitserklärung mit Sicherheitsermittlungen (Ü3)" und lesen Sie erst die jeweiligen Erläuterungen zu den nachstehenden Fragen bevor Sie diese beantworten.
2. Machen Sie Ihre Angaben bitte
   - mittels **PC** oder
   - in **gut lesbaren Druckbuchstaben in schwarzer Farbe (nur im Ausnahmefall).**
3. Alle Felder sind verpflichtend auszufüllen!
   "Keine" oder „entfällt" dürfen nur angekreuzt werden, wenn tatsächlich keine Informationen vorliegen.

Anders ausgefüllte Vordrucke können aus Gründen der Datenverarbeitung nicht angenommen werden.

Sicherheitserklärung für die

☐ **erweiterte Sicherheitsüberprüfung (Ü2)**

☐ **erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3)**
(die Art der Überprüfung wird vom BMWK festgelegt)

Zutreffendes bitte ankreuzen bzw. ausfüllen [X]

1. Angaben zu Ihrer Person			aktuelles Lichtbild *verpflichtend*
1.1 Personalien			
Name			
ggf. frühere(r) Name(n) (z.B. Geburtsname, frühere Ehenamen etc.)	☐ keine		
Vorname(n)			
ggf. frühere(r) Vorname(n)	☐ keine	**Jahr der Aufnahme:**	
Geburtsdatum (TT/MM/JJJJ)			
Geburtsort, Kreis, Bundesland, Staat			
gegenwärtige Staatsangehörigkeit(en)			
frühere Staatsangehörigkeit(en)	☐ keine	☐ ja, bitte angeben: (bitte Nachweis beifügen)	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers
Familienstand/auf Dauer angelegte Gemeinschaft:	☐ ledig ☐ getrennt lebend ☐ verheiratet ☐ verwitwet	☐ Lebenspartnerschaft ☐ geschieden / aufgehobene Lebenspartnerschaft ☐ Lebenspartner/in verstorben	☐ auf Dauer angelegte Gemeinschaft
Nummer des Personalausweises: ausstellende Behörde: Ausstellungsdatum:	**oder**	Nummer des Reisepasses: ausstellende Behörde: Ausstellungsdatum:	
ausgeübter Beruf			
Arbeitgeberin/Arbeitgeber (Anschrift, Vorwahl, Rufnummer oder E-Mail-Adresse)			

1.2 Wohnsitze/Aufenthalte in Deutschland

- von längerer Dauer als zwei Monate in den letzten **fünf Jahren** (in zeitlicher Reihenfolge)
- **einschließlich derzeitiger Anschrift, sofern sie in Deutschland liegt** (ansonsten siehe Nr. 1.3)

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Bundesland)	**Hauptwohnsitz**	
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**

1.3 Wohnsitze/Aufenthalte im Ausland

- von längerer Dauer als zwei Monaten seit Vollendung des 18. Lebensjahres, in jedem Fall aber in den vergangenen fünf Jahren
- soweit nicht unter Nr. 8.1 – Wohnsitze in Staaten gemäß §13 Abs. 1 Nr. 17 SÜG – anzugeben

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Staat)	**Anlass des Aufenthalts**

2. Angaben zu Ihrer Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihrem Ehegatten/Lebenspartner/Lebensgefährten			
☐ **entfällt**			
Name			
ggf. früherer Name (z.B. Geburtsname, frühere Ehenamen etc.)	☐ keine		
Vorname(n)			
ggf. frühere(r) Vorname(n)	☐ keine		
Geburtsdatum (TT/MM/JJJJ)			
Geburtsort, Kreis, Bundesland, Staat			
gegenwärtige Staatsangehörigkeit(en)			
frühere Staatsangehörigkeit(en)	☐ keine	☐ ja, bitte angeben: (bitte Nachweis beifügen)	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers

Nummer des Personalausweises: **oder** ausstellende Behörde: Ausstellungsdatum:	Nummer des Reisepasses: ausstellende Behörde: Ausstellungsdatum:
ausgeübter Beruf	
Arbeitgeberin/Arbeitgeber (Anschrift, Vorwahl, Rufnummer oder E-Mail-Adresse)	

2.2 Wohnsitze/Aufenthalte in Deutschland

- von längerer Dauer als zwei Monate in den letzten **fünf Jahren** (in zeitlicher Reihenfolge)
- **einschließlich derzeitiger Anschrift, sofern sie in Deutschland liegt** (ansonsten siehe Nr. 2.3)

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Bundesland)	**Hauptwohnsitz**	
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**
			☐ **ja**	☐ **nein**

2.3 Wohnsitze/Aufenthalte im Ausland

- von längerer Dauer als zwei Monaten seit Vollendung des 18. Lebensjahres, in jedem Fall aber in den vergangenen fünf Jahren
- soweit nicht unter Nr. 8.2 – Wohnsitze in Staaten gemäß §13 Abs. 1 Nr. 17 SÜG – anzugeben

☐ **keine**

von (Monat/Jahr)	**bis** (Monat/Jahr)	**Wohnsitz/Aufenthalt** (Straße, Hausnummer, PLZ, Ort, Staat)	**Anlass des Aufenthalts**

3. Weitere Personalien

3.1 Angaben zu den weiteren Personen über 18 Jahren, die mit Ihnen in einem Haushalt leben

☐ **entfällt**

	1. Person			**2. Person**		
Name (ggf. auch frühere Namen, z.B. Geburtsname, frühere Ehenamen)						
Vorname(n)						
Beziehung (z.B. Kind)						
Geburtsdatum (TT/MM/JJJJ)						
Geburtsort, Kreis, Bundesland, Staat						
Staatsangehörigkeit(en)						
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers	☐ weiblich	☐ männlich	☐ divers
	3. Person			**4. Person**		
Name (ggf. auch frühere Namen, z.B. Geburtsname, frühere Ehenamen)						
Vorname(n)						
Beziehung (z.B. Kind)						
Geburtsdatum (TT/MM/JJJJ)						
Geburtsort, Kreis, Bundesland, Staat						
Staatsangehörigkeit(en)						
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers	☐ weiblich	☐ männlich	☐ divers

3.2 Angaben zu Ihrem Vater		
☐ verstorben (bitte auch dann die Personalien – ohne Wohnsitz – angeben)		
Name		
ggf. früherer Name (z.B. Geburtsname, frühere Ehenamen, etc.)	☐ keine	
Vorname(n)		
Geburtsdatum (TT/MM/JJJJ)		
Geburtsort, Kreis, Bundesland, Staat		
Staatsangehörigkeit		
Wohnsitz (Straße, Hausnummer, PLZ, Ort)		
3.3 Angaben zu Ihrer Mutter		
☐ verstorben (bitte auch dann die Personalien – ohne Wohnsitz – angeben)		
Name		
ggf. früherer Name (z.B. Geburtsname, frühere Ehenamen, etc.)	☐ keine	
Vorname(n)		
Geburtsdatum (TT/MM/JJJJ)		
Geburtsort, Kreis, Bundesland, Staat		
Staatsangehörigkeit		
Wohnsitz (Straße, Hausnummer, PLZ, Ort)		

4. Ihre Ausbildung, Beschäftigung, Nichtbeschäftigung, Wehr-, Bundesfreiwilligen- und Zivildienst seit der Schulentlassung			
Schulentlassung: (Monat / Jahr)		Name, Bezeichnung und Anschrift der Ausbildungsstätte/ Beschäftigungsstelle; bei Nichtbeschäftigung: Aufenthaltsort, sofern der jeweilige Zeitraum **ununterbrochen** mehr als drei Monate umfasst; bei Wehr-/Bundesfreiwilligen-/Zivildienst: Standort/Dienstort	tätig als
Dauer			
von (Monat/Jahr)	**bis** (Monat/Jahr)		

5. Angaben zur Internetpräsenz bzw. Mitgliedschaften bzw. Teilnahme in sozialen Netzwerken	
5.1 Betreiben Sie eine oder mehrere eigene Internetseite(n)?	
☐ nein	☐ ja, bitte nähere Angaben:
5.2 Bestehen Mitgliedschaften in sozialen Netzwerken (z.B. Facebook, Twitter etc.)	
☐ nein	☐ ja, bitte nähere Angaben:

6. Angaben zur finanziellen Situation	
6.1 Sind Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte in der Lage, Ihren finanziellen Verpflichtungen nachzukommen und sind auch keine Veränderungen absehbar, die dies in Frage stellen?	
☐ ja	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 13)
6.2 Sind in den letzten fünf Jahren Zwangsvollstreckungsmaßnahmen gegen Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihren Ehegatten/Lebenspartner/Lebensgefährten erfolgt? Laufen oder liefen in den letzten fünf Jahren Insolvenzverfahren für Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihren Ehegatte/Lebenspartner/Lebensgefährten?	
☐ ja, (bitte entsprechende Unterlagen beifügen)	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 13)

7. Kontakte zu ausländischen Nachrichtendiensten oder zu Nachrichtendiensten der ehemaligen DDR, die auf einen Anbahnungs- oder Werbungsversuch hindeuten können	
Sind Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte in irgendeiner Form angesprochen, angeschrieben oder sonst kontaktiert worden, die vermuten lässt, dass durch einen ausländischen Nachrichtendienst oder einen Nachrichtendienst der ehemaligen DDR eine nachrichtendienstliche Beziehung angeknüpft werden sollte?	
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 13)
☐ siehe nähere Angaben:	

8. Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG (s. beigefügte Staatenliste)

8.1 Wohnsitze/Aufenthalte in diesen Staaten

Haben oder hatten Sie Wohnsitz(e) oder Aufenthalt(e) in einem dieser Staaten?

☐ nein ☐ ja, bitte nähere Angaben:

Dauer von bis (Monat/Jahr)	(Monat/Jahr)	**Wohnsitze/Aufenthalte** (Straße, Hausnummer, PLZ, Ort, Staat)	**Anlass**

8.2 Wohnsitze/Aufenthalte Ihrer Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihres Ehegatten/Lebenspartners/Lebensgefährten in diesen Staaten

Hat oder hatte Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte Wohnsitz(e) oder Aufenthalt(e) in einem dieser Staaten?

☐ nein ☐ ja, bitte nähere Angaben:

Dauer von bis (Monat/Jahr)	(Monat/Jahr)	**Wohnsitze/Aufenthalte** (Straße, Hausnummer, PLZ, Ort, Staat)	**Anlass**

8.3 Reisen / sonstige Aufenthalte

Haben Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte Reisen in oder durch diese Staaten unternommen oder sich aus anderen Gründen dort aufgehalten?

☐ nein ☐ ja, bitte nähere Angaben:

Dauer von (Datum)	bis (Datum)	**Ziel** (Ort, Staat) **und Anlass der Reise/des Aufenthaltes** (z.B. Urlaub, Verwandtenbesuch, Dienstgeschäft, Montageaufenthalt etc.)	**Von wem** wurde die Reise/ der Aufenthalt durchgeführt?

8.4 Nahe Angehörige

Haben Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte nahe Angehörige in einem dieser Staaten? (ausgenommen sind Personen, die sich im amtlichen Auftrag der Bundesrepublik Deutschland dort aufhalten)

☐ nein	☐ ja, bitte nähere Angaben:

8.5 Sonstige Beziehungen

Haben Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte sonstige Beziehungen in einen dieser Staaten **<u>oder</u> zu außerhalb des Gebiets dieser Staaten lebenden Vertreterinnen/Vertretern eines solchen Staates?**

☐ nein	☐ ja, bitte nähere Angaben:

9. Beziehungen zu verfassungsfeindlichen Organisationen

Sind oder waren Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte Mitglied in einer für verfassungswidrig erklärten oder anderen verfassungsfeindlichen Organisation? Besteht oder bestand eine anderweitige Beziehung zu einer solchen Organisation?

☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 13)

10. Anhängige Strafverfahren einschließlich Ermittlungsverfahren und Disziplinarverfahren, strafrechtliche Verurteilungen im Ausland

10.1 Anhängige Verfahren

Ist zurzeit ein Strafverfahren und/oder ein Ermittlungsverfahren und/oder Disziplinarverfahren gegen Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihren Ehegatten/Lebenspartner/Lebensgefährten anhängig?

☐ nein	☐ ja, bitte nähere Angaben:

10.2 Verurteilungen im Ausland

Wurden Sie, Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte im Ausland strafrechtlich verurteilt?

☐ nein	☐ ja, bitte nähere Angaben:

11. Sonstiges		
11.1 Sind Ihnen sonstige Umstände bekannt, die für die Sicherheitsüberprüfung von Bedeutung sein können?		
☐ nein	☐ Ich bitte um ein Gespräch. (siehe Nr. 13)	
11.2 Wurde für Sie bereits früher eine Zuverlässigkeits- bzw. Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgestz (SÜG) durchgeführt?		
☐ nein	☐ ja, (soweit Ihnen bekannt)	
am (Datum)	**von, Anlass der Überprüfung** (Behörde oder Stelle, die die Überprüfung durchgeführt hat)	**Überprüfungsart**

12. Referenzpersonen Nur anzugeben bei der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3)			
erste Referenzperson			
bekannt seit (Jahr)			
Art des Kontaktes			
Name			
Vorname(n)			
Geburtsdatum (TT/MM/JJJJ)		**Geburtsort, Kreis, Bundesland, Staat**	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers
ausgeübter Beruf			
berufliche Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	
private Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	

zweite Referenzperson			
bekannt seit (Jahr)			
Art des Kontaktes			
Name			
Vorname(n)			
Geburtsdatum (TT/MM/JJJJ)		**Geburtsort, Kreis, Bundesland, Staat**	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers
ausgeübter Beruf			
berufliche Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	
private Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	
dritte Referenzperson			
bekannt seit (Jahr)			
Art des Kontaktes			
Name			
Vorname(n)			
Geburtsdatum (TT/MM/JJJJ)		**Geburtsort, Kreis, Bundesland, Staat**	
Geschlechtseintrag	☐ weiblich	☐ männlich	☐ divers
ausgeübter Beruf			
berufliche Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	
private Anschrift (Straße, Hausnummer, PLZ, Ort)			
Telefon (Vorwahl, Rufnummer)		**E-Mail-Adresse**	

13. Gewünschtes persönliches Gespräch	
☐ **nein**	
Ich möchte ein Gespräch mit	
☐ der/dem Sicherheitsbevollmächtigten	☐ einer Vertreterin/einem Vertreter des Bundesamtes für Verfassungsschutz (BfV)

14. Ergänzende Angaben	
keine	
zu Nr.	

15. Erreichbarkeit		
Ich bin erreichbar: **(diese Felder bitte immer ausfüllen)**		
beruflich: (Uhrzeit von - bis)	Telefon: (Vorwahl, Rufnummer)	E-Mail-Adresse:
privat: (Uhrzeit von - bis)	Telefon: (Vorwahl, Rufnummer)	E-Mail-Adresse:

Ich habe die vorstehenden Angaben unter Berücksichtigung der "Anleitung zum Ausfüllen der Sicherheitserklärung für die erweiterte Sicherheitsüberprüfung und die erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen" gemacht. Sie erfolgten nach bestem Wissen wahrheitsgemäß und vollständig.

Meiner Sicherheitsüberprüfung stimme ich zu.

Sollten mir künftig Umstände bekannt werden, die auf einen Anbahnungs- oder Werbungsversuch eines ausländischen Nachrichtendienstes (insbesondere von Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG) hindeuten, ist mir bewusst, dass ich diese unverzüglich mitteilen sollte, da eine unterlassene oder verspätete Mitteilung im Zweifel das Vorliegen eines Sicherheitsrisikos begründen kann. Gleiches gilt für neue Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG (s. beigefügte Staatenliste) und sonstige sicherheitsrelevante Umstände, die Gegenstand dieser Sicherheitserklärung sind.

Änderungen des Familienstandes, zu einer auf Dauer angelegten Gemeinschaft, des Namens, des Vornamens, des Geschlechtseintrages, des Wohnsitzes und der Staatsangehörigkeit werde ich unverzüglich mitteilen.

Ich bin mir bewusst, dass ich im Falle meiner Betrauung mit einer sicherheitsempfindlichen Tätigkeit als Geheimnisträger/-in wegen meiner evtl. in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG lebenden nahen Angehörigen im Hinblick auf die dortigen Nachrichtendienste einer Gefährdung ausgesetzt sein könnte. Dies gilt gleichermaßen für die evtl. dort lebenden Angehörigen. Mir ist bekannt, dass meine evtl. sonstigen Beziehungen in Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG u.U. gleiche Gefährdungen zur Folge haben könnten. Ich bin dennoch bereit, mich mit einer sicherheitsempfindlichen Tätigkeit betrauen zu lassen.

Ich bin mir bewusst, dass im Falle meiner Betrauung mit einer sicherheitsempfindlichen Tätigkeit jede private und dienstliche Reise, insbesondere in oder durch Staaten gemäß § 13 Abs. 1 Nr. 17 SÜG, mit einer nachrichtendienstlichen Gefährdung verbunden sein kann.

Ort, Datum, Unterschrift der zu überprüfenden Person

Anfragen an ausländische Sicherheitsbehörden bei unter Nr. 1.3 angegebenen Auslandsaufenthalten von ununterbrochen längerer Dauer als sechs Monaten in den vergangenen fünf Jahren stimme ich zu.

zusätzlich bei früheren und jetzigen Wohnsitzen im Ausland:
Ort, Datum, Unterschrift der zu überprüfenden Person

Zustimmung der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/Lebensgefährten:

Ich stimme zu, dass ich in die Sicherheitsüberprüfung meiner Ehegattin/Lebenspartnerin/Lebensgefährtin oder meines Ehegatten/Lebenspartners/ Lebensgefährten einbezogen werde. Mir ist bekannt, dass über mich hierbei erhobene Daten gespeichert werden.

Ort, Datum Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/ Lebensgefährten

Anfragen an ausländische Sicherheitsbehörden bei unter Nr. 2.3 angegebenen Auslandsaufenthalten von ununterbrochen längerer Dauer als sechs Monaten in den vergangenen fünf Jahren stimme ich zu.

Ort, Datum, Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/ Lebensgefährten

Ergänzung der Angaben nach fünf Jahren bzw. auf besondere Anforderung

Ich habe meine Angaben im Vordruck „Sicherheitserklärung für die erweiterte Sicherheitsüberprüfung (Ü2)/ erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü3)“ überprüft und ergänzt, soweit sich Änderungen ergeben haben. Ergänzungen zu Ziffer(n): _____ habe ich am Rand farblich gekennzeichnet.

Ggf. weitere Anmerkungen:

Persönliches Gespräch

☐ Ich benötige kein persönliches Gespräch.

☐ Ich wünsche ein Gespräch mit

- der/dem Sicherheitsbevollmächtigten
- einer Vertreterin/einem Vertreter des Bundesamtes für Verfassungsschutz (BfV)

_____

Ort/Datum/Unterschrift der zu überprüfenden Person

Anfragen an ausländische Sicherheitsbehörden bei unter Ziffer 1.3 ergänzten Auslandsaufenthalten von ununterbrochen längerer Dauer als <u>sechs Monaten</u> in den vergangenen <u>fünf Jahren</u> stimme ich zu.

_____

Ort/Datum/Unterschrift der zu überprüfenden Person -zusätzlich bei früheren und aktuellen Wohnsitzen im Ausland-

<u>Einverständniserklärung der Ehegattin/Lebenspartnerin/Lebensgefährtin bzw. des Ehegatten/Lebenspartners/Lebensgefährten:</u>

Die Angaben zu meiner Person wurden überprüft. Ergänzungen, soweit sie sich ergeben haben, erfolgten mit meinem Einverständnis.

_____

Ort/Datum/Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin bzw. des Ehegatten/Lebenspartners/Lebensgefährten

Anfragen an ausländische Sicherheitsbehörden bei unter Ziffer 2.3 ergänzten Auslandsaufenthalten von ununterbrochen längerer Dauer als <u>sechs Monaten</u> in den vergangenen <u>fünf Jahren</u> stimme ich zu.

_____

-zusätzlich bei früheren und jetzigen Wohnsitzen im Ausland-

Ort / Datum / Unterschrift der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/Lebensgefährten

Beiblatt zur Sicherheitserklärung Ü1

gemäß § 12 Abs. 4 Sicherheitsüberprüfungsgesetz (SÜG)

Bitte nur ausfüllen/ankreuzen, wenn Sie
vor dem 1. Januar 1970 geboren wurden!

Bitte hier den Vornamen, Nachnamen und das Geburtsdatum der Person eintragen, welche die Sicherheitserklärung abgibt.

Haben Sie

- bis zum Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt? ja ☐ nein ☐
- vor dem Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt, jedoch das Gebiet nach dem 13. August 1961 (Mauerbau) verlassen? ja ☐ nein ☐

Ort, Datum, Unterschrift

Hinweis zum Beiblatt:
Nach § 12 Abs. 4 des Sicherheitsüberprüfungsgesetzes fragt das BMWK zur Feststellung einer hauptamtlichen Tätigkeit der betroffenen Person für den Staatssicherheitsdienst der ehemaligen DDR beim "Bundesarchiv" an, wenn die betroffene Person vor dem 1. Januar 1970 geboren wurde und in dem Gebiet der ehemaligen DDR wohnhaft war oder Anhaltspunkte für eine Tätigkeit für den Staatssicherheitsdienst der ehemaligen DDR vorliegen.
Sofern diese Voraussetzungen bei Ihnen vorliegen, werden Sie gebeten, für sich den "Antrag auf Feststellung einer eventuellen Tätigkeit für den Staatssicherheitsdienst der ehemaligen DDR" (Anlage 19e GHB) zu stellen.

Anlage 19d (2) GHB

Beiblatt zur Sicherheitserklärung Ü2/Ü3

gemäß § 12 Abs. 4 Sicherheitsüberprüfungsgesetz (SÜG)

Bitte nur ausfüllen/ankreuzen, wenn Sie und/oder Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte **vor dem 1. Januar 1970 geboren wurde(n)!**

Bitte hier den Vornamen, Nachnamen und das Geburtsdatum der Person eintragen, welche die Sicherheitserklärung abgibt.

1. Haben Sie

- bis zum Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt? ja ☐ nein ☐
- vor dem Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt, jedoch das Gebiet nach dem 13. August 1961 (Mauerbau) verlassen? ja ☐ nein ☐

2. Hat Ihre Ehegattin/Lebenspartnerin/Lebensgefährtin oder Ihr Ehegatte/Lebenspartner/Lebensgefährte

- bis zum Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt? ja ☐ nein ☐
- vor dem Beitritt der ehemaligen DDR zur Bundesrepublik Deutschland im Gebiet der ehemaligen DDR gewohnt, jedoch das Gebiet nach dem 13. August 1961 (Mauerbau) verlassen? ja ☐ nein ☐

Ort, Datum, Unterschrift

Hinweis zum Beiblatt:
Nach § 12 Abs. 4 des Sicherheitsüberprüfungsgesetzes fragt das BMWK zur Feststellung einer hauptamtlichen Tätigkeit der betroffenen Person oder der mitbetroffenen Person für den Staatssicherheitsdienst der ehemaligen DDR beim "Bundesarchiv" an, wenn die betroffene Person oder die mitbetroffene Person vor dem 1. Januar 1970 geboren wurde und in dem Gebiet der ehemaligen DDR wohnhaft war oder Anhaltspunkte für eine Tätigkeit für den Staatssicherheitsdienst der ehemaligen DDR vorliegen.
Sofern diese Voraussetzungen bei Ihnen oder der mitbetroffenen Person vorliegen, werden Sie gebeten, für sich und ggf. die mitbetroffenen Person den "Antrag auf Feststellung einer eventuellen Tätigkeit für den Staatssicherheitsdienst der ehemaligen DDR" (Anlage 19e GHB) zu stellen.

Antrag auf Feststellung einer eventuellen Tätigkeit für den Staatssicherheitsdienst der ehemaligen Deutschen Demokratischen Republik (DDR) für

Name, Vorname (ggf. Rufname)	Geburtsdatum
ggf. frühere Namen (z.B. Geburtsname, frühere Ehenamen) sowie alle Vornamen	
derzeitige Anschrift (Straße, Hausnummer, PLZ, Ort)	
Wohnanschrift(en) seit dem 18. Lebensjahr in der ehemaligen DDR (Straße, Hausnummer, PLZ, Ort) (Bei einer evtl. Umbenennung von Straßennamen nach dem 03.10.1990 im Beitrittsgebiet ist ggf. auch der ehemalige Straßenname anzugeben.)	

☐ Fortsetzung auf separatem Blatt

_____

Ort, Datum, Unterschrift der betroffenen Person oder der mitbetroffenen Person

Diesen Antrag bitte zusammen mit den übrigen Unterlagen zur Sicherheitsüberprüfung über den SiBe an das Bundesministerium für Wirtschaft und Klimaschutz senden.

Hinweise
zur Sicherheitsüberprüfung im Bereich Geheimschutz

Die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes sind im Sicherheitsüberprüfungsgesetz (SÜG) geregelt. Durch die folgenden Informationen soll eine kurze Zusammenfassung darüber gegeben werden, wer zu überprüfen ist, wozu die Sicherheitsüberprüfung dient und was sie im Wesentlichen umfasst. Für weitere Fragen steht die oder der Sicherheitsbevollmächtigte zur Verfügung.

Wer wird sicherheitsüberprüft?

Überprüft werden Personen, die eine Tätigkeit ausüben sollen, bei der sie Zugang zu geheimhaltungsbedürftigen Angelegenheiten erhalten oder sich verschaffen können und ihrer Sicherheitsüberprüfung zugestimmt haben (siehe § 1 Abs. 2 und § 2 Abs. 1 SÜG). Hierzu gehören z.B. Bearbeiterinnen und Bearbeiter von Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher.

Tätigkeiten der genannten Art werden als "sicherheitsempfindliche Tätigkeiten" bezeichnet.

Wozu dient eine Sicherheitsüberprüfung?

Ausländische Nachrichtendienste versuchen fortwährend auch an im staatlichen Interesse geheimhaltungsbedürftige Angelegenheiten zu gelangen (z.B. durch nachrichtendienstliche Anwerbung von Personen). Dies bedeutet eine ständige Gefahr für die Sicherheit der Bundesrepublik Deutschland, die nach dem Grundgesetz verpflichtet ist, für die innere und äußere Sicherheit des Landes und seiner Bürger zu sorgen.

Die Sicherheitsüberprüfung von Personen, die eine sicherheitsempfindliche Tätigkeit ausüben sollen, ist deshalb eine verfassungsgemäße Aufgabe und Pflicht.

Die Bundesrepublik Deutschland ist aber auch als Mitglied der NATO und anderer über- oder zwischenstaatlicher Organisationen verpflichtet, beim Austausch von Verschlusssachen mit den Partnerstaaten bestimmte Sicherheitsvorkehrungen auf dem Gebiet des personellen Geheimschutzes einzuhalten. Dies geschieht sowohl im nationalen Interesse der Bundesrepublik Deutschland als auch im Interesse der Sicherheit jedes einzelnen.

Mit einer sicherheitsempfindliche Tätigkeit darf daher nur betraut werden, wer zuvor auf seine Zuverlässigkeit hin überprüft wurde.

Durch die Sicherheitsüberprüfung soll individuell festgestellt werden, ob einer Person eine sicherheitsempfindliche Tätigkeit übertragen werden kann oder ob tatsächliche Anhaltspunkte vorliegen, die die Betrauung mit einer solchen Tätigkeit aus Gründen des staatlichen Geheimschutzes verbieten (sogenannte "Sicherheitsrisiken").

Sicherheitsrisiken sind gegeben, wenn tatsächliche Anhaltspunkte vorliegen, die

- Zweifel an der gebotenen Zuverlässigkeit bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen,
- eine besondere Gefährdung, insbesondere die Besorgnis einer Erpressbarkeit, bei möglichen Anbahnungs- oder Werbungsversuchen ausländischer Nachrichtendienste, extremistischer oder terroristischer Organisationen oder krimineller Vereinigungen, begründen,
- Zweifel begründen, dass eine Person sich zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes bekennt und bereit ist, jederzeit für deren Erhaltung einzutreten.

Ein Sicherheitsrisiko kann auch auf Grund tatsächlicher Anhaltspunkte zur mitbetroffenen Person, z.B. der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/Lebenspartners/ Lebensgefährten, gegeben sein.

Bei der Beurteilung, ob ein Sicherheitsrisiko vorliegt, sind die Umstände des Einzelfalles maßgebend. Auf ein Verschulden kommt es nicht an.

Welche Maßnahmen umfasst die Sicherheitsüberprüfung?

Es gibt drei Arten von Sicherheitsüberprüfungen, die einfache Sicherheitsüberprüfung (Ü 1), die erweiterte Sicherheitsüberprüfung (Ü 2) und die erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen (Ü 3).

Die jeweilige Art der durchzuführenden Sicherheitsüberprüfung richtet sich nach der Sicherheitsempfindlichkeit der Tätigkeit, die die betroffene Person wahrnehmen soll. Sie hängt grundsätzlich von der Höhe des Geheimhaltungsgrades der Verschlusssachen ab, zu denen Zugang gewährt werden soll oder sich Zugang verschafft werden kann.

Die Sicherheitsüberprüfung erfolgt durch das Bundesministerium für Wirtschaft und Klimaschutz über die/den Sicherheitsbevollmächtigte(n) unter Mitwirkung des Bundesamtes für Verfassungsschutz, das erforderliche Anfragen und Ermittlungen durchführt.

Die Grundlage für die Sicherheitsüberprüfung ist die von der betroffenen Person abgegebene "Sicherheitserklärung". Die Angabe personenbezogener Daten erfolgt auf freiwilliger Basis. Stimmt die betroffene Person ihrer Sicherheitsüberprüfung zu, ist sie zugleich auch verpflichtet, die in der Sicherheitserklärung geforderten Daten anzugeben.

Je nach Überprüfungsart kann die Sicherheitsüberprüfung u.a. noch folgende Maßnahmen umfassen:

- Prüfung der Angaben in der Sicherheitserklärung
- Einsicht der oder des Sicherheitsbevollmächtigten in die Personalakte der betroffenen Person (soweit vorhanden und zugänglich) sowie sonstige erforderliche Unterlagen
- Anfragen an das Bundeszentralregister, an das Zentrale staatsanwaltschaftliche Verfahrensregister, an Polizeibehörden und Nachrichtendienste
- Bei Bedarf Anfragen an das Archiv für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, an ausländische Sicherheitsbehörden oder das Ausländerzentralregister sowie an andere geeignete Stellen, ob und ggf. welche sicherheitsrelevanten Erkenntnisse über die betroffene Person vorliegen
- Einsicht in öffentlich sichtbare Internetseiten
- Einsicht in den öffentlich sichtbaren Teil sozialer Netzwerke bei der Ü2 und Ü3.
- Prüfung der Identität der betroffenen Person bei der Ü 2 und Ü 3
- Ermittlungen im näheren Lebensumfeld der betroffenen Person (z.B. Befragung der von ihr benannten Referenzpersonen), ob Hinweise auf Sicherheitsrisiken vorliegen, in der Regel bei der Ü 3
- Einbeziehung der Ehegattin/Lebenspartnerin/Lebensgefährtin oder des Ehegatten/ Lebenspartners/Lebensgefährten in die Sicherheitsüberprüfung bei der Ü 2 und Ü 3 mit deren/dessen Zustimmung
- Gespräch(e) mit der betroffenen Person über ihre persönliche Sicherheitssituation (soweit dies nach dem Ergebnis der Sicherheitsüberprüfung geboten erscheint)
- In bestimmten Zeitabständen sowie bei Bedarf eine Aktualisierung/Wiederholung der Sicherheitsüberprüfung oder einzelner Maßnahmen

Rechtsstaatliches Verfahren, Zweckbindung der Daten, Auskunftsrecht

Sicherheitsüberprüfungen werden unter Wahrung der rechtsstaatlichen Grundsätze durchgeführt. Die betroffene Person hat Anspruch, gehört zu werden, bevor der Zugang zu einer sicherheitsempfindlichen Tätigkeit abgelehnt oder aufgehoben wird. Zu der Anhörung kann sie eine Rechtsanwältin oder einen Rechtsanwalt beiziehen. Gegen die ablehnende oder aufhebende Entscheidung kann sie Rechtsmittel einlegen. Ehegattinnen/Lebenspartnerinnen/Lebensgefährtinnen oder Ehegatten/Lebenspartner/Lebensgefährten wird Gelegenheit gegeben sich zu äußern, wenn sich sicherheitserhebliche Erkenntnisse zu ihrer Person ergeben haben.

Die im Rahmen der Sicherheitsüberprüfung erhobenen personenbezogenen Daten dürfen von der zuständigen Stelle oder mitwirkenden Behörde nur für die mit der Sicherheitsüberprüfung verfolgten Zwecke, die mit sonstigen gesetzlich geregelten Überprüfungsverfahren zur Feststellung der Zuverlässigkeit verfolgten Zwecke, Zwecke der Verfolgung von Straftaten von erheblicher Bedeutung sowie Zwecke parlamentarischer Untersuchungsausschüsse genutzt und übermittelt werden.

Auf Antrag ist von der zuständigen Stelle oder mitwirkenden Behörde Auskunft zu erteilen, welche Daten über die anfragende Person im Rahmen der Sicherheitsüberprüfung gespeichert wurden.

Die "goldene Brücke" bei nachrichtendienstlicher Verstrickung

Jede oder jeder kann ohne eigenes Verschulden zum Zielobjekt ausländischer Nachrichtendienste werden. Wer Verrat begeht, schadet nicht nur seinem Land, sondern auch sich selbst. Häufig erkennen die betroffenen Personen aber zu spät, wofür sie missbraucht wurden.

Um aus einer nachrichtendienstlichen Verstrickung oder Verratstätigkeit mit möglichst geringem persönlichen Schaden herauszukommen, bleibt nur die Möglichkeit, sich bei den zuständigen Abwehrbehörden freiwillig zu offenbaren, da diese in einem solchen Falle grundsätzlich von einer Anzeige absehen können. Aber auch für das Strafverfahren und bei den Strafbestimmungen hat der Gesetzgeber "goldene Brücken" gebaut. Nach § 153 e der Strafprozessordnung und § 98 Abs. 2 des Strafgesetzbuches kann in solchen Fällen von einer Strafverfolgung oder Bestrafung abgesehen werden.

Nutzen Sie gegebenenfalls diese Möglichkeiten!

Ansprechpartnerinnen oder Ansprechpartner sind neben der oder dem Sicherheitsbevollmächtigten und den zuständigen Polizei- und Verfassungsschutzbehörden der Bundesländer folgende Bundesbehörden:

Bundesamt für Verfassungsschutz	Bundeskriminalamt	Der Generalbundesanwalt beim Bundesgerichtshof
Merianstraße 100 50765 Köln	65173 Wiesbaden	Brauerstraße 30 76135 Karlsruhe
0228-99/792-0 oder 030-18/792-0	0611/55-0	0721/8191-0

Straftaten von erheblicher Bedeutung

In §138 StGB und §3 des Artikel 10-Gesetzes – G 10 genannte Straftaten[1]

1.	§ 80 a.	Aufstacheln zum Verbrechen der Aggression.
2.	§ 81.	Hochverrat gegen den Bund.
3.	§ 82.	Hochverrat gegen ein Land.
4.	§ 83.	Vorbereitung eines hochverräterischen Unternehmens.
5.	§ 84.	Fortführung einer für verfassungswidrig erklärten Partei.
6.	§ 85.	Verstoß gegen ein Vereinigungsverbot.
7.	§ 86.	Verbreiten von Propagandamitteln verfassungswidriger Organisationen.
8.	§ 87.	Agententätigkeit zu Sabotagezwecken.
9.	§ 88.	Verfassungsfeindliche Sabotage.
10.	§ 89.	Verfassungsfeindliche Einwirkung auf Bundeswehr und Sicherheitsorgane.
11.	§ 89 a.	Vorbereitung einer schweren staatsgefährdenden Gewalttat.
12.	§ 89 b.	Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat.
13.	§ 89 c Absatz 1 bis 4	Terrorismusfinanzierung.
14.	§ 94.	Landesverrat.
15.	§ 95.	Offenbaren von Staatsgeheimnissen.
16.	§ 96.	Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen.
17.	§ 97 a.	Verrat illegaler Geheimnisse.
18.	§ 97 b.	Verrat in irriger Annahme eines illegalen Geheimnisses.
19.	§ 98.	Landesverräterische Agententätigkeit.
20.	§ 99.	Geheimdienstliche Agententätigkeit.
21.	§ 100.	Friedensgefährdende Beziehungen.
22.	§ 100 a.	Landesverräterische Fälschung.
23.	§ 109 e.	Sabotagehandlungen an Verteidigungsmitteln.
24.	§ 109 f.	Sicherheitsgefährdender Nachrichtendienst.
25.	§ 109 g.	Sicherheitsgefährdendes Abbilden.
26.	§ 129 a.	Bildung terroristischer Vereinigungen.
27.	§ 129 b.	Kriminelle und terroristische Vereinigungen im Ausland.
28.	§ 130.	Volksverhetzung.
29.	§ 146.	Geldfälschung.
30.	§ 151.	Wertpapiere.
31.	§ 152.	Geld, Wertzeichen und Wertpapiere eines fremden Währungsgebiets.
32.	§ 152 b Abs. 1 bis 3	Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks.
33.	§ 202 a.	Ausspähen von Daten (soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet).
34.	§ 202 b.	Abfangen von Daten (soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik

[1] **Paragraphen ohne Gesetzesbezeichnung sind solche des StGB.**

		Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet).
35.	§ 211.	Mord.
36.	§ 212.	Totschlag.
37.	§ 232 Abs. 3 Satz 2	Menschenhandel (soweit es sich um Verbrechen handelt).
38.	§ 232 a Abs. 3, 4 oder 5	Zwangsprostitution (soweit es sich um Verbrechen handelt).
39.	§ 232 b Abs. 3 oder 4	Zwangsarbeit (soweit es sich um Verbrechen handelt).
40.	§ 233 a Abs. 3 oder 4	Ausbeutung unter Ausnutzung einer Freiheitsberaubung (soweit es sich um Verbrechen handelt).
41.	§ 234.	Menschenraub.
42.	§ 234 a.	Verschleppung.
43.	§ 239 a.	Erpresserischer Menschenraub.
44.	§ 239 b.	Geiselnahme.
45.	§ 249.	Raub.
46.	§ 250.	Schwerer Raub.
47.	§ 251.	Raub mit Todesfolge.
48.	§ 255.	Räuberische Erpressung.
49.	§ 303 a.	Datenveränderung (soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet).
50.	§ 303 b.	Computersabotage (soweit sich die Straftat gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland, insbesondere gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richtet).
51.	§ 306.	Brandstiftung.
52.	§ 306 a.	Schwere Brandstiftung.
53.	§ 306 b.	Besonders schwere Brandstiftung.
54.	§ 306 c.	Brandstiftung mit Todesfolge.
55.	§ 307 Abs. 1 bis 3	Herbeiführen einer Explosion durch Kernenergie.
56.	§ 308 Abs. 1 bis 4	Herbeiführen einer Sprengstoffexplosion.
57.	§ 309 Abs. 1 bis 5	Missbrauch ionisierender Strahlen.
58.	§ 310.	Vorbereitung eines Explosions- oder Strahlungsverbrechens.
59.	§ 313.	Herbeiführen einer Überschwemmung.
60.	§ 314.	Gemeingefährliche Vergiftung.
61.	§ 315 Abs. 3	Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr.
62.	§ 315 b Abs. 3	Gefährliche Eingriffe in den Straßenverkehr.
63.	§ 316 a.	Räuberischer Angriff auf Kraftfahrer.
64.	§ 316 b Abs. 3	Störung öffentlicher Betriebe.
65.	§ 316 c.	Angriff auf den Luft- und Seeverkehr.
66.	§ 20 Abs. 1 Nr. 1-4 VereinsG.	Zuwiderhandlung gegen Verbote.
67.	§ 95 Abs. 1 Nr. 8 AufenthG.	Strafvorschriften.
68.	§ 6 Völkerstraf-Gesetzbuch (VStGB)	Völkermord.
69.	§ 7 VStGB	Verbrechen gegen die Menschlichkeit.
70.	§ 8 VStGB	Kriegsverbrechen gegen Personen.

71.	§ 9 VStGB	Kriegsverbrechen gegen Eigentum und sonstige Rechte.
72.	§ 10 VStGB	Kriegsverbrechen gegen humanitäre Operationen und Embleme.
73.	§ 11 VStGB	Kriegsverbrechen des Einsatzes verbotener Methoden der Kriegsführung.
74.	§ 12 VStGB	Kriegsverbrechen des Einsatzes verbotener Mittel der Kriegsführung.
75.	§ 13 VStGB	Verbrechen der Aggression.

Name, Vorname, Abteilung

Einverständniserklärung zur Weiterleitung personenbezogener Daten im Rahmen des Besuchskontrollverfahrens

Zum Zwecke des Besuchskontrollverfahrens gemäß Ziffer 5 des Geheimschutzhandbuches (GHB) erkläre ich mich gemäß § 51 Abs. 1 Bundesdatenschutzgesetz damit einverstanden, dass die personenbezogenen Daten (Name, Vorname, Geburtsdatum und –ort, Staatsangehörigkeit, Personalausweis- bzw. Reisepassnummer sowie Ort und Datum der Ausstellung, Überprüfungsart und Ermächtigungsgrad) erhoben, verarbeitet und genutzt werden. Ich stimme zu, dass diese Daten an die jeweils nach dem Besuchskontrollverfahren zuständigen Stellen im In- und Ausland weitergeleitet werden.

Diese Einverständniserklärung schließt auch eine elektronische Übermittlung der Daten mit ein, wenn hierfür vom Bundesministerium für Wirtschaft und Klimaschutz genehmigte IT-Anwendungen eingesetzt werden.

Diese Einwilligung kann gemäß § 51 Abs. 3 Bundesdatenschutzgesetz jederzeit mit Wirkung für die Zukunft widerrufen werden. Durch den Widerruf wird die Rechtmäßigkeit der Datenweitergabe für bereits erfolgte Besuchskontrollverfahren nicht berührt.

Ich bin darauf hingewiesen worden, dass die Verweigerung meines Einverständnisses dazu führt, dass eine Bestätigung meiner Ermächtigung zum Zugang zu Verschlusssachen (VS) gegenüber anderen Stellen im In- und Ausland nicht abgegeben werden kann. Damit ist mir eine auswärtige Bearbeitung eines VS-Auftrages nicht möglich.

Ort, Datum

Unterschrift

H I N W E I S

zum

**Widerspruchsrecht nach § 36a Abs. 2 Sicherheitsüberprüfungsgesetz (SÜG)
bezüglich der Kontrolle von Akten über die Sicherheitsprüfung
durch die oder den
Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI)**

Nach § 36a Abs. 2 SÜG kontrolliert die oder der BfDI bei den öffentlichen Stellen des Bundes und nichtöffentlichen Stellen die Einhaltung der Vorschriften des BDSG bzw. des SÜG und anderer Vorschriften über den Datenschutz. Sinn solcher Kontrollmaßnahmen ist es, dazu beizutragen, dass die oder der Einzelne beim Umgang mit ihren oder seinen personenbezogenen Daten nicht in ihrem oder seinem Persönlichkeitsrecht beeinträchtigt wird. § 36a Abs. 2 Satz 3 SÜG sieht vor, dass personenbezogene Daten in Akten über die Sicherheitsprüfung **dann der Kontrolle durch die oder den BfDI nicht unterliegen, wenn die betroffene Person der Kontrolle ihrer Daten im Einzelfall gegenüber der oder dem BfDI widerspricht.**

Betroffene Personen, die von diesem Recht Gebrauch machen wollen, werden auf folgendes hingewiesen:

Der Widerspruch ist nach dem Gesetzeswortlaut grundsätzlich gegenüber der oder dem BfDI einzulegen, die oder der ihn im Einzelfall zu beachten hat. Ein **an die oder den BfDI adressierter Widerspruch kann durch die Widerspruchsführerin oder den Widerspruchsführer aber auch zur Sicherheitsakte bei der oder dem Sicherheitsbevollmächtigten gegeben werden.** Die oder der BfDI wird auch solche Widersprüche berücksichtigen.

Der Widerspruch kann **auch auf die beim Bundesamt für Verfassungsschutz (BfV) geführte Sicherheitsüberprüfungsakte erstreckt werden.** Auch in diesem Fall ist der Widerspruch gegenüber der oder dem BfDI einzulegen. Die oder der BfDI wird allerdings auch solche Widersprüche beachten, die bei der oder dem **Sicherheitsbevollmächtigten** oder beim **BfV** eingelegt wurden und ihr oder ihm bekannt werden.

Durch die Beifügung des an die oder den BfDI adressierten Widerspruchs zur Sicherheitsakte/Sicherheitsüberprüfungsakte ist auf bestmöglichste Weise gewährleistet, dass die oder der BfDI bei einer Kontrolle den Widerspruch beachtet und im Interesse der betroffenen Person von einer Kontrolle ihrer personenbezogenen Daten absieht.

Merkblatt
Anleitung für die Geheimhaltung in der Wirtschaft

1. Allgemeines

Als Mitarbeiter/in Ihres Unternehmens, der/die zum Zugang zu staatlichen Geheimnissen (Verschlusssachen) ermächtigt ist oder Mitarbeiter/in in einem sicherheitsempfindlichen Bereich tragen Sie in besonderem Maße Verantwortung für die Sicherheit Ihrer Kollegen, des Unternehmens und der Bundesrepublik Deutschland. Diese Anleitung soll Ihnen ein Grundwissen über die wichtigsten Maßnahmen zum Schutz staatlicher Verschlusssachen sowie über mögliche Bedrohungen (Terrorismus, Extremismus, Kriminalität wie z.B. Konkurrenz-auspähung oder die Arbeitsweise fremder Nachrichtendienste) vermitteln.

Die Vorschriften zum Schutze von Verschlusssachen (VS) sind sorgfältig zu beachten. Einschränkungen, Unbequemlichkeiten oder Verzögerungen, die sich hierbei ergeben können, müssen hingenommen werden, damit der notwendige Schutz der VS, Ihres Unternehmens und der Mitarbeiter gewährleistet ist.

Auch nach den weltweiten politischen Veränderungen sind die Bundesrepublik Deutschland und ihre Unternehmen ein Ziel für fremde Nachrichtendienste für Konkurrenzausspähungen von Verschlusssachen/Staatsgeheimnissen. Diejenigen, die Verrat begehen, schaden dabei nicht nur unserem Land, ihrem Arbeitgeber oder den Kollegen, sondern auch sich selbst. Häufig erkennen sie erst viel zu spät, wofür sie missbraucht wurden.

Jeder kann ohne eigenes Verschulden zum Zielobjekt von Konkurenzunternehmen, terroristischen Organisationen oder fremder Nachrichtendienste werden.

Um aus einer nachrichtendienstlichen Verstrickung oder Verratstätigkeit anderer Art (z.B. leichtfertige Preisgabe von VS an Konkurrenzunternehmen oder leichtfertige Preisgabe der Funktionsweise von Sicherheitsvorkehrungen an terroristische Organisationen usw.) ohne persönlichen Schaden herauszukommen, bleibt nur die Möglichkeit der freiwilligen Offenbarung bei den zuständigen Behörden. Die Verfassungsschutzbehörden können in vielen Fällen von einer Anzeige absehen. Auch die strafrechtlichen Bestimmungen sehen vor, dass dann von einer Strafverfolgung abgesehen werden kann (§ 153 e Strafprozessordnung). Nutzen Sie diese Möglichkeit - in Ihrem Interesse und im Interesse unseres freiheitlichen Rechtsstaates.

Zentrale/r Ansprechpartner/in in allen Sicherheitsfragen für Sie ist der/die von Ihrer Geschäftsführung bestellte/r Sicherheitsbevollmächtigte/r (SiBe), an den/die Sie sich in allen Sicherheitsbelangen wenden können. Der/die SiBe unterliegt gegenüber der Geschäftsführung in personellen Geheimschutzangelegenheiten einer Schweigeverpflichtung.

2. Wozu Geheimschutz?

In einer freiheitlichen Demokratie ist staatliches Handeln auf Transparenz angelegt, so dass es grundsätzlich für jedermann offenkundig ist. Im Interesse der äußeren und inneren Sicherheit und des Schutzes der Wirtschaft und seiner Bürger muss aber auch der demokratische Staat bestimmte Informationen geheimhalten.

Die Bundesrepublik Deutschland ist Mitglied im weltweiten Bündnis zur Bekämpfung des Terrorismus und demzufolge ein potentielles Zielobjekt für Anschläge. Die leichtfertige Preisgabe z.B. des Aufbaues und der Funktionsweise von Sicherheitsvorkehrungen in Ihrem Unternehmen könnte derartige Anschläge ermöglichen oder erleichtern. Wenn darüber hinaus VS z.B. über den Bau von Kriegswaffen in die falschen Hände geraten, wäre dies ein erhebliches Gefährdungspotential für die weltweite Bekämpfung terroristischer Anschläge.

Konkurrenzunternehmen sind daran interessiert, das entsprechende Know-How Ihres Unternehmens zu erhalten, ohne sich durch teure und langwierige Forschungen usw. dieses Wissen zu erarbeiten. Als Mitarbeiter Ihres Unternehmens tragen sie auch Verantwortung für den Schutz dieser Informationen, insbesondere, wenn sie als VS eingestuft sind.

Die meisten Staaten betreiben „Auslandsaufklärung“ durch ihren Nachrichtendienst. Aus der Sicht der betroffenen Staaten ist dies Spionage, die wegen der möglichen politischen, militärischen und wirtschaftlichen Schäden unter erhebliche Strafe gestellt ist. Die Bundesrepublik Deutschland ist aufgrund ihrer wirtschaftlichen und politischen Bedeutung sowie ihrer geografischen Lage ein wichtiges Spionageziel fremder Nachrichtendienste.

Zum Schutz der VS werden Personen zur Feststellung der persönlichen Eignung zum Zugang zu VS einer Sicherheitsüberprüfung unterzogen. Die Sicherheitsüberprüfung von Personen richtet sich nach dem Sicherheitsüberprüfungsgesetz (§ 25 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes vom 20.04.1994 – BGBl. I Seite 867, zuletzt geändert durch Artikel 4 des Gesetzes vom 18.07.2017 (BGBl. I S. 2732), welches Mindestanforderungen berücksichtigt, zu denen die Bundesrepublik Deutschland auch gegenüber ausländischen Staaten und als Mitglied zwischenstaatlicher Einrichtungen (z.B. NATO, OCCAR) vertraglich oder im Rahmen der EU rechtlich verpflichtet ist.

Dabei müssen die Bestimmungen für den Schutz gespeicherter personenbezogener Daten aus dem Bundesdatenschutzgesetz berücksichtigt werden (Vgl. § 36 Abs. 1 und 2 SÜG).

3. Das Wichtigste zum Geheimschutz in Kürze

3.1. Begriff der Verschlusssache (VS)

VS sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform (z.B. Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, Magnetspeicher, elektrische Signale, Geräte oder technische Einrichtungen sowie das gesprochene Wort). Sie werden entsprechend ihrer Schutzwürdigkeit als STRENG GEHEIM, GEHEIM, VS-VERTRAULICH oder VS-NUR FÜR DEN DIENSTGEBRAUCH von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.

3.2. VS-Einstufung

Die Einstufung einer VS wird von einer amtlichen Stelle (Behörde) vorgenommen und wird Ihnen von Ihrem VS-Auftraggeber in einer VS-Einstufungsliste oder auf andere schriftliche Weise (z.B. bei einer geringen Zahl von einzustufenden VS) vorgegeben. Diese Vorgaben sind strikt einzuhalten und durchgehend zu berücksichtigen (auch bei künftigen Aufträgen Ihres Unternehmens, in die eine bereits früher als VS eingestufte Information einfließen soll). Sollte sich eine VS-Einstufung als nicht praktikabel erweisen, ist sofort Ihr/e SiBe zu informieren, der/die dies mit dem Auftraggeber und BMWK klärt.

3.3. Grundsatz „Kenntnis nur, wenn nötig“

Von VS, die VS-VERTRAULICH oder höher eingestuft sind, dürfen nur entsprechend sicherheitsüberprüfte und zum Zugang zu VS ermächtigte Personen Kenntnis erhalten.

Aber auch diese VS-Ermächtigten dürfen nur insoweit Kenntnis von VS erhalten, als dies zwingend für die Erledigung des Auftrages erforderlich ist. Dies und die Schweigepflicht gelten auch gegenüber den engsten Kolleginnen und Kollegen, auch persönlichen Vertrauenspersonen (Ehegatte/in, Lebenspartner/in, Lebensgefährte/in, Freunde, Ärzte usw.) dürfen niemals über den Inhalt von VS informiert werden.

In den meisten Spionage- oder sonstigen Verratsfällen hätte der Schaden wesentlich begrenzt werden können, wäre dieser Grundsatz „Kenntnis nur, wenn nötig“ beachtet worden.

3.4. Verschwiegenheit

Erörtern Sie VS oder sonstige wichtige Informationen nicht in Gegenwart Unbefugter oder in der Öffentlichkeit (Gaststätten, Eisenbahn, Flugzeuge usw). Nutzen Sie die von Ihrem/r SiBe eingerichteten (evtl. abhörsicheren oder abhörgeschützten) Besprechungsräume für Gespräche über VS bzw. die Kontroll- oder Sperrzonen zur Bearbeitung von VS und befolgen Sie genau alle hierfür erlassenen Anweisungen (z.B. Zugangskontrolle, Fotografier- und Handyverbot, offenes Tragen des Firmenausweises usw.).

3.5. Persönliche Verantwortung, Weitergabe von VS

VS-VERTRAULICH und höher eingestufte VS dürfen nur an VS-Ermächtigte über die VS-Registratur gegen Quittung weitergegeben werden. Eine Liste mit den Namen der VS-Ermächtigten Ihres Unternehmens befindet sich bei dem/der SiBe und bei dem/der VS-Verwalter/in. Für den Schutz einer von Ihnen bei der VS-Registratur empfangenen VS sind Sie persönlich verantwortlich. Sie müssen die VS dorthin sobald wie möglich zurückgeben. Eine evtl. Weitergabe an eine/n Kollegen/in im Unternehmen ist ebenfalls nur über die VS-Registratur zulässig. Sie werden dann dort entlastet und Ihr/e Kollege/in belastet.

Lassen Sie VS auch bei kürzerer Abwesenheit nicht unbeaufsichtigt an Ihrem Arbeitsplatz zurück, sondern sorgen Sie dafür, dass unbefugte Personen keine Kenntnis hiervon erhalten können. Einzelheiten hierzu wird Ihnen Ihr/e SiBe mitteilen.

Sollte Ihnen irrtümlich auf andere Weise als durch die VS-Registratur eine VS zugehen, sind Sie für deren Schutz ebenfalls persönlich verantwortlich und haben dies unverzüglich Ihrer VS-Registratur und dem/der SiBe zu melden.

Für die Weitergabe von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften VS gelten erleichterte Vorschriften. Erforderlich ist, dass der Empfänger anhand des VS-NfD-Merkblattes nachweisbar belehrt wurde, die Regeln einhält und verschwiegen ist. Der Grundsatz „Kenntnis nur, wenn nötig“ ist auch hier zu beachten. Fragen Sie hierzu Ihre/n SiBe.

3.6. Herstellung und Vervielfältigung von VS, VS-Zwischenmaterial (VS-VERTRAULICH und höher)

VS-VERTRAULICH oder höher eingestufte VS dürfen nur unter Einschaltung der VS-Registratur an dafür zugelassenen Stellen (Einzelzimmer, Kontroll- oder Sperrzonen usw.) gefertigt werden.

Bei der Herstellung oder Vervielfältigung anfallende Zwischen- und Nebenprodukte, die in irgend einer Form VS-Informationen enthalten (z.B. handschriftliche Entwürfe, Disketten) sind wie die VS selbst zu schützen und sofort der VS-Registratur anzuzeigen, die das Weitere festlegt.

3.7. Aufbewahrung, Versendung und Mitnahme von VS

VS-VERTRAULICH oder höher eingestufte VS sind in der VS-Registratur aufzubewahren. Für VS-NUR FÜR DEN DIENSTGEBRAUCH genügt die Aufbewahrung in einem abgeschlossenen Zimmer (Einzelschloss, keine Schließanlage) oder in einem abgeschlossenen Schrank oder Schreibtisch.

VS-VERTRAULICH oder höher eingestufte VS sind über die VS-Registratur außerhalb des Unternehmens zu versenden. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS können im Inland als gewöhnlicher Brief bzw. Paket versandt werden.

Die Bearbeitung von VS in der Privatwohnung ist untersagt. Die Mitnahme von VS auf Reisen und zu Besprechungen bedarf der Genehmigung des/der SiBe. Die persönliche Mitnahme von STRENG GEHEIM eingestuften VS ist unzulässig.

3.8. Nutzung der Informationstechnik

Bei Nutzung der Informationstechnik (Computer, Telefaxgerät usw.) für VS bestehen besondere Risiken.

Deshalb müssen vor der informationstechnischen Verarbeitung oder Übertragung von VS-VERTRAULICH oder höher eingestuften VS besondere Sicherheitsvorkehrungen getroffen werden und die Anwendung der Informationstechnik für den jeweiligen Geheimhaltungsgrad ausdrücklich durch BMWK freigegeben sein.

Elektronische Datenträger (Disketten, Wechselplatten usw.) unterliegen der Mehrfachnutzung. Hinsichtlich ihrer Kennzeichnung, Löschung und Vernichtung gelten besondere Bestimmungen. Wenden Sie sich an Ihren/e SiBe.

Wird Informationstechnik für die Verarbeitung oder Übertragung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufter VS genutzt, so sind zur Wahrung

der Vertraulichkeit geeignete Maßnahmen entsprechend dem „VS-NfD-Merkblatt“ zu treffen.

4. Was tun, wenn ... ?

Nachrichtendienste, terroristische oder kriminelle Organisationen aber auch Konkurrenzunternehmen haben viele Methoden, um bestimmte Personen für ihre Zwecke nutzbar zu machen. Bevor z.B. ein fremder Nachrichtendienst an Sie herantritt und sich für eine bestimmte Werbemethode entscheidet, wird er die Frage klären, wer Sie sind, welche Aufgaben Sie wahrnehmen oder künftig wahrnehmen könnten, welche Neigungen, Wünsche und Gewohnheiten Sie haben, wo Ihre besonderen Interessen (Theater, Freizeit, Hobby usw.) liegen, welche politischen Auffassungen Sie vertreten und ob Sie besondere Probleme oder Schwächen (finanzielle Schwierigkeiten, drohende Insolvenz, zu aufwendiger Lebensstil usw.) haben?

Das Ergebnis der Nachforschungen, die sich im Geheimen abspielen, bestimmt die Methode der geheimdienstlichen oder andersgelagerten Anwerbung.

Erhält ein/e Agent/in schließlich den Auftrag, Sie anzuwerben, weiß er/sie bestens über Sie Bescheid. Er/sie kennt Ihre Neigungen, Schwächen, Wünsche, Gewohnheiten.

Die Kontaktaufnahme mit Ihnen wird immer „rein zufällig“ erfolgen, ob im Café oder im Urlaub, ob auf einem abendlichen Empfang oder an Ihrer Haustür, ob über eine Zeitungsannonce oder einen unverfänglichen Briefwechsel. Bevor Sie zu einer Mitarbeit veranlasst werden, wird dieser Kontakt langfristig, auch über viele Jahre gepflegt und gefestigt.

Oft treten Agenten/Agentinnen unter sogenannter falscher Flagge auf, d.h. unter Vortäuschung der Mitarbeit für eine andere unverdächtige Stelle.

Ähnlich wie fremde Nachrichtendienste könnten auch fremde, bekannte oder vertraute Personen an Sie herantreten, die Ziele auf den Gebieten der Konkurrenzausspähung, Spionage oder des Terrorismus verfolgen.

Um Schwierigkeiten oder Gefahren für Ihre Kollegen/innen, Ihr Unternehmen oder sogar die Bundesrepublik Deutschland zu vermeiden, kommt es darauf an, eine solche Kontaktaufnahme rechtzeitig zu erkennen.

Jemand, für den Ihr Unternehmen interessanter ist als Sie selbst, dürfte wohl kein guter Freund sein. Ein/e Bekannte/r, der/die kein Verständnis dafür hat, dass Sie über geheimhaltungsbedürftige Angelegenheiten nicht sprechen, verdient nicht Ihren Respekt.

Jedem/r, der/die versucht, Sie zur Preisgabe vertraulicher Informationen zu überreden oder unter Missachtung von VS-Vorschriften zu „kleinen Gefälligkeiten“ zu bewegen, sollten Sie mit Vorsicht begegnen.

Gehen Sie den Dingen auf den Grund. Sucht der/die Bekannte wirklich Ihren Kontakt, Ihre Freundschaft, oder nur Informationen?

Wenden Sie sich, falls Zweifel oder Fragen bleiben, vertrauensvoll an Ihre/n SiBe oder auch an das Bundesamt für Verfassungsschutz in Köln oder die zuständige Landesbehörde für Verfassungsschutz. Fragen kostet nichts! Es kann Ihnen jedoch viel Ärger ersparen. Auf Wunsch werden Ihre Informationen vertraulich behandelt.

Um aus einer bereits erfolgten nachrichtendienstlichen Verstrickung oder Verratstätigkeit anderer Art ohne größeren Schaden herauszukommen, bleibt immer die Möglichkeit der freiwilligen Offenbarung gegenüber dem/der SiBe oder direkt an die Verfassungsschutzbehörden. Nutzen Sie in Ihrem eigenen Interesse diese Möglichkeit und führen Sie in Ihrem Leben wieder selbst Regie.

5. Zusammenfassung

Die Sicherheit für Leib und Leben Ihrer Kollegen und Kolleginnen, die Möglichkeit für Ihr Unternehmen im wirtschaftlichen Wettbewerb zu bestehen und die innere und äußere Sicherheit der Bundesrepublik Deutschland obliegt nicht allein den hierfür vorgesehenen Behörden, sondern ist Verpflichtung jedes Bürgers. Als zum Zugang zu VS ermächtigter Mitarbeiter Ihres Unternehmens tragen Sie besondere Verantwortung. Darum sind Sie aufgefordert, in enger Zusammenarbeit mir Ihrem/r SiBe und dem BMWK die Bestimmungen zur Behandlung von VS genauestens einzuhalten, aber auch Abweichungen hiervon bei Anderen oder sonstige wichtige Wahrnehmungen (Antreffen von unbekannten Personen in Sperr- oder Kontrollzonen, Auffinden von „herrenlosen“ Gepäckstücken, nicht angekündigte Wartungsarbeiten an Ihrem Telefon oder PC usw.), sofort dem/der SiBe anzuzeigen, der/die Ihre Wahrnehmung vertraulich behandeln wird. Dies gilt ebenfalls für mögliche Ausspähungen Ihres Unternehmens von Konkurrenzunternehmen oder terroristischen Organisationen. Leichtfertigkeit oder auch falsch verstandene Kameradschaft schadet allen, auch Ihnen - Ihrem Arbeitsplatz, Ihrer Sicherheit, evtl. auch Ihrer Gesundheit oder sogar Ihrem Leben.

6. Aufruf

Helfen Sie mit, den sensiblen Bereich der Verschlusssachen vor Angriffen jeder Art und nachrichtendienstlicher Ausspähung zu schützen, um irreparable Schäden von unserer Volkswirtschaft abzuwenden. Bleiben Sie vorsichtig und misstrauisch, wenn Sie Zugang zu VS haben und halten Sie sich akribisch an alle Vorschriften und Anweisungen zum Schutze der VS. Leichtsinn, Fahrlässigkeit, Renommiersucht oder unbedachter Umgang mit Kommunikationstechnik haben schon oft zu Verlust von wertvollen Informationen zum Schaden unserer Volkswirtschaft, Ihres Unternehmens und für den Betroffenen selbst geführt. Helfen Sie mit, dies zu vermeiden.

Anmerkung:

Die nachstehenden Strafvorschriften mit Ausnahme des § 353 b Abs. 2 sind für jedermann gültig; einer besonderen Verpflichtung zur Geheimhaltung bedarf es nicht.

7. Auszug aus dem Strafgesetzbuch:

§ 93 Begriff des Staatsgeheimnisses

(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.

(2) Tatsachen, die gegen die freiheitliche demokratische Grundordnung oder unter Geheimhaltung gegenüber den Vertragspartnern der Bundesrepublik Deutschland gegen zwischenstaatlich vereinbarte Rüstungsbeschränkungen verstoßen, sind keine Staatsgeheimnisse.

§ 94 Landesverrat

(1) Wer ein Staatsgeheimnis

1. einer fremden Macht o der einem ihrer Mittelsmänner mitteilt oder

2. sonst an einen Unbefugten gelangen lässt oder öffentlich bekannt macht, um die Bundesrepublik Deutschland zu benachteiligen oder eine fremde Macht zu begünstigen,

und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft.

(2) In besonders schweren Fällen ist die Strafe lebenslange Freiheitsstrafe oder Freiheitsstrafe nicht unter fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. eine verantwortliche Stellung missbraucht, die ihn zur Wahrung von Staatsgeheimnissen besonders verpflichtet, oder

2. durch die Tat die Gefahr eines besonders schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt.

§ 95 Offenbaren von Staatsgeheimnissen

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen lässt oder öffentlich bekannt macht und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft, wenn die Tat nicht in § 94 mit Strafe bedroht ist.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. § 94 Abs. 2 Satz 2 ist anzuwenden.

§ 96 Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen

(1) *Wer sich ein Staatsgeheimnis verschafft, um es zu verraten (§ 94), wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft.*

(2) *Wer sich ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, verschafft, um es zu offenbaren (§ 95), wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. Der Versuch ist strafbar.*

§ 97 Preisgabe von Staatsgeheimnissen

(1) *Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen lässt oder öffentlich bekannt macht und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*

(2) *Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird und das ihm kraft seines Amtes, seiner Dienststellung oder eines von einer amtlichen Stelle erteilten Auftrags zugänglich war, leichtfertig an einen Unbefugten gelangen lässt und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*

(0) .....

§ 97a Verrat illegaler Geheimnisse

Wer ein Geheimnis, das wegen eines der in § 93 Abs. 2 bezeichneten Verstöße kein Staatsgeheimnis ist, einer fremden Macht oder einem ihrer Mittelsmänner mitteilt und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird wie ein Landesverräter (§ 94) bestraft. § 96 Abs. 1 in Verbindung mit § 94 Abs. 1 Nr. 1 ist auf Geheimnisse der in Satz 1 bezeichneten Art entsprechend anzuwenden.

§ 97b Verrat in irriger Annahme eines illegalen *Geheimnisses*

(1) *Handelt der Täter in den Fällen der §§ 94 bis 97 in der irrigen Annahme, das Staatsgeheimnis sei ein Geheimnis der in § 97a bezeichneten Art, so wird er, wenn*

1. *dieser Irrtum ihm vorzuwerfen ist,*
2. *er nicht in der Absicht handelt, dem vermeintlichen Verstoß entgegenzuwirken, oder*
3. *die Tat nach den Umständen kein angemessenes Mittel zu diesem Zweck ist,*

nach den bezeichneten Vorschriften bestraft. Die Tat ist in der Regel kein angemessenes Mittel, wenn der Täter nicht zuvor ein Mitglied des Bundestages um Abhilfe angerufen hat.

(2) *War dem Täter als Amtsträger oder als Soldat der Bundeswehr das Staatsgeheimnis dienstlich anvertraut oder zugänglich, so wird er auch dann bestraft, wenn nicht zuvor der Amtsträger einen Dienstvorgesetzten, der Soldat*

einen Disziplinarvorgesetzten um Abhilfe angerufen hat. Dies gilt für die für den öffentlichen Dienst besonders Verpflichteten und für Personen, die im Sinne des § 353 b Abs. 2 verpflichtet worden sind, sinngemäß.

§ 98 Landesverräterische Agententätigkeit

(1) Wer

1. *für eine fremde Macht eine Tätigkeit ausübt, die auf die Erlangung oder Mitteilung von Staatsgeheimnissen gerichtet ist, oder*
2. *gegenüber einer fremden Macht oder einem ihrer Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt,*

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in § 94 oder § 96 Abs. 1 mit Strafe bedroht ist. In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren; § 94 Abs. 2 Satz 2 Nr. 1 gilt entsprechend.

(2) Das Gericht kann die Strafe nach seinem Ermessen mildern (§ 49 Abs. 2) oder von einer Bestrafung nach diesen Vorschriften absehen, wenn der Täter freiwillig sein Verhalten aufgibt und sein Wissen einer Dienststelle offenbart. Ist der Täter in den Fällen des Absatzes 1 Satz 1 von der fremden Macht oder einem ihrer Mittelsmänner zu seinem Verhalten gedrängt worden, so wird er nach dieser Vorschrift nicht bestraft, wenn er freiwillig sein Verhalten aufgibt und sein Wissen unverzüglich einer Dienststelle offenbart.

§ 99 Geheimdienstliche Agententätigkeit

(1) Wer

1. *für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist, oder*
2. *gegenüber dem Geheimdienst einer fremden Macht oder einem seiner Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt,*

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in § 94 oder § 96 Abs. 1, in § 97a oder in § 97b in Verbindung mit § 94 oder § 96 Abs. 1 mit Strafe bedroht ist.

(2) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden, mitteilt oder liefert und wenn er

1. *eine verantwortliche Stellung missbraucht, die ihn zur Wahrung solcher Geheimnisse besonders verpflichtet, oder*
2. *durch die Tat die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführt.*

(3) § 98 Abs. 2 gilt entsprechend.

§ 353b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht

(1) Wer ein Geheimnis, das ihm als

1. Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten oder

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Hat der Täter durch die Tat fahrlässig wichtige öffentliche Interessen gefährdet, so wird er mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Wer, abgesehen von den Fällen des Absatzes 1, unbefugt einen Gegenstand oder eine Nachricht, zu deren Geheimhaltung er

1. auf Grund des Beschlusses eines Gesetzgebungsorgans des Bundes oder eines Landes oder eines seiner Ausschüsse verpflichtet ist oder

2. von einer anderen amtlichen Stelle unter Hinweis auf die Strafbarkeit der Verletzung der Geheimhaltungspflicht förmlich verpflichtet worden ist,

an einen anderen gelangen lässt oder öffentlich bekannt macht und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Der Versuch ist strafbar.

(3a) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geheimnisses oder des Gegenstandes oder der Nachricht, zu deren Geheimhaltung eine besondere Verpflichtung besteht, beschränken.

(4) Die Tat wird nur mit Ermächtigung verfolgt. Die Ermächtigung wird erteilt

1. von dem Präsidenten des Gesetzgebungsorgans

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einem oder für ein Gesetzgebungsorgan des Bundes oder eines Landes bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 1;

2. von der obersten Bundesbehörde

a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit sonst bei einer oder für eine Behörde oder bei einer anderen amtlichen Stelle des Bundes oder für eine solche Stelle bekanntgeworden ist,

b) in den Fällen des Absatzes 2 Nr. 2, wenn der Täter von einer amtlichen Stelle des Bundes verpflichtet worden ist;

3. von der obersten Landesbehörde in allen übrigen Fällen der Absätze 1 und 2 Nr. 2.

Auszug aus der Strafprozessordnung

§ 153 e

Absehen von Strafverfolgung bei tätiger Reue

(1) Hat das Verfahren Straftaten der in § 74a Abs. 1 Nr. 2 bis 4 und in § 120 Abs. 1 Nr. 2 bis 7 des Gerichtsverfassungsgesetzes bezeichneten Art zum Gegenstand, so kann der Generalbundesanwalt mit Zustimmung des nach § 120 des Gerichtsverfassungsgesetzes zuständigen Oberlandesgerichts von der Verfolgung einer solchen Tat absehen, wenn der Täter nach der Tat, bevor ihm deren Entdeckung bekanntgeworden ist, dazu beigetragen hat, eine Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder die verfassungsmäßige Ordnung abzuwenden. Dasselbe gilt, wenn der Täter einen solchen Beitrag dadurch geleistet hat, dass er nach der Tat sein mir ihr zusammenhängendes Wissen über Bestrebungen des Hochverrats, der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit einer Dienststelle offenbart hat.

(2) Ist die Klage bereits erhoben, so kann das nach § 120 des Gerichtsverfassungsgesetzes zuständige Oberlandesgericht mit Zustimmung des Generalbundesanwalts das Verfahren unter den in Absatz 1 bezeichneten Voraussetzungen einstellen.

MERKBLATT

für Auslandsreisen von VS-Ermächtigten

1. Personen, die eine sicherheitsempfindliche Tätigkeit ausüben, sind im besonderen Maße Ziel fremder Nachrichtendienste. Die Erfahrung lehrt, dass Ansprachen oder Anbahnungsversuche mit nachrichtendienstlicher Zielsetzung häufig auf Auslandsreisen durchgeführt werden.

   Sie müssen die Möglichkeit von Ansprachen durch fremde Nachrichtendienste auch bei Auslandsreisen immer im Gedächtnis haben. Sollten Sie konkrete Fragen zur nachrichtendienstlichen Lage auch bezogen auf Ihr Reiseland haben, können Sie sich vor Reiseantritt an Ihren/Ihre Sicherheitsbevollmächtigte(n) wenden.

   Die nachfolgenden Hinweise sollen Personen, die eine sicherheitsempfindliche Tätigkeit ausüben, eine Orientierungshilfe sein, derartige Gefahren zu erkennen und ihnen zu begegnen.

2. Bei Auslandsreisen sollten vor allem folgende Verhaltensregeln beachtet werden:
   - Informieren Sie sich über die im Reiseland geltenden Vorschriften und beachten Sie diese genau. Handlungen, die in der Bundesrepublik Deutschland erlaubt sind, können im Reiseland strafbar sein. In folgenden Bereichen sind die Kenntnis und die Einhaltung der Vorschriften besonders wichtig:
     - Visa- und Meldebestimmungen, Vorschriften über die Ein- und Ausfuhr von Devisen, ggf. sonstige Ein- und Ausfuhrbestimmungen, insbesondere bei Kunstgegenständen und Antiquitäten
     - Verkehrsbestimmungen (in einigen Staaten gilt absolutes Alkoholverbot im Straßenverkehr),
     - Fotografier- und Filmverbote.
   - Um fremden Nachrichtendiensten keinen Ansatzpunkt für eine Ansprache zu bieten, sollten Sie darüber hinaus noch folgendes beachten:
     - Nehmen Sie auf privaten Reisen keine dienstlichen Unterlagen mit.
     - Wahren Sie bitte Zurückhaltung auch im persönlichen Verhalten und seien Sie gegenüber Unbekannten reserviert. Lassen Sie sich weder zu Gefälligkeiten verleiten, die Ihnen nachteilig ausgelegt werden könnten, noch zu negativen Äußerungen über das Reiseland.

- Sollten Sie verschuldet oder unverschuldet gegenüber den Behörden des Reiselandes in Schwierigkeiten geraten, so verständigen Sie bitte sofort die nächste diplomatische oder konsularische Vertretung der Bundesrepublik Deutschland. (Sie sollten daher die Telefonnummer der in Frage kommenden Botschaften/Konsulate mitführen.)

  Machen Sie grundsätzlich wahrheitsgemäße Angaben zu Ihrer Person. Bei Fragen nach Ihrer beruflichen Tätigkeit sind Sie allenfalls zur Angabe Ihres Arbeitgebers und Ihrer Stellung verpflichtet. Berufen Sie sich im übrigen auf Ihre Verschwiegenheitspflicht.
- Versuche, Sie zu nachrichtendienstlicher Mitarbeit zu gewinnen, sollten Sie höflich, aber bestimmt ablehnen. Unterschreiben Sie keine Verpflichtungserklärung (auch nicht zum Schein). Unterrichten Sie nach Ihrer Rückkehr umgehend Ihren/Ihre Sicherheitsbevollmächtigten/e von solchen Versuchen. Dabei sollten Sie sich alle Einzelheiten des Vorfalls einschließlich einer Personenbeschreibung des oder der Gesprächspartner und des an Sie gestellten Ansinnens genau einprägen. Das gleiche gilt für alle Umstände, die Ihnen auffallen und die Ihnen nach der Lebenserfahrung ungewöhnlich erscheinen und als besonderes Interesse an Ihrer Person gedeutet werden können.
- Wenn Sie aus Angst oder unter Druck trotz allem eine nachrichtendienstliche Verpflichtung eingegangen sind, wenden Sie sich bitte sofort nach Rückkehr an Ihren/Ihre Sicherheitsbevollmächtigten/e. Er/Sie wird Ihnen helfen. Die Verfassungsschutzbehörden unterstützen Sie auf Ihren Wunsch dabei.

Bescheinigung des/der Sicherheitsbevollmächtigten (SiBe) im nationalen Besuchskontrollverfahren (SiBe-Bescheinigung)

Betriebs-Nr.: (Absender)	
Name des/der SiBe (Absender)	
Adresse des/der SiBe (Absender)	
Betriebs-Nr.[1]: (zu besuchendes Unternehmen)	
Name des/der SiBe (zu besuchendes Unternehmen/ Geheimschutzbeauftragte/r)	
Adresse des/der SiBe (zu besuchendes Unternehmen/ Geheimschutzbeauftragte/r)	

BESCHEINIGUNG

Nr.: Gültig bis zum:

Folgende/r Besucher/in wird angemeldet:

Name, Vorname ,

Geburtsdatum und –ort ,

Staatsangehörigkeit

Inhaber/in des Reisepasses/ Personalausweises Nr.

Ausgestellt in am:

Angehörige/r des Unternehmens

Besuchszeitraum bis

Besuchszweck

Gesprächspartner/in

Es wird bestätigt, dass der/die Besucher/in vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund einer Sicherheitsüberprüfung zum Zugang zu VS der Geheimhaltungsgrade

VS-VERTRAULICH

ermächtigt worden ist. Überprüfungsart: ☐ § 10 SÜG = Ü 3 ☐ § 9 SÜG = Ü 2 ☐ § 8 SÜG = Ü 1
Der/die Besucher/in ist berechtigt, VS als Kurier zu befördern. Ja ☐[2] Nein ☐

,
(Ort, Datum)

(Unterschrift des / der SiBe)

[1] nicht bei Behörden
[2] In diesem Fall muss Kurierausweis ausgestellt werden.

Sammelbescheinigung des/der Sicherheitsbevollmächtigten (SiBe) im nationalen Besuchskontrollverfahren (Sammel-SiBe-Bescheinigung)

Betriebs-Nr.: (Absender)	
Name des/der SiBe (Absender)	
Adresse des/der SiBe (Absender)	
Betriebs-Nr.[1]**:** (zu besuchendes Unternehmen)	
Name des/der SiBe (zu besuchendes Unternehmen/ Geheimschutzbeauftragte/r)	
Adresse des/der SiBe (zu besuchendes Unternehmen/ Geheimschutzbeauftragte/r)	

BESCHEINIGUNG

Nr.: Gültig bis zum:

Hiermit wird bestätigt, dass die unter den lfd. Nrn. bis aufgeführten Besucher/innen vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund einer Sicherheitsüberprüfung zum Zugang zu VS der Geheimhaltungsgrade

VS-VERTRAULICH/ GEHEIM

ermächtigt worden sind.

Die unter den lfd. Nr/n. _____ aufgeführten Besucher/innen sind berechtigt, VS als Kurier zu befördern.

Ja ☐ [2] Nein ☐

_____, _____

(Ort, Datum)

(Unterschrift des / der SiBe)

[1] nicht bei Behörden

[2] In diesem Fall muss Kurierausweis ausgestellt werden.

Folgende Besucher/innen werden angemeldet:

Angehörige des Unternehmens:	
Besuchszeitraum:	
Besuchszweck:	
Gesprächspartner/in:	

Lfd. Nr.	Name	Vorname	Geb.-Datum	Geb.-Ort	Staats-angehörigkeit	Reisepass- oder Personalausweis-Nr.:	Ausgestellt am:	Ausgestellt in:	Überprüfungsart: § 10 SÜG = Ü 3 § 9 SÜG = Ü 2 § 8 SÜG = Ü 1	Ermächtigt bis: (VS-Vertraulich, Geheim, NC, NS)

All fields must be completed and the form communicated via Government-to-Government

REQUEST FOR VISIT

TO:
(Country / international organisation name)

1. TYPE OF VISIT REQUEST	2. TYPE OF INFORMATION / MATERIAL OR SITE ACCESS	3. SUMMARY
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment	☐ CONFIDENTIAL or above ☐ Access to security areas without access to classified information / material *Only if required by the laws / regulations of the countries involved* ☐ Unclassified / RESTRICTED	No. of sites: 1 No. of visitors: 1

4. ADMINISTRATIVE DATA:

Requestor:		NSA/DSA RFV Reference No.	
To:		Date (dd/mm/yyyy):	

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ NATO ☐ EU ☐ Other

NAME:			
POSTAL ADDRESS:			
E-MAIL ADDRESS:			
FAX NO:		TELEPHONE NO:	

6. GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM TO

8. TYPE OF INITIATIVE *(Select one from each column)*:

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

All fields must be completed and the form communicated via Government-to-Government

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification of the selected subject:

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided):*

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:

Only if required by the laws/regulations of the countries involved

☐ Unclassified ☐ RESTRICTED ☐ CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐ Other

12. PARTICULARS OF VISITOR(S) - *(Annex 2 to be completed)*

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:
TELEPHONE NO:
E-MAIL ADDRESS:
SIGNATURE:

STAMP

All fields must be completed and the form communicated via Government-to-Government

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:		STAMP	
ADDRESS:			
TELEPHONE NO:			
E-MAIL ADDRESS:			
SIGNATURE:		DATE (*dd/mm/yyyy*):	

15. REQUESTING NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY:

NAME:		STAMP	
ADDRESS:			
TELEPHONE NO:			
E-MAIL ADDRESS:			
SIGNATURE:		DATE *(dd/mm/yyyy)*:	

16. REMARKS *(Mandatory justification required in case of an emergency visit):*

ANNEX 1 TO RFV FORM

All fields must be completed and the form communicated via Government-to-Government

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

Add

☐Military ☐Government ☐Industry ☐NATO ☐EU ☐Other

NAME:	
ADDRESS:	
TELEPHONE NO:	
FAX NO:	
NAME OF POINT OF CONTACT:	
E-MAIL:	
TELEPHONE NO:	
NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT:	
E-MAIL:	
TELEPHONE NO:	

Delete

ANNEX 2 TO RFV FORM

All fields must be completed and the form communicated via Government-to-Government

PARTICULARS OF VISITOR(S)

Add

☐ Military ☐ Defence Public Servant ☐ Government ☐ Industry/Embedded Contractor ☐ NATO Employee ☐ EU Employee ☐ Other

SURNAME:

FORENAMES (as per passport):

RANK (if applicable):

DATE OF BIRTH (dd/mm/yyyy):

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/AGENCY:

Delete

Bearbeitungsfristen internationale Besuchsanträge

Die von den Besuchsländern vorgeschriebenen, nachstehend aufgelisteten Antragsfristen müssen vom Antragsteller unbedingt eingehalten werden. Sie umfassen die Vorlagefrist im Besuchsland inklusive der Bearbeitungszeit in den deutschen Behörden sowie des gelegentlichen erheblichen Zeitaufwands für den Postversand an die Botschaft des Besuchslandes. Die für den Antragsteller bindende Gesamtfrist beginnt mit dem Eingang bei der zuständigen Stelle.

Anträge, die diese Fristen unterschreiten oder unvollständige Angaben enthalten, werden im Regelfall von den zuständigen ausländischen Dienststellen nicht entgegengenommen und unbearbeitet an den Antragsteller zurückgegeben.

Die zuständige ausländische Dienststelle akzeptiert Änderungen, wenn sie eine bestimmte Anzahl von Arbeitstagen vor dem geplanten Besuch liegen und sich ausschließlich auf Besuchsdaten und Hinzufügen von Besuchern beziehen. Solche Änderungen sollten auf die ursprünglichen Anträge verweisen. Die Gesamtvorlagefristen (einschl. Bearbeitungszeit bei den zuständigen deutschen Behörden, Kurierweg, etc.) sind in der nachstehenden Tabelle dargestellt.

Im Rahmen von projektspezifische Regelungen können jedoch auch kürzere Fristen zur Anwendung kommen.

Besuche in NATO-Mitgliedstaaten	**Bearbeitungsfrist (Arbeitstage)**	**Fristen bei Änderungen von Besuchsanträgen (Arbeitstage)**
Albania	20	10
Belgium	10	5
Bulgaria	15	10
Canada	20	5
Croatia	20	7
Czech Republic	20	7
Denmark	15	7
Estonia	21	5
France	25	5
Germany	20	7
Greece	20	10
Hungary	20	10
Iceland	-	-
Italy	20	7
Latvia	20	5
Lithuania	14	-
Luxembourg	10	5
Netherlands	10	5
Norway	10	-

Besuche in NATO-Mitgliedstaaten	Bearbeitungsfrist (Arbeitstage)	Fristen bei Änderungen von Besuchsanträgen (Arbeitstage)
Poland	25	10
Portugal	15	10
Romania	25	10
Slovakia	20	10
Slovenia	21	7
Spain	20	7
Turkey	25	10
United Kingdom	21	7
United States	21	5

Besuche bei NATO-Management-Agenturen und Büros	Bearbeitungsfrist (Arbeitstage)	Fristen bei Änderungen von Besuchsanträgen (Arbeitstage)
Central European Pipeline Management Agency (CEPMA)	3	-
NATO HAWK Management Office (NHMO)	7	-
NATO EF2000 and Tornado Development, Production & Logistics Management Agency (NETMA)	3	-
NATO Maintenance & Supply Agency (NAMSA)	3	-
NATO Consultation, Command & Control Agency (NC3A)	3	-
NATO Airborne Early Warning and Control Programme Management Agency (NAPMA)	3	1
NATO ACCS Management Agency (NACMA)	-	-
NATO Helicopter D&D Production & Logistics Management Agency (NAHEMA)	3	-
NATO Medium Extended Air Defence System D&D, Production & Logistics Management Agency (NAMEADSMA)	-	-
NATO BICES Agency (NBA)	-	-

NATO-Agenturen,

die NATO-Programme betreuen, bei denen BMWK für die Annahme von Besuchsanträgen zuständig ist

NATO Management Agency / Office

Central European Pipeline Management Agency	CEPMA
NATO HAWK Management Office	NHMO
NATO EF2000 and Tornado Development, Production & Logistics Management Agency	NETMA
NATO Maintenance & Supply Agency	NAMSA
NATO Consultation, Command & Control Agency	NC3A
NATO Airborne Early Warning and Control Programme Management Agency	NAPMA
NATO ACCS Management Agency	NACMA
NATO Helicopter D&D Production & Logistics Management Agency	NAHEMA
NATO BICES Agency	NBA

Bearbeitungsfristen für NATO-Besuchsanträge:

Die von den Besuchsländern vorgeschriebenen, nachstehend aufgelisteten Antragsfristen müssen vom Antragsteller unbedingt eingehalten werden. Sie umfassen die Vorlagefrist im Besuchsland inklusive der Bearbeitungszeit in den deutschen Behörden sowie des gelegentlichen erheblichen Zeitaufwands für den Postversand an die Botschaft des Besuchslandes. Die für den Antragsteller bindende Gesamtfrist beginnt mit dem Eingang bei der zuständigen Stelle.

Anträge, die diese Fristen unterschreiten oder unvollständige Angaben enthalten, werden im Regelfall von den zuständigen ausländischen Dienststellen nicht entgegengenommen und unbearbeitet an den Antragsteller zurückgegeben.

Die zuständige ausländische Dienststelle akzeptiert Änderungen, wenn sie eine bestimmte Anzahl von Arbeitstagen vor dem geplanten Besuch liegen und sich ausschließlich auf Besuchsdaten und Hinzufügen von Besuchern beziehen. Solche Änderungen sollten auf die ursprünglichen Anträge verweisen. Die Gesamtvorlagefristen (einschl. Bearbeitungszeit bei den zuständigen deutschen Behörden, Kurierweg, etc.) sind in der nachstehenden Tabelle dargestellt.

	Bearbeitungsfrist (Arbeitstage)	Fristen bei Änderungen von Besuchsanträgen (Arbeitstage)
Belgien	10	5
Dänemark	15	-
Frankreich	25	5
Griechenland	20	10
Großbritannien	15	7
Italien	20	7
Kanada	20	-
Luxemburg	10	5
Niederlande	14	-
Norwegen	21	-
Portugal	20	10
Spanien	20	7
Türkei	25	10
USA	21	5

EDIR/FA REQUEST FOR VISIT[1]

☐One-time
☐Recurring
☐More than 21 days

REQUESTING ESTABLISHMENT/COMPANY/AGENCY			
Name:			
Address:			
Security Officer:			
Telephone **Fax** **E-mail:**		**Point of contact:**	

ESTABLISHMENT/COMPANY/AGENCY TO BE VISITED			
Name:			
Address:			
Security Officer:			
Telephone **Fax** **E-mail:**		**Point of contact:**	

DATE OF VISIT (dd/MM/yyyy)			
From:		**to:**	

SUBJECT TO BE DISCUSSED:		
Project/Contract/Programme:		
Anticipated Level of Discussions	☐ **C**	☐ **S**

VISITOR DETAILS			
Name:		**Passport N°:**	
Date of Birth:		**Nationality:**	
Security Clearance level:		**Expiry Date:**	
Company/Agency:		**Rank/Grade:**	
		Position:	

Continue on additional sheets for extra visitors.

Signature:		**Date:**	

[1] To be completed in the English language.
Stand: 20.07.2009

Vergleichbare internationale Geheimhaltungsgrade

Vergleichbarkeitstabelle von VS über- oder zwischenstaatlicher Einrichtungen oder Stellen

Für VS über- oder zwischenstaatlicher Einrichtungen und Stellen, bei denen Deutschland Vertragspartner ist, sind folgenden Geheimhaltungsgrade mit deutschen Geheimhaltungsgraden vergleichbar. VS dieser Einrichtungen sind in Deutschland aber nach den speziellen Vorschriften der jeweiligen Einrichtung zu schützen.

Deutschland	**GEHEIM**	**VS-VERTRAULICH**	**VS-NUR FÜR DEN DIENSTGEBRAUCH**
NATO	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
EU	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
ESA	ESA SECRET	ESA CONFIDENTIAL	ESA RESTRICTED
OCCAR	OCCAR SECRET	OCCAR CONFIDENTIAL	OCCAR RESTRICTED

Bilaterale Geheimschutzabkommen

Eine vollständige, aktuelle Liste der gültigen bilateralen Geheimschutzabkommen mit anderen Ländern findet sich im passwortgeschützten Bereich des BMWK-Geheimschutzportals https://bmwk-sicherheitsforum.de unter Rubrik: “Rund um den Geheimschutz/Aktuelles/Bilaterale Geheimschutzabkommen“.

Vergleichstabelle der EDIR-Geheimhaltungsgrade

Bei den Geheimhaltungsgraden der Vertragsparteien gelten folgende Entsprechungen:

	GEHEIM	**VS-VERTRAULICH**	**VS-NUR FÜR DEN DIENSTGEBRAUCH**
Frankreich	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Großbritannien	SECRET	CONFIDENTIAL	RESTRICTED
Italien	SEGRETO	RISERVATISSIMO	RISERVATO
Schweden	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL	HEMLIG/ RESTRICTED
Spanien	RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA

Mindestanforderungen zur Erstellung von Kontrollzonenanweisungen

Kontrollzonen sind Bereiche, in denen VS bearbeitet werden, wenn der persönliche Gewahrsam nicht gewährleistet werden kann. Die Aufbewahrung von VS außerhalb von VS-Verwahrgelassen ist hier nicht zulässig. Für Kontrollzonen sind Anweisungen zu erstellen, die alle Angaben zur ordnungsgemäßen Handhabung von VS in diesem Bereich enthalten. Die Anweisungen bedürfen der Einwilligung des BMWi. Sie müssen insbesondere folgende Punkte enthalten:

1. Beschreibung der Kontrollzone
- Bezeichnung der Kontrollzone
- Nummer der Kontrollzone
- Lage der Kontrollzone (Gebäude, Raum)
- Geltende Vorschriften (GHB, VS-NfD-Merkblatt, IT-Geheimschutzanweisung, firmeninterne Vorschriften)
- Ziel der Kontrollzonenanweisung

2. Kontrollzonenverantwortliche/r und seine/ihre Aufgaben
- Name des/der Kontrollzonenverantwortlichen und seines/seiner/ihres/ihrer Vertreters/Vertreterin
- Aufgaben des/der Kontrollzonenverantwortlichen und seiner/ihrer Aufgaben
- Hinweis auf oberste Verantwortung des/der SiBes/SiBe (Vorfälle, nicht Geregeltes)

3. Zutrittsregelung
- Zutrittsregelung (wer darf Kontrollzone betreten, wer legt dies fest, wie wird kontrolliert, VS-Ermächtigte, Nicht-VS-Ermächtigte, Besucher)
- Reinigung (wann, wer)

4. Verhaltensmaßnahmen
- Mobiltelefonregelung (Handyverbot)
- Bildaufzeichnungsregelung (Fotografierverbot)
- Maßnahmen bei VS-Bearbeitung (Zutrittskontrolle, Sichtschutz, Lauschabwehr, Abstrahlschutz [Zeitmatrix])
- VS-Aufbewahrung
- Ggf. Scharf-/Unscharfschaltung (wer, wann, wie)
- Aufbewahrung Schlüssel/Reserveschlüssel

5. Anlagen
- Lageplan
- Liste der in der Kontrollzone Beschäftigten

Ggf. sind weitere Maßnahmen oder Informationen in die Anweisung aufzunehmen.

Mindestanforderungen zur Erstellung von Sperrzonenanweisungen

Sperrzonen sind Bereiche, in denen VS bearbeitet und/oder auch außerhalb der Arbeitszeit aufbewahrt werden. Für Sperrzonen sind Anweisungen zu erstellen, die alle Angaben zur ordnungsgemäßen Handhabung und/oder Aufbewahrung von VS in diesem Bereich enthalten. Die Anweisungen bedürfen der Einwilligung des BMWi. Sie müssen insbesondere folgende Punkte enthalten:

1. Beschreibung der Sperrzone
- Bezeichnung der Sperrzone
- Nummer der Sperrzone
- Lage der Sperrzone (Gebäude, Raum)
- Geltende Vorschriften (GHB, VS-NfD-Merkblatt, IT-Geheimschutzanweisung, firmeninterne Vorschriften)
- Ziel der Sperrzonenanweisung

2. Sperrzonenverantwortliche/r und seine/ihre Aufgaben
- Name des/der Sperrzonenverantwortlichen und seines/seiner/ihres/ihrer Vertreters/Vertreterin
- Aufgaben des/der Sperrzonenverantwortlichen und seiner/ihrer Aufgaben
- Hinweis auf oberste Verantwortung des/der SiBes/SiBe (Vorfälle, nicht Geregeltes)

3. Zutrittsregelung
- Zutrittsregelung (wer darf Sperrzonen betreten, wer legt dies fest, wie wird kontrolliert, VS-Ermächtigte, Nicht-VS-Ermächtigte, Begleitung)
- Reinigung (wann, wer)

4. Verhaltensmaßnahmen
- Besucherbuch
- Ggf. Sperrzonenausweis (Tragepflicht, Verbot der Weitergabe)
- Mobiltelefonregelung (Handyverbot)
- Bildaufzeichnungsregelung (Fotografierverbot)
- Maßnahmen bei VS-Bearbeitung (Zutrittskontrolle, Lauschabwehr, Abstrahlschutz [Zeitmatrix])
- VS-Aufbewahrung
- Scharf-/Unscharfschaltung (wer, wann, wie)
- Aufbewahrung Schlüssel/Reserveschlüssel

5. Anlagen
- Lageplan
- Liste der in der Sperrzone Beschäftigten

Ggf. sind weitere Maßnahmen oder Informationen in die Anweisung aufzunehmen.

Leitfaden für „Unternehmensinterne Kontrollen des/der Sicherheitsbevollmächtigten (SiBe) zum Schutz von Verschlusssachen (VS) einschließlich Geheimschutzplan (Kontrollrichtlinie)“

1. Allgemeines

Kontrollen zum Schutz von VS (VS-Kontrollen) sind ein wesentlicher Bestandteil der Geheimschutzmaßnahmen. Sie gewährleisten, dass die personellen, materiellen und organisatorischen Sicherheitsmaßnahmen wirksam werden und bleiben.

Wenn die Anzahl oder die Art der VS oder die Gefährdung des Unternehmens es erfordern, ist ein Geheimschutzplan (Anlage) zu erstellen, in dem die wichtigsten Vorkehrungen des Unternehmens für den Schutz von VS zusammengefasst sind. Die in der Anlage zusammengestellten Positionen sind beispielhaft. Der Geheimschutzplan ist bei dem/der SiBe verschlossen aufzubewahren.

Art, Umfang und Durchführung der Kontrollen plant und regelt der/die SiBe. Kontrollen und ihre Ergebnisse sind aktenkundig zu machen.

Die Kontrollen sind in aller Regel unangekündigt durchzuführen. In besonders sicherheitsempfindlichen Arbeitsbereichen ist häufiger zu kontrollieren. Bei festgestellten Fehlern oder Verdachtsfällen ist nach 3.3.5 GHB zu verfahren.

2. Einzelmaßnahmen

2.1 Herstellung und Vernichtung von VS

Kontrolle/Prüfung, ob die für die Herstellung oder Vernichtung von VS geltenden Regeln eingehalten werden (Kennzeichnung, Registrierung, VS-Vernichtungsprotokoll), insbesondere, ob die Anzahl der Ausfertigungen (z.B. Ablichtungen) auf das Mindestmaß beschränkt ist und dem Auftrag entspricht.

2.2 VS-Einstufung

Kontrolle/Prüfung, ob die Kennzeichnung der VS in Übereinstimmung mit der amtlichen VS-Einstufung erfolgt ist.

2.3 VS-Zwischenmaterial

Kontrolle/Prüfung, ob die Regeln für die Behandlung von VS-Zwischenmaterial gemäß 1.6.2 GHB eingehalten werden.

2.4 Datenträger aller Art

Kontrolle/Prüfung, des Verbleibs von Datenträgern aller Art, die zur Herstellung von VS eingesetzt werden.

Kontrolle/Prüfung (z.B. mit Hilfe von Kennzeichen), ob Datenträger ausgetauscht worden sind.

2.5 Kopiergeräte

Kontrolle,

- ob ein Verzeichnis der Kopiergeräte, auf denen VS vervielfältigt werden dürfen, geführt wird,
- ob Kopiergeräte (in deren Nähe VS bearbeitet oder verwaltet werden) und auf denen VS nicht vervielfältigt werden dürfen, gut sichtbar entsprechend gekennzeichnet sind,
- dass VS nicht unbefugt vervielfältigt werden.

2.6 Posteingang, Postausgang

Kontrolle/ Prüfung, ob eingehende VS gemäß den geltenden Regeln ungeöffnet dem befugten Empfänger zugeleitet werden.

2.7 Arbeitsplatz

Kontrolle/ Prüfung am Arbeitsplatz von VS-Verwaltern, VS-Bearbeitern, Schreibkräften, ob die überlassenen VS vorhanden, vollständig und vorschriftsmäßig aufbewahrt sind bzw. der Verbleib nachgewiesen werden kann.

2.8 VS-Verwahrgelasse

Kontrolle/ Prüfung, ob die überlassenen VS vorhanden und vollständig sind. Es kann zweckmäßig sein, VS-Verwahrgelasse größerer Organisationseinheiten zusammenhängend zu überprüfen.

VS-Verwahrgelasse können auch in Abwesenheit der Benutzer geöffnet und überprüft werden. Bei Überprüfungen in Abwesenheit der Benutzer ist der/die zuständige VS-Verwalter/in oder eine andere VS-ermächtigte Person zu beteiligen.

Die Umschläge mit den benötigten Reserveschlüsseln und Zahlenkombinationen sind in Anwesenheit aller an der Kontrolle Beteiligten zu öffnen und danach wieder sicher zu verwahren.

Über die Kontrolle ist am Arbeitsplatz dem Betroffenen eine Nachricht zu hinterlassen, die auch einen Hinweis auf 6.9.3 GHB enthält.

2.9 Gefahrenmeldeanlagen

Kontrolle, ob die Gefahrenmeldeanlagen in den vorgeschriebenen Zeiträumen gewartet wurde.

Soweit VS-Verwahrgelasse technisch überwacht werden, sind z.B. anhand von Zeitschreibern die Ein- und Ausschaltzeiten der Gefahrenmeldeanlagen zu überprüfen. Bei Anwesenheit von VS-Bearbeitern oder VS-Verwaltern außerhalb der üblichen Arbeitszeit ist deren Notwendigkeit zu prüfen.

2.10 Zahlenkombinationen

Hinweis, dass

- keine leicht zu ermittelnden Zahlen oder Zusammenstellungen verwendet werden und

Kontrolle, ob

- die jeweilige Kombination fristgerecht und nachweisbar umgestellt wurde.

Öffnungsversuche sind mit früher gültigen Zahlenkombinationen vorzunehmen.

2.11 Technische Prüfungen

Soweit technische Prüfungen erforderlich werden, ist BMWi zu unterrichten.

Geheimschutzplan, Anlage zur Kontrollrichtlinie

Der Geheimschutzplan ist VS-NfD einzustufen und soll u.a. enthalten:

1. Vorschriften

Die anzuwendenden unternehmensinternen Vorschriften zum Schutz von VS sowie die besonderen Weisungen und Anordnungen des Bundesministeriums für Wirtschaft und Technologie.

2. Personalübersichten

2.1 VS-Ermächtigte, geordnet nach Namen/Organisationseinheiten mit Geheimhaltungsgraden; auftragsbezogenes VS-Personalverzeichnis,

2.2 VS-Verwalter/in,

2.3 Schreib- und Vorzimmerkräfte (soweit VS-ermächtigt),

2.4 VS-Kuriere,

2.5 Verzeichnisse des Personals, das besondere Zugangsberechtigung besitzt (z.B. Krypto-Verwalter, ELOKA-Verpflichtete).

2.6 Anordnungsbefugte (Vervielfältigungen von VS, Vernichtung von VS)

3. Übersicht über die vorhandenen Sicherungseinrichtungen

3.1 VS-Verwahrgelasse und VS-Schlüsselbehälter

3.1.1 Standorte und Benutzer/innen,

3.1.2 Namen der Verwalter/innen der Reserveschlüssel und Zahlenkombinationen,

3.1.3 Aufbewahrungsorte der Reserveschlüssel und Zahlenkombinationen sowie Zugangsmöglichkeiten (auch außerhalb der Arbeitszeit).

3.2 Gefahrenmeldeanlagen

3.2.1 VS-Verwahrgelasse, die durch Gefahrenmeldeanlagen abgesichert sind sowie Angaben darüber, wer befugt ist, die Gefahrenmeldeanlagen scharf und unscharf schalten, wer die Ein- und Ausschaltzeiten überprüft und wo und durch wen die Reserveschlüssel und Zahlenkombinationen aufbewahrt bzw. verwaltet werden.

3.2.2 Angaben, bei welcher Stelle (Polizei) Alarm ausgelöst und was in diesem Falle veranlasst wird.

3.2.3 Plan über den Verlauf der Leitungen der Gefahrenmeldeanlagen innerhalb des Unternehmensgeländes.

4. Sicherheitsbereiche

Lagepläne über VS-Sperr- und VS-Kontrollzonen sowie die zu deren Schutz getroffenen Maßnahmen.

5. Geräte zur Vernichtung von VS

Standorte und Art der vorhandenen Geräte.

6. Vervielfältigungsgeräte

Standorte der Kopier- und Druckgeräte, mit denen Verschlusssachen gefertigt werden dürfen.

Angaben über Maßnahmen zur Verhinderung der unbefugten Vervielfältigung von Verschlusssachen.

7. Übersicht über sonstige technische und organisatorische Maßnahmen zum Schutz von VS

7.1 Angaben über Verwaltung und Sicherung der Schlüssel zu Räumen, in denen Verschlusssachen bearbeitet werden; Schließplan.

7.2 Angaben über Abhörschutzmaßnahmen (abhörtechnische Prüfungen, abhörgeschützte Telefone, abhörgeschützte / abhörsichere Räume einschließlich Zutrittsregelung, Reinigung, Schlüsselaufbewahrung usw.).

7.3 Standorte der Kryptogeräte und verwendete Kryptodatenträger (Schlüsselbereiche).

7.4 VS-Übergabeverhandlungen und VS-Empfangsscheine für VS-Bestandsverzeichnisse.

Anschriften der Verfassungsschutzbehörden des Bundes und der Länder

Bund	Bundesamt für Verfassungsschutz (BfV) Merianstrasse 100 50765 Köln Tel.: 0221/792-0 Internet: https://www.verfassungsschutz.de E-Mail: poststelle@bfv.bund.de
Baden-Württemberg	Landesamt für Verfassungsschutz Baden-Württemberg Taubenheimstr. 85 a 70372 Stuttgart Telefon: 0711-954400 Telefax: 0711-9544444 Internet: http://www.verfassungsschutz-bw.de E-Mail: info@lfvbw.bwl.de
Bayern	Bayerisches Landesamt für Verfassungsschutz Postfach 45 01 45 80901 München Telefon: 089-312010 Telefax: 089-31201380 Internet: http://www.verfassungsschutz.bayern.de E-Mail: poststelle@lfv.bayern.de
Berlin	Senatsverwaltung für Inneres und Sport Berlin Abteilung II Klosterstr. 47 10179 Berlin Telefon: 030-90129111 Telefax: 030-90129844 Internet: http://www.berlin.de/sen/inneres/verfassungsschutz E-Mail: info@verfassungsschutz-berlin.de
Brandenburg	Ministerium des Innern und für Kommunales des Landes Brandenburg - Abteilung V - Henning von Tresckow Straße 9-13 14467 Potsdam Telefon: 0331-8662500 Telefax: 0331-8662609 Internet: http://www.verfassungsschutz-brandenburg.de E-Mail: info@verfassungsschutz-brandenburg.de
Bremen	Freie Hansestadt Bremen - Der Senator für Inneres Abteilung 4 Postfach 28 61 57 28361 Bremen Telefon: 0421-53 77-0 Fax: 0421-53 77-195 Internet: www.verfassungsschutz.bremen.de E-Mail: office@lfv.bremen.de

Hamburg	Landesamt für Verfassungsschutz Hamburg Johanniswall 4/III 20095 Hamburg Telefon: 040-244443 Telefax: 040-338360 Internet: http://www.verfassungsschutz.hamburg.de E-Mail: poststelle@verfassungsschutz.hamburg.de
Hessen	Landesamt für Verfassungsschutz Hessen Konrad Adenauer Ring 49 65187 Wiesbaden Telefon: 0611-7200 Telefax: 0611-720179 Internet: https://lfv.hessen.de E-Mail: poststelle@lfv.hessen.de
Mecklenburg-Vorpommern	Ministerium für Inneres, Bau und Digitalisierung Abt. II 5 - Verfassungsschutz Postfach 11 05 52 19055 Schwerin Telefon: 0385-74200 Telefax: 0385-714438 Internet: http://www.verfassungsschutz-mv.de E-Mail: info@verfassungsschutz-mv.de
Niedersachsen	Niedersächsisches Landesamt für Verfassungsschutz Büttnerstraße 28 30165 Hannover Telefon: 0511-67090 Telefax: 0511-6709388 Internet: http://www.verfassungsschutz.niedersachsen.de E-Mail: oeffentlichkeitsarbeit@mi.niedersachsen.de
Nordrhein-Westfalen	Ministerium des Innern des Landes Nordrhein-Westfalen Abteilung VI Friedrichstr. 62-80 40217 Düsseldorf Telefon: 0211-8712821 Telefax: 0211-8712980 Internet: https://www.im.nrw/themen/verfassungsschutz E-Mail: kontakt.verfassungsschutz@im1.nrw.de
Rheinland-Pfalz	Ministerium des Innern und für Sport des Landes Rheinland- Pfalz Abteilung 6 Schillerplatz 3-5 55116 Mainz Telefon: 06131-163773 Internet: https://mdi.rlp.de/de/unsere-themen/verfassungsschutz/ E-Mail: info.verfassungsschutz@mdi.rlp.de

Saarland	Verfassungsschutz im Ministerium für Inneres, Bauen und Sport Abteilung V Postfach 10 20 63 66020 Saarbrücken Telefon: 0681-30380 Telefax: 0681-3038109 Internet: http://www.saarland.de E-Mail: verfassungsschutz@innen.saarland.de
Sachsen	Landesamt für Verfassungsschutz Sachsen Neuländer Straße 60 01129 Dresden Telefon: 0351-85850 Telefax: 0351-8585500 Internet: https://www.verfassungsschutz.sachsen.de/ E-Mail: verfassungsschutz@lfv.smi.sachsen.de
Sachsen-Anhalt	Ministerium des Innern des Landes Sachsen-Anhalt Abteilung 4 Nachtweide 82 39124 Magdeburg Telefon: 0391-5673900 Telefax: 0391-5673999 Internet: http://www.mi.sachsen-anhalt.de/verfassungsschutz E-Mail: verfassungsschutz@mi.sachsen-anhalt.de
Schleswig-Holstein	Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung des Landes Schleswig-Holstein Abteilung IV 7 Düsternbrooker Weg 92 24105 Kiel Telefon: 0431-9883500 Telefax: 0431-9883503 Internet: http://www.verfassungsschutz.schleswig-holstein.de E-Mail: verfassungsschutz.schleswig-holstein@im.landsh.de
Thüringen	Amt für Verfassungsschutz beim Thüringer Ministerium für Inneres und Kommunales Postfach 45 01 21 99051 Erfurt Telefon: 0361-573313-850 Telefax: 0361-573313-482 Internet: http://www.verfassungsschutz.thueringen.de E-Mail: afvkontakt@tmik.thueringen.de

Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik in Unternehmen (VS-IT-Richtlinien / U - VSITR/U)

Die vorliegenden IT-Richtlinien gelten für Unternehmen und Einzelpersonen, die sich gegenüber dem Bundesministerium für Wirtschaft und Technologie (BMWi) zur Einhaltung der Vorschriften des Handbuchs für den Geheimschutz in der Wirtschaft (GHB) verpflichtet haben. Aufgrund dieser Richtlinien kann es sinnvoll sein, allgemeine IT-spezifische Maßnahmen in einer betriebsinternen Anweisung festzulegen.
Der Begriff Informationstechnik (IT) umfasst im folgenden Geräte und Verfahren, die auf elektronischer Grundlage zur automatischen Erfassung, Darstellung, Speicherung, Verarbeitung oder Übermittlung von Informationen in Form von Texten, Daten, Bildern oder Sprache dienen.

I. Allgemeiner Teil

§ 1 Zweck und Anwendungsbereich

(1) Die Richtlinien regeln, welche Maßnahmen zur Geheimhaltung von VS beim Einsatz von Informationstechnik (IT) ergänzend zu den Regelungen des GHB zu treffen sind.
(2) Die Richtlinien sind anzuwenden, wenn VS-VERTRAULICH oder höher eingestufte VS mit IT verarbeitet oder übertragen werden. Sie richten sich an
- Unternehmen und
- Personen, die selbständig tätig oder in Unternehmen beschäftigt sind und die IT für die Verarbeitung, Speicherung oder Übertragung von VS nutzen oder Tätigkeiten an IT-Systemen ausüben, bei denen sie sich Zugang zu VS verschaffen können oder die für den Geheimschutz beim Einsatz von IT für VS zuständig sind.

§ 2 Begriffsbestimmungen

Im Sinne dieser Richtlinien umfasst
- "VS-Datenträger" ein Speichermedium, das VS enthält,
- "Kryptosystem" alle Mittel, die für eine bestimmte Kryptierung und Dekryptierung benötigt werden (z. B. Kryptogerät und Kryptodaten),
- "Kryptodaten" eine Folge von Zeichen, die als Parameter zum Kryptieren und Dekryptieren benötigt werden,
- "IT-Sicherheitsfunktion" eine mit IT realisierte Sicherheitsvorkehrung, insbesondere zur Kryptierung, Abstrahlsicherheit, Zugriffskontrolle, Beweissicherung, Protokollauswertung, Wiederaufbereitung oder Wahrung der Unverfälschtheit von Software.

II. Zuständigkeiten

§ 3 Verantwortliche/r für IT-Geheimschutzmaßnahmen

Unternehmen mit komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS bestimmen eine/n IT-VS-Beauftragte/n mit IT-Fachkenntnissen, der/die den/die SiBe bei der Umsetzung dieser Richtlinien unterstützt. Er/sie soll nicht zugleich Aufgaben eines Systemadministrators bei für VS eingesetzten IT-Systemen wahrnehmen und soll in der Durchführung dieser Richtlinien durch BMWi besonders geschult sein. Sofern der/die IT-VS-

Beauftragte Funktionen des/der betrieblichen Datenschutzbeauftragten wahrnimmt, darf er/sie nicht gleichzeitig Aufgaben des/der SiBe ausüben, die sich auf personenbezogene Daten nach dem SÜG beziehen. Wird ein/e IT-VS-Beauftragte/r nicht bestimmt, so verbleiben dessen/deren Aufgaben bei dem/der SiBe.

§ 4 Aufgaben von BMWi bei der Umsetzung dieser Richtlinien

(1) BMWi berät die Unternehmen bei der Umsetzung dieser Richtlinien und führt Schulungen durch. Insbesondere wird die Notwendigkeit von Zulassungen nach § 14 Abs. 2 oder davon abweichenden Maßnahmen durch BMWi festgestellt und, falls erforderlich, durch das BMWi veranlasst. BMWi kann zu seiner Unterstützung andere Stellen, insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), hinzuziehen.

(2) Zur Umsetzung dieser Richtlinien kann BMWi weitere Hinweise herausgeben, die sich insbesondere auf folgendes erstrecken:
- Hinweise zur Erstellung von IT-Geheimschutz-Anweisungen,
- Maßnahmen gegen kompromittierende Abstrahlung,
- Verwendung von Passworten und Personenidentifikationsnummern (PIN),
- Installation von Hardware, die für VS eingesetzt werden soll,
- Sicherung von Leitungen für die unkryptierte Übertragung von VS,
- Schutz von IT-Betriebsräumen und Produkten mit IT-Sicherheitsfunktionen,
- Überprüfung neuer oder geänderter Betriebs- / Anwendungssoftware,
- Überprüfung der Geheimschutzmaßnahmen vor Freigabe von IT für VS,
- Durchführung technischer Prüfungen.

III. IT-Planung

§ 5 IT-Planung und -Beschaffung

(1) Ist geplant, IT für VS einzusetzen, so ist der/die SiBe bzw. der/die IT-VS-Beauftragte bereits zu Planungsbeginn zu beteiligen. Bei komplexen IT-Systemen oder vielfältigen IT-Anwendungen für VS soll BMWi frühzeitig beratend hinzugezogen werden.

(2) Bereits vor der Beschaffung von IT bzw. vor der Modifizierung vorhandener IT, die für VS eingesetzt wird, muss - im Einvernehmen mit BMWi - festgelegt werden, welche IT-Sicherheitsfunktionen das IT-System enthalten muss und welche Sicherheitsleistungen die IT-Hersteller / -Vertreiber zu erbringen haben. Es ist insbesondere zu beachten, dass
- Produkte mit IT-Sicherheitsfunktionen amtlich zugelassen sein müssen,
- Produkte mit IT-Sicherheitsfunktionen, sobald feststeht, dass sie für VS eingesetzt werden sollen, geschützt aufbewahrt und transportiert werden müssen,
- eine sicherheitsgerechte Wartung und Instandsetzung der IT-Systeme erfolgt.

§ 6 IT-Geheimschutz-Anweisung

(1) In einer IT-Geheimschutz-Anweisung (ITGA) ist das Sicherheitskonzept für die eingesetzte IT zu beschreiben. Folgende Unterlagen sind Teil der ITGA:
- Übersicht über die
  -- VS-Projekte, die mit dem IT-System bearbeitet werden (sollen),
  -- VS-Einstufungen der Daten / Programme,

  - -- eingesetzte/vorgesehene IT (z.B. Hardware, Betriebssysteme, Anwendungssoftware, Datenträger) und die darin enthaltenen IT-Sicherheitsfunktionen.
  - Systemspezifische Verfahrensanweisungen für den Betrieb der IT-Systeme, insbesondere Benennung der berechtigten Nutzer, der Systemverwalter und sonstigen Funktionsträger sowie
  - Geheimschutzvorkehrungen für den Notfall, Störungsfall oder Schadensfall.

(2) Die ITGA muss BMWi zur Genehmigung zugeleitet werden. Der VS-Betrieb der IT-Systeme darf erst nach Genehmigung durch BMWi aufgenommen werden. Alle Änderungen in bezug auf Hardware, Software, Organisation, Anwendungsbereich und (räumliche) Umgebung sind in der ITGA zu ergänzen. Sofern diese geheimschutzrelevant sind, ist erneut die Genehmigung von BMWi einzuholen.

IV. IT-Einsatz
§ 7 Zugangs - / Zugriffskontrolle und Zugriffsrechte

(1) IT-Systeme, die für VS eingesetzt werden, müssen über ein Zugangs- und Zugriffskontrollsystem verfügen, das sicherstellt, dass nur Befugte im Rahmen der ihnen erteilten Zugriffsrechte Zugang erhalten und auf VS zugreifen können. Wiederholt abgewiesene Zugangs-/Zugriffsversuche sollen für diesen Nutzer zur Systemsperrung führen, die nur von hierzu besonders beauftragten Personen aufgehoben werden darf.

(2) Bei der Vergabe, Änderung und Rücknahme von Zugriffsrechten muss gewährleistet sein, dass
  - der Antrag dazu von einer berechtigten Stelle stammt (z.B. Projektleiter),
  - die zu berechtigende Person ausreichend VS-ermächtigt ist,
  - der Grundsatz "Kenntnis nur, wenn nötig" beachtet wird und
  - keine sicherheitsmäßig unvereinbare Bündelung von Funktionen entsteht.

  Die Übertragung der Befugnis zur Vergabe und Änderung von Zugriffsrechten bedarf der Zustimmung des/der IT-VS-Beauftragten.

(3) Die Vergabe, Änderung und Rücknahme von Zugriffsrechten ist so zu dokumentieren, dass jederzeit feststellbar ist, wer zu welchen Zeiten
  - zur Vergabe, Änderung oder Rücknahme von Rechten in welchem Umfang berechtigt war und
  - welche für den Geheimschutz relevanten Rechte ausüben konnte.

  Die Dokumentation ist mindestens fünf Jahre aufzubewahren.

(4) Zur Identifizierung/Authentisierung eingesetzte Mittel eines Rechteinhabers in Form von
  - Besitz (z.B. Chipkarten) sind wie Schlüssel zu VS-Verwahrgelassen und
  - Wissen (z.B. PIN oder Passwort) sind wie Zahlenkombinationen zu VS-Verwahrgelassen

  zu behandeln. Besitzmittel können anstelle der Aufbewahrung in einem VS-Schlüsselbehälter auch in persönlichem Gewahrsam gehalten werden. Einzelheiten über die Auswahl, Vergabe, Kontrolle und den Wechsel von Passworten/PIN sind in der ITGA festzulegen.

(5) Anstelle der in Absatz 1 bis 4 genannten Maßnahmen können auch andere Schutzvorkehrungen getroffen werden (z. B. Betrieb in einem VS-Aktensicherungsraum), soweit damit ein vergleichbarer Schutz erreicht wird.

§ 8 Beweissicherung und Protokollauswertung

(1) Für VS eingesetzte IT-Systeme sollen, über eine automatische Beweissicherung
- abgewiesene Zugangs-/Zugriffsversuche,
- Ausdrucke, Ausgaben von VS auf Datenträger und Übermittlungen von VS sowie
- Zugriffe auf VS-Daten

aufzeichnen.
Es soll möglich sein, sicherheitserhebliche Ereignisse bezogen auf einzelne Benutzer, Benutzergruppen und zugriffsgeschützte Objekte zuverlässig und nachvollziehbar aufzubereiten.

(2) Abgewiesene Zugangs-/Zugriffsversuche sollen vom IT-System unmittelbar dem/der IT-VS-Beauftragten oder einem/einer von ihm/ihr Beauftragten angezeigt oder revisionssicher protokolliert werden. Ausdrucke und Ausgaben von VS auf Datenträger, die zur Weitergabe an Dritte oder zur Archivierung bestimmt sind, sowie Übermittlungen von VS sind vom IT-System oder auf andere Weise der VS-Registratur anzuzeigen.

(3) Der Zugriff auf die Aufzeichnungen nach Absatz 1 sowie ihre Löschung darf nur durch den/die IT-VS-Beauftragte/n oder eine/n von ihm/ihr Beauftragte/n durchgeführt werden. Die Aufzeichnungen sind, soweit keine zwingenden Gründe entgegenstehen, nach Überprüfung durch den/die IT-VS-Beauftragte/n oder eine/n von ihm/ihr Beauftragte/n zu löschen.

(4) Falls keine automatische Beweissicherung möglich ist, sind manuelle Protokolle zumindest über
- die VS-Bearbeitungszeiten der berechtigten Nutzer bzw. Zeiten, zu denen an VS-IT-Systemen gearbeitet wurde und
- Ausdrucke und sonstige Ausgaben (z.B. auf Datenträger) oder Übermittlungen von VS (gilt nicht für VS-Zwischenmaterial)

zu erstellen. Im Einzelfall können weitere Aufzeichnungen gefordert werden.

§ 9 Wiederaufbereiten, Löschen und Vernichten von VS-Datenträgern

(1) VS-Datenträger mit unkryptierten VS sind vor einer Wiederverwendung durch IT-Nutzer ohne Zugriffsberechtigung zu allen gespeicherten Daten so aufzubereiten, dass eine Kenntnisnahme des früheren Inhalts nicht möglich ist. Beim Wiederanlauf von IT-Systemen sowie bei Wartungs- und Instandsetzungsarbeiten muss sichergestellt sein, dass Unbefugte keine Kenntnis von VS erhalten.

(2) Nicht mehr benötigte VS-Datenträger, die eingestufte VS unkryptiert enthalten haben, sind physikalisch zu löschen oder zu vernichten.

§ 10 Schutz der Software und Testläufe

(1) Für VS eingesetzte Betriebs- / Anwendungssoftware soll so geschützt sein, dass Veränderungen durch Unbefugte erkennbar werden (Gewährleistung der Unverfälschtheit).

(2) Der Einsatz neuer oder geänderter Betriebs- / Anwendungssoftware sowie Testläufe sind dem/der IT-VS-Beauftragten rechtzeitig vorher anzuzeigen, der/die
- bei neuer oder geänderter Betriebs- / Anwendungssoftware feststellt, ob eine Überprüfung erforderlich ist und im Bedarfsfall entscheidet, wie diese zu erfolgen hat, und
- bei Testläufen sicherstellt, dass diese nicht während der VS-Verarbeitung / Übertra-

gung durchgeführt werden, grundsätzlich nicht mit VS erfolgen und dass Geheimschutzvorkehrungen nicht beeinträchtigt werden.

Soweit wesentliche Beeinträchtigungen des Geheimschutzes möglich sind, ist der Einsatz von Betriebs-/Anwendungssoftware bis zur Vorlage eines positiven Prüfergebnisses und die Durchführung von Testläufen untersagt.

§ 11 Systemwartung

(1) Vor Wartungs- oder Instandsetzungsarbeiten sollen die VS aus dem IT-System entfernt werden. Ist dies nicht möglich, ist entsprechend ermächtigtes Wartungs- oder Instandsetzungspersonal einzusetzen oder dieses durch geeignetes Fachpersonal zu beaufsichtigen. Während der VS-Verarbeitung / -Übertragung ist eine Wartung oder Instandsetzung des IT-Systems grundsätzlich nicht zulässig.

(2) Eine Fernwartung durch eigenes Personal ist zulässig, wenn
- für die Übertragungen im Rahmen der Fernwartung für VS zugelassene Kryptosysteme eingesetzt werden und
- eine zuverlässige Zugriffskontrolle, Beweissicherung und Überprüfung der Aufzeichnungen erfolgt.

Die Fernwartung soll grundsätzlich nicht während der VS-Verarbeitung / -Übertragung durchgeführt werden. Dabei müssen alle im IT-System zugänglichen VS-Daten kryptiert oder entfernt werden.

(3) Sofern die Fernwartung durch ein anderes Unternehmen durchgeführt werden soll, muss zusätzlich zu den unter (2) genannten Bedingungen
- BMWi für das (die) jeweilige(n) Projekt(e) zustimmen,
- ein Sicherheitsbescheid von BMWi über dieses Unternehmen vorliegen,
- jeder Fernwartungsvorgang durch das eigene Unternehmen gesondert freigeschaltet und beendet werden.

§ 12 Abstrahlsicherheit

(1) IT-Hardware, die VS unkryptiert führt, ist unter Beachtung der Hinweise von BMWi zu installieren.

(2) Durch den amtlichen VS-Auftraggeber ist festzustellen, ob kompromittierende Abstrahlung zu einem untragbaren Sicherheitsrisiko führt. Die abschließende Entscheidung über die Erforderlichkeit von Maßnahmen gegen kompromittierende Abstrahlung obliegt BMWi. Sofern Maßnahmen erforderlich sind, muss die IT-Hardware
- in amtlich zugelassenen abstrahlsicheren Räumen oder Behältern betrieben werden,
- eine amtliche Zulassung für den Betrieb innerhalb einer bestimmten Sicherheitszone aufweisen und innerhalb einer solchen betrieben werden, oder
- vom BSI als abstrahlsicher zugelassen sein.

Sofern nur in sehr geringem Umfang - maximal 20 Std. pro Monat zu unregelmäßigen Zeiten - mit kompromittierender Abstrahlung zu rechnen ist, kann im Einvernehmen mit BMWi auf weitergehende Maßnahmen verzichtet werden.

§ 13 Speicherung, Übertragung und Netzanbindung

(1) VS sind bei Speicherung und Übertragung zu kryptieren. Bei der Speicherung von VS

auf Rechnern ohne Anbindung an oder Zugang zu einem anderen Kommunikationsnetz ist eine Kryptierung nicht erforderlich, wenn die VS materiell gemäß GHB gesichert sind. Bei der Übertragung von VS kann die Kryptierung außerdem unterbleiben,

- innerhalb eines zutrittsgeschützten IT-Betriebsraumes, oder
- wenn die Übertragungseinrichtungen so geschützt sind, dass ein Zugriff Unbefugter unverzüglich erkannt wird (approved circuits), oder
- wenn in einem lokalen Netz maximal GEHEIM eingestufte VS übertragen werden und
  - -- ein Zugriffskontrollsystem nach **§ 7** Abs. 1 eingesetzt ist,
  - -- die Übertragungseinrichtungen sich vollständig in einem Bereich mit zuverlässiger Zutrittskontrolle befinden oder außerhalb nach Nummer 2 geschützt sind.

Bei Verbindung mit einem anderen Kommunikationsnetz muss dieses und die Verbindung zu diesem mindestens wie ein lokales Netz geschützt sein.

(2) Soweit die für den Betrieb eines Kryptosystems benötigten Kryptodaten nicht automatisch bereitgestellt werden, dürfen diese nur von amtlichen Stellen oder in deren Auftrag hergestellt werden. BMWi teilt den Unternehmen im Bedarfsfall die jeweils zuständige Stelle mit. Für die Verwaltung von auf dem Kurier-/Postweg bereitgestellten Kryptodaten ist ein/eine Kryptoverwalter/in und Vertreter/in zu bestellen. Der/die Kryptoverwalter/in gibt die Kryptodaten in die Kryptosysteme ein oder bei Bedarf an die befugten IT-Nutzer aus. Namen und Anschrift des/der Kryptoverwalters/in und Vertreters/in sowie Änderungen sind BMWi mitzuteilen. BMWi leitet die Angaben - sofern erforderlich - an die für die Herstellung und Verteilung von Kryptodaten zuständige Stelle weiter.

§ 14 Zulassung von Produkten mit IT-Sicherheitsfunktionen

(1) Produkte mit Funktionen zur Kryptierung, Abstrahlsicherheit, Löschung oder Vernichtung von VS-Datenträgern oder Sicherung von Übertragungsleitungen (approved circuits) müssen vom BSI zugelassen sein. Die in der Zulassung angegebenen Einsatz- und Betriebsbedingungen sind zu beachten.

(2) Produkte mit Funktionen zur Zugriffskontrolle, Beweissicherung und Protokollauswertung oder Wiederaufbereitung oder Unverfälschtheit von Software sollen vom BSI zugelassen sein. BMWi kann die Verwendung anderer Produkte erlauben, wenn keine geeigneten zugelassenen oder geprüften Produkte verfügbar sind und eine Zulassung oder Prüfung nicht oder nicht zeitgerecht veranlasst werden kann. In diesem Fall sind Produkte zu bevorzugen, die ein amtlich anerkanntes Prüfzertifikat aufweisen.

(3) Die Zulassungen/Prüfungen erfolgen abgestuft nach der Schutzbedürftigkeit von IT-Anwendungen für VS auf der Grundlage allgemein anerkannter Sicherheitskriterien und Verfahren, die bei Bedarf um besondere Prüfungen zum Schutz vor nachrichtendienstlichen Angriffen zu ergänzen sind.

§ 15 Schutz von IT-Betriebsräumen und Produkten mit IT-Sicherheitsfunktionen

(1) Räume, in denen VS unkryptiert verarbeitet oder übertragen werden, sind gegen unbemerkten Zutritt Unbefugter zu schützen.

(2) Produkte mit IT-Sicherheitsfunktionen sind ab dem Zeitpunkt, zu dem feststeht, dass sie für VS eingesetzt werden sollen,

- in Räumen nach Absatz 1 oder entsprechend geschützten Räumen aufzubewahren,
- unter ständiger Kontrolle von VS-ermächtigtem Personal zu transportieren oder so

zu verpacken, dass ein Zugriff Unbefugter erkennbar wird,
- durch VS-ermächtigtes Personal zu installieren, zu warten und instand zu setzen, soweit nicht durch organisatorische Maßnahmen (z.B. keine Verarbeitung/Übertragung von VS in Anwesenheit von Personen und Beaufsichtigung dieser) ein Zugang zu VS auszuschließen ist, und
- in einem gesonderten Verzeichnis nachzuweisen (z. B. in der ITGA).

§ 16 Kennzeichnung von VS

(1) Bei der Darstellung von VS - z. B. Schriftgut - auf Sichtgeräten soll sich, soweit möglich, der Geheimhaltungsgrad auf jeder Seite oder Darstellung deutlich vom dargestellten Inhalt abheben (z.B. durch größere Schrift und Fettdruck); einer farblichen Unterscheidung bedarf es nicht.
(2) VS-Ausdrucke müssen gemäß 6.4 GHB gekennzeichnet sein. Davon abweichend braucht sich der Geheimhaltungsgrad farblich nicht vom ausgedruckten Inhalt zu unterscheiden. Bei STRENG GEHEIM oder GEHEIM eingestuften VS ist der Geheimhaltungsgrad jedoch auf der ersten Seite in roter Farbe anzubringen; ausgenommen VS-Zwischenmaterial, das nicht an Dritte weitergegeben wird.
(3) Datenträger mit unkryptierten VS sind mit dem höchsten Geheimhaltungsgrad der darauf gespeicherten VS gemäß GHB zu kennzeichnen. Bei fest installierten Datenträgern kann hierauf verzichtet werden. Die Kennzeichnung ist für kryptierte VS nicht erforderlich.

§ 17 Nachweis von VS

(1) Gespeicherte VS brauchen nicht einzeln nachgewiesen zu werden, ausgenommen die Fälle nach **§ 8** Abs. 2 Satz 2. Bei Übertragung von VS an Dritte genügt eine elektronische Empfangsbestätigung.
(2) Ausdrucke von VS sind unverzüglich der VS-Registratur zuzuleiten und im VS-Bestandsverzeichnis zu registrieren, ausgenommen VS-Zwischenmaterial, das nicht an Dritte weitergegeben wird.
(3) VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem VS-Bestandsverzeichnis nachzuweisen. Zur Erfassung genügt die Angabe eines Ordnungskriteriums (z.B. fortlaufende Nummer) sowie des Einsatzbereichs (Organisationseinheit, IT-Nutzer) und eine Kurzangabe des Aufgabengebiets. VS-Datenträger sind grundsätzlich nur gegen Quittung weiterzugeben.

§ 18 Datensicherung und Wiederanlauf

(1) Im Rahmen der Datensicherung hinterlegte VS-Daten (einschließlich VS-eingestufter Programme) sind gemäß den VS-Vorschriften zu behandeln. Sind die VS-Daten kryptiert, sind die zum Dekryptieren benötigten Kryptodaten gesondert und entsprechend ihrer VS-Einstufung aufzubewahren.
(2) Bei Wiederanlauf-Vorkehrungen sind die erforderlichen Geheimschutzmaßnahmen einzubeziehen.

§ 19 Überprüfung der Maßnahmen und Freigabe von IT für VS

(1) Bevor ein IT-System erstmals für VS eingesetzt wird, hat der/die IT-VS-Beauftragte zu prüfen, ob die erforderlichen Geheimschutzmaßnahmen getroffen sind.
(2) Der/die IT-VS-Beauftragte entscheidet über die Freigabe des IT-Systems für VS. Grundsätzlich darf die Freigabe erst nach Genehmigung der entsprechenden ITGA durch BMWi erfolgen. Die Freigabe ist zu dokumentieren.
(3) Alle geheimschutzrelevanten Änderungen bei freigegebenen IT-Systemen bedürfen der vorherigen Zustimmung des/der IT-VS-Beauftragten. Die Änderungen sind in der ITGA zu dokumentieren. Bei wesentlichen Änderungen muss erneut die Genehmigung von BMWi eingeholt werden.

§ 20 Kontrollen/Auswertungen

(1) Der/die IT-VS-Beauftragte veranlasst in angemessenen zeitlichen Abständen schwerpunktmäßige Kontrollen. Es ist insbesondere zu kontrollieren, ob
- IT-Sicherheitskomponenten sicherheitsgerecht eingesetzt, gewartet und instandgesetzt werden,
- Zugriffsrechte in der erteilten Form erforderlich sind,
- Zugriffsrechte im IT-System korrekt zugewiesen sind und
- die Mittel zur Identifizierung / Authentisierung vorschriftsgemäß geschützt sind.

(2) Die protokollierten Daten im Rahmen der Beweissicherung sind regelmäßig daraufhin zu überprüfen, ob
- Zugangs-/Zugriffsversuche durch Unbefugte oder versuchte Rechteüberschreitungen vorgekommen sind und
- Zugriffe auf VS-Daten offensichtlich ungerechtfertigt erfolgten.

(3) Die Ergebnisse der Kontrollen sind zu dokumentieren.

§ 21 Technische Prüfungen

(1) Der/die IT-VS-Beauftragte hat bei IT-Systemen, die für VS eingesetzt werden in angemessenen zeitlichen Abständen folgende technischen Prüfungen zu veranlassen:
- Prüfung des IT-Systems unter den spezifischen Einsatzbedingungen, ob die erforderlichen IT-Sicherheitsfunktionen
  -- sachgerecht implementiert sind, keine erkennbaren Manipulationen aufweisen und auch nach Implementierung in das jeweilige IT-System wirksam greifen und nicht über einen Systemweg manipuliert oder umgangen werden können und
  -- auch bei einem Verbund mit anderen IT-Systemen diese Sicherheit aufweisen,
- Abstrahlsicherheits- und Manipulationsprüfungen bei abstrahlsicheren Räumen / Behältern, bei zonenvermessenen Räumen und bei für VS eingesetzter Hardware. Sofern sich Anhaltspunkte für technische Mängel ergeben, sind diese unverzüglich BMWi anzuzeigen.

(2) Für die Verarbeitung von STRENG GEHEIM eingestufte VS kann BMWi im Einzelfall besondere Regelungen für technische Prüfungen festlegen.

V. Schlussbestimmungen
§ 22 Sicherheitsvorkommnisse

(1) Wenn beim IT-Einsatz für VS oder im Zusammenhang damit bekannt wird oder der Verdacht entsteht, dass
- Unbefugte Zugriff auf VS erhalten haben oder ihn sich verschaffen wollten,
- IT-Systeme / -Komponenten sicherheitserhebliche Mängel aufweisen, manipuliert oder entwendet wurden oder
- die Geheimhaltung von VS in anderer Weise verletzt wurde oder gefährdet ist,

ist unverzüglich der/die IT-VS-Beauftragte zu benachrichtigen.

(2) Der/die IT-VS-Beauftragte veranlasst bei Gefahr im Verzuge die unmittelbar erforderlichen Maßnahmen. Er/sie hat bei Feststellung schwerwiegender Mängel bis zu deren Beseitigung den IT-Einsatz für VS einzuschränken oder zu untersagen. Der/die SiBe ist unverzüglich zu unterrichten.

(3) Sicherheitsvorkommnisse und daraufhin veranlasste Maßnahmen sind zu dokumentieren. Die Dokumentation ist mindestens fünf Jahre aufzubewahren.

§ 23 IT-Geheimschutzdokumentation

Es ist eine IT-Geheimschutzdokumentation zu führen, die
- IT-Geheimschutz-Anweisungen (ITGA's) und Freigabebestätigungen für IT-Systeme und zugrundeliegende Prüfungsergebnisse, für jeweils fünf Jahre sowie
- Dokumentationen der Vergabe, Änderung und Rücknahme von Zugriffsrechten, Kontroll-/Prüfberichte und Berichte über Sicherheitsvorkommnisse für jeweils fünf Jahre

enthält.

Zusatzvereinbarung zum (Arbeits-)Vertrag zwischen dem/der Verpflichteten und dem Unternehmen

Herr/Frau

wurde durch die Ermächtigungsurkunde des Bundesministeriums für Wirtschaft und Klimaschutz vom unter Hinweis auf die Strafbarkeit einer Geheimnisverletzung im Sinne des § 353 b Abs. 2 Strafgesetzbuch zur Geheimhaltung aller Angelegenheiten verpflichtet, die von einer amtlichen Stelle oder auf deren Veranlassung als geheimhaltungsbedürftig gekennzeichnet oder ihm/ihr gegenüber auf andere Weise entsprechend bezeichnet worden sind. Die Strafbarkeit einer Geheimnisverletzung nach anderen Vorschriften bleibt unberührt. Der/Die Verpflichtete hat die Anleitung für die Geheimhaltung in der Wirtschaft erhalten.

Das Unternehmen erklärt und der/die Verpflichtete erkennt an, dass die Pflicht des/der Verpflichteten zur Geheimhaltung zugleich Bestandteil des (Arbeits-)Vertrages ist.

Der/die Verpflichtete erklärt außerdem, dass er/sie bei der Nutzung des Internets (z.B. innerhalb sozialer Netzwerke wie Facebook, Xing o.ä.) mit der Preisgabe persönlicher Informationen sehr zurückhaltend sein wird und keine vertraulichen Informationen über das Unternehmen oder die übertragene Aufgabe preisgibt, die einen Rückschluss auf die VS-Ermächtigung zulassen können. Soweit dem/der Verpflichteten im Unternehmen die Funktion des Sicherheitsbevollmächtigten, des VS-IT-Beauftragten, des VS-Verwalter oder eine entsprechende Vertreterfunktion übertragen worden ist, erklärt der/die Verpflichtete, keine Informationen in das Internet einzustellen, die einen Rückschluss auf die besondere herausgehobene Stellung im Geheimschutz erkennen lassen.

_____,	_____
Ort, Datum	Unternehmen
_____,	_____
Ort, Datum	Verpflichteter/e

Zusatzvereinbarung zum Arbeitsvertrag/Dienstvertrag/Werkvertrag bei der VS-Ermächtigung von Personen, die aufgrund einer Abstellungsvereinbarung in einem anderen Unternehmen tätig sind

Herr/Frau

ist bei dem Unternehmen
beschäftigt (Beschäftigungsunternehmen)

Aufgrund der Abstellungsvereinbarung vom

ist er/sie seit dem

in dem Unternehmen
zur Dienstleistung eingesetzt (Einsatzunternehmen)

Herr/Frau

wurde im Hinblick auf seine/ihre Tätigkeit bei dem Einsatzunternehmen mit der Ermächtigungsurkunde des Bundesministeriums für Wirtschaft und Klimaschutz vom unter Hinweis auf die Strafbarkeit einer Geheimnisverletzung im Sinne des § 353 b Abs. 2 Strafgesetzbuch zur Geheimhaltung aller Angelegenheiten des Einsatzunternehmens verpflichtet, die von einer amtlichen Stelle oder auf deren Veranlassung als geheimhaltungsbedürftig gekennzeichnet oder ihm/ihr gegenüber auf andere Weise entsprechend bezeichnet worden sind. Die Strafbarkeit einer Geheimnisverletzung nach anderen Vorschriften bleibt unberührt. Der/Die Verpflichtete hat die Anleitung für die Geheimhaltung in der Wirtschaft erhalten.

Die Pflicht zur Geheimhaltung besteht auch gegenüber den Vorgesetzten und Mitarbeitern des Beschäftigungsunternehmens, soweit eine Kenntnisnahme nicht zur Durchführung eines VS-Auftrages erforderlich ist. Das Beschäftigungsunternehmen verzichtet darauf, derartige Informationen zu verlangen.

Das Beschäftigungsunternehmen und das Einsatzunternehmen erklären und der/die Verpflichtete erkennt an, dass er/sie während seiner/ihrer Abstellung in allen Geheimschutzangelegenheiten, die das Einsatzunternehmen betreffen, ausschließlich der Weisungsbefugnis des Einsatzunternehmens unterliegt und in VS-Angelegenheiten nur für dieses Einsatzunternehmen tätig sein darf. Ansonsten bleibt das Weisungsrecht gegenüber der/dem Verpflichteten beim Beschäftigungsunternehmen.

Das Beschäftigungsunternehmen und das Einsatzunternehmen unterrichten sich gegenseitig unverzüglich über persönliche Veränderungen und nachträgliche Erkenntnisse. Die Nachberichtspflichten gegenüber dem Bundesministerium für Wirtschaft und Klimaschutz übernimmt das Beschäftigungsunternehmen/Einsatzunternehmen[1].

[1] Nichtzutreffendes bitte streichen

Das Beschäftigungsunternehmen erklärt und der/die Verpflichtete erkennt an, dass auch die gegenüber dem Einsatzunternehmen bestehenden Pflichten zur Geheimhaltung Bestandteil des Arbeitsvertrages/Dienstvertrages/Werkvertrages sind.

Das Beschäftigungsunternehmen erklärt und der /die Verpflichtete willigt ein, dass der/die Sicherheitsbevollmächtigte des Einsatzunternehmens die Vollständigkeit und Richtigkeit der Angaben in der Sicherheitserklärung prüft und hierzu auch, soweit dies erforderlich ist, die Personalunterlagen des Beschäftigungsunternehmens beiziehen darf.

Der/die Verpflichtete erklärt, dass er/sie bei der Nutzung des Internets (z.B. innerhalb sozialer Netzwerke wie Facebook, Xing o.ä.) mit der Preisgabe persönlicher Informationen sehr zurückhaltend sein wird und keine vertraulichen Informationen über das Einsatzunternehmen oder den übertragenen Auftrag preisgibt, die einen Rückschluss auf die VS-Ermächtigung zulassen können.

Der/ die Verpflichtete willigt ein, dass seine/ihre Sicherheitsakte bei dem/der Sicherheitsbevollmächtigten des Einsatzunternehmen geführt wird.

, _____ _____

Ort, Datum Beschäftigungsunternehmen

, _____ _____

Ort, Datum Verpflichteter/e

, _____ _____

Ort, Datum Einsatzunternehmen

Zusatzvereinbarung zum Vertrag mit freien Mitarbeitern/innen

Herr/Frau

(Name, Vorname**)**

wurde durch die Ermächtigungsurkunde des Bundesministeriums für Wirtschaft und Klimaschutz vom unter Hinweis auf die Strafbarkeit einer Geheimnisverletzung im Sinne des § 353 b Abs. 2 Strafgesetzbuch zur Geheimhaltung aller Angelegenheiten verpflichtet, die von einer amtlichen Stelle oder auf deren Veranlassung als geheimhaltungsbedürftig gekennzeichnet oder ihm/ihr gegenüber auf andere Weise entsprechend bezeichnet worden sind. Die Strafbarkeit einer Geheimnisverletzung nach anderen Vorschriften bleibt unberührt. Der/Die Verpflichtete hat die Anleitung für die Geheimhaltung in der Wirtschaft erhalten.

Der VS-Auftraggeber erklärt und der/die Verpflichtete erkennt an, dass er/sie während seiner/ihrer Tätigkeit als freier/e Mitarbeiter/in in allen Geheimschutzangelegenheiten der Weisungsbefugnis des VS-Auftraggebers unterliegt und in VS-Angelegenheiten nur für diesen VS-Auftraggeber tätig sein darf. Der/Die freie Mitarbeiter/in verpflichtet sich, dem VS-Auftraggeber jede personelle Veränderung unverzüglich mitzuteilen.

Der/die Verpflichtete erklärt, dass er/sie bei der Nutzung des Internets (z.B. innerhalb sozialer Netzwerke wie Facebook, Xing o.ä.) mit der Preisgabe persönlicher Informationen sehr zurückhaltend sein wird und keine vertraulichen Informationen über den VS-Auftraggeber oder den übertragenen Auftrag preisgibt, die einen Rückschluss auf die VS-Ermächtigung zulassen können.

Der VS-Auftraggeber erklärt und der/die Verpflichtete erkennt an, dass die Pflicht des/der freien Mitarbeiters/in zur Geheimhaltung zugleich Bestandteil des Vertrages mit dem/der freien Mitarbeiter/in ist. Der/Die freie Mitarbeiter/in willigt ein, dass seine/ihre Sicherheitsakte beim VS-Auftraggeber geführt wird.

,

Ort, Datum — VS-Auftraggeber

,

Ort, Datum — freier/e Mitarbeiter/in

GHB - Anlage 41

Erklärung

zur Datenübermittlung zwischen

.....

(Beschäftigungsunternehmen)

und

.....

((verbundenem Unternehmen) (kapitalmäßige Beteiligung/Konzernzugehörigkeit))

Ich bin/ Wir sind darüber unterrichtet, dass die Übermittlung personenbezogener Daten der Betroffenen aus der Sicherheitsüberprüfung zwischen

.....(Beschäftigungsunternehmen)

und

.....(verbundenem Unternehmen)

nur insoweit zulässig ist, als dies für die Erfüllung der Aufgaben nach dem Sicherheitsüberprüfungsgesetz erforderlich ist und dass eine Datenübermittlung zwischen Beschäftigungsunternehmen und verbundenem Unternehmen wie eine Datenübermittlung an Dritte zu behandeln ist.

.....

.....

.....

.....

(Ort, Datum, Namen und Unterschriften der Mitarbeiter, die die Sicherheitsakten führen)

Kennzeichnung einer GEHEIM eingestuften Verschlusssache (VS)

1. Eine GEHEIM eingestufte VS ist am oberen und unteren Rand mit dem Geheimhaltungsgrad in roter Farbe zu kennzeichnen. Sollte eine VS aus mehreren Seiten bestehen, ist die Kennzeichnung am oberen und unteren Rand jeder beschriebenen Seite durchzuführen. Entsprechendes gilt auch für eingestufte Anlagen.

2. GEHEIM eingestufte VS müssen folgende Angaben enthalten:

   a) Erstellendes Unternehmen (sog. Ersteller), Ortsangabe, Datum

   b) VS-Tgb.-Nr. mit Jahreszahl und Abkürzung „Geh.“.

      Auf dem Deckblatt oder der ersten Seite ist die Gesamtzahl der Seiten und die Zahl der Seiten mit unterschiedlicher VS-Einstufung anzugeben (z.B. Gesamtzahl der Seiten 20; davon 8 geh., 4 VS-Vertr. und 8 VS-NfD). Die erste Seite trägt immer den höchsten Geheimhaltungsgrad der VS.

   c) Alle beschriebenen Seiten – ggf. auch die der Anlagen – sind zu nummerieren. Bei doppelseitig bedruckten VS sind nicht beschriebene Rückseiten in die Nummerierung einzubeziehen (Aufdruck: - LEERSEITE -).

   d) Jede GEHEIM eingestufte VS muss eine Ausfertigungsnummer erhalten. Im VS-Tagebuch (und falls verwendet auch im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis) sind alle gefertigten Ausfertigungen und das Original (z.B. als „O“, Aktenexemplar) einzutragen. Die Ausfertigungsnummer sowie die Gesamtseitenzahl der VS ist auf der ersten Seite anzugeben.

3. Auf der VS ist der Zeitpunkt des Ablaufs der VS-Einstufung zu bestimmen. Die Regelfrist für die Einstufung der VS beträgt 30 Jahre. Der öffentliche VS-Herausgeber kann jedoch je nach Schutzbedürftigkeit kürzere oder längere Fristen bestimmen. Die Frist endet mit Ablauf des Jahres, in welches das Fristende fällt. Sie wird durch Änderungen der Einstufung grundsätzlich nicht verändert. Die Einstufungsfrist ist auf der ersten Seite der VS und auf allen Ausfertigungen mit folgendem Vermerk anzugeben: *„Die VS-Einstufung endet mit Ablauf des Jahres …“*. Lässt die Beschaffenheit einer VS die Kennzeichnung nicht zu, ist sinngemäß zu verfahren (z.B. Kennzeichnung in der zugehörigen Dokumentation). Bestimmt der VS-Herausgeber eine Verlängerung der Frist für die Einstufung, ist diese auf der VS zu vermerken.

Beispiel eines Briefes mit VS-Inhalt

GEHEIM
auf amtliche Veranlassung geheim gehalten
Die VS-Einstufung endet mit Ablauf des Jahres 2050

Geheimhaltungsgrad mit dem Zusatz „auf amtliche Veranlassung geheim gehalten“ in roter Farbe durch Stempel oder Druck am oberen und unteren Rand jeder beschriebenen Seite

Ende der Einstufungsfrist

Musterfirma GmbH
Elektrotechnische Werkstätten
Sanddornstraße 8
22040 Hamburg

TEL.-ZENTRALE	(040) 3667 - 1
BEARBEITET VON	Musterfirma GmbH
TEL	(040) 3667 - 268
FAX	(040) 3667 - 222
E-MAIL	
UNSER ZEICHEN	Dr.W.Kr E-230 Tgb.-Nr. 2/20 Geh.
DATUM	Hamburg, 3. August 2020

Geschäftszeichen und Tagebuchnummer mit Abkürzung des Geheimhaltungsgrades

Datum

Seite 1 von 2

Seitenzahl

1 Ausfertigung
2 Seiten, davon 2 Seiten Geh.

Ausfertigungsnummer

Gesamtseitenanzahl

Bundesministerium für Wirtschaft und Klimaschutz
z. Hd. Herrn Konrad Muster o.V.i.A.
Referat RS 3
53107 Bonn

Ihr Zeichen ZS-2380 Tgb.-Nr. 95/19 Geh.
Ihre Nachricht vom 12.12.2019

Betreff: Geheimschutz in der Wirtschaft
hier: Auftrag ‘Entwicklung K 2‘

Bezug: Schreiben des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung vom 3.12.2019
- ZA 13 – 06-20-01 – Tgb.-Nr. 186/19 – Geh.

Anrede,

- T e x t -

GEHEIM
auf amtliche Veranlassung geheim gehalten
Die VS-Einstufung endet mit Ablauf des Jahres 2050

GEHEIM
auf amtliche Veranlassung geheim gehalten
Die VS-Einstufung endet mit Ablauf des Jahres 2050

Geheimhaltungsgrad mit dem Zusatz „auf amtliche Veranlassung geheim gehalten“ in roter Farbe durch Stempel oder Druck am oberen und unteren Rand jeder beschriebenen Seite

Seite 2 von 2

- T e x t -

Ende der Einstufungsfrist

Mit freundlichen Grüßen

GEHEIM
auf amtliche Veranlassung geheim gehalten
Die VS-Einstufung endet mit Ablauf des Jahres 2050

Kennzeichnung einer VS-VERTRAULICH eingestuften Verschlusssache (VS)

1. Eine VS-VERTRAULICH eingestufte VS ist am oberen Rand mit dem Geheimhaltungsgrad in schwarzer oder blauer Farbe zu kennzeichnen. Sollte eine VS aus mehreren Seiten bestehen, ist die Kennzeichnung am oberen Rand jeder beschriebenen Seite durchzuführen. Entsprechendes gilt auch für eingestufte Anlagen.

2. VS-VERTRAULICH eingestufte VS müssen folgende Angaben enthalten:

   a) Erstellendes Unternehmen (Ersteller), Ortsangabe, Datum

   b) VS-Tgb.-Nr. mit Jahreszahl und Abkürzung „VS-Vertr.“.

      Auf dem Deckblatt oder der ersten Seite ist die Gesamtzahl der Seiten und die Zahl der Seiten mit unterschiedlicher VS-Einstufung anzugeben (z.B. Gesamtzahl der Seiten 20; davon 12 VS-Vertr. und 8 VS-NfD). Die erste Seite trägt immer den höchsten Geheimhaltungsgrad der VS.

   c) Alle beschriebenen Seiten – ggf. auch die der Anlagen – sind zu nummerieren. Bei doppelseitig bedruckten VS sind nicht beschriebene Rückseiten in die Nummerierung einzubeziehen (Aufdruck: - LEERSEITE -).

   d) Jede VS-VERTRAULICH eingestufte VS muss eine Ausfertigungsnummer erhalten. Im VS-Tagebuch (und falls verwendet auch im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis) sind alle gefertigten Ausfertigungen und das Original (z.B. als „O“, Aktenexemplar) einzutragen. Die Ausfertigungsnummer sowie die Gesamtseitenzahl der VS ist auf der ersten Seite anzugeben.

3. Auf der VS ist der Zeitpunkt des Ablaufs der VS-Einstufung zu bestimmen. Die Regelfrist für die Einstufung der VS beträgt 30 Jahre. Der öffentliche VS-Herausgeber kann jedoch je nach Schutzbedürftigkeit kürzere oder längere Fristen bestimmen. Die Frist endet mit Ablauf des Jahres, in welches das Fristende fällt. Sie wird durch Änderungen der Einstufung grundsätzlich nicht verändert. Die Einstufungsfrist ist auf der ersten Seite der VS und auf allen Ausfertigungen mit folgendem Vermerk anzugeben: *„Die VS-Einstufung endet mit Ablauf des Jahres …“.* Lässt die Beschaffenheit einer VS die Kennzeichnung nicht zu, ist sinngemäß zu verfahren (z.B. Kennzeichnung in der zugehörigen Dokumentation). Bestimmt der VS-Herausgeber eine Verlängerung der Frist für die Einstufung, ist diese auf der VS zu vermerken.

Beispiel eines Briefes mit VS-Inhalt

VS-VERTRAULICH
auf amtliche Veranlassung geheim gehalten
Die VS-Einstufung endet mit Ablauf des Jahres 2050

Geheimhaltungsgrad mit dem Zusatz „auf amtlich Veranlassung geheim gehalten“ in schwarzer oder blauer Farbe durch Stempel oder Druck am oberen Rand jeder beschriebenen Seite

Ende der Einstufungsfrist

Musterfirma GmbH
Elektrotechnische Werkstätten
Sanddornstraße 8
22040 Hamburg

TEL.-ZENTRALE	(040) 3667 - 1
BEARBEITET VON	Musterfirma GmbH
TEL	(040) 3667 - 268
FAX	(040) 3667 - 222
E-MAIL	
UNSER ZEICHEN	Dr.W.Kr E-230 Tgb.-Nr. 2/20 VS-Vertr.
DATUM	Hamburg, 3. August 2020

Geschäftszeichen und Tagebuchnummer mit Abkürzung des Geheimhaltungsgrades

Datum

Seite 1 von 2

Seitenzahl

1 Ausfertigung
2 Seiten, davon 2 Seiten VS-Vertr.

Ausfertigungsnummer

Gesamtseitenanzahl

Bundesministerium für Wirtschaft und Klimaschutz
z. Hd. Herrn Konrad Muster o.V.i.A.
Referat RS 3
53107 Bonn

Ihr Zeichen ZS-2380 Tgb.Nr. 95/19 VS-Vertr.
Ihre Nachricht vom 12.12.2019

Betreff: Geheimschutz in der Wirtschaft
hier: Auftrag ‘Entwicklung K 2‘

Bezug: Schreiben des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung vom 3.12.2019
- ZA 13 – 06-20-01 – Tgb.-Nr. 186/19 – VS-Vertr.

Anrede,

- T e x t -

VS-VERTRAULICH
auf amtliche Veranlassung geheim gehalten
(Die VS-Einstufung endet mit Ablauf des Jahres 2050)

Geheimhaltungsgrad mit dem Zusatz „auf amtliche Veranlassung geheim gehalten“ in schwarzer oder blauer Farbe durch Stempel oder Druck am oberen Rand jeder beschriebenen Seite

Seite 2 von 2

Ende der Einstufungsfrist

- T e x t -

Im Auftrag

Beispiel eines Briefes mit VS-Inhalt[1]

VS-VERTRAULICH
auf amtliche Veranlassung geheimgehalten

Silesia GmbH
Elektrotechnische Werkstätten
Sanddornstraße 8
22040 Hamburg,

3. August 2020

Bundesministerium für Wirtschaft und Energie
z. Hd. Herrn Konrad Muster o.V.i.A.
Referat RS 3
53107 Bonn

1. Ausfertigung
1 Seite, davon 1 Seite VS-Vertr.
Die VS-Einstufung endet mit Ablauf des Jahres 2050

Ihr Zeichen	Ihre Nachricht	Unser Zeichen	Telefon:
ZS-2380	vom 5.2.2019	Dr.W.-Kr.	(040) 3667 - 1
Tgb.-Nr.		E-230	(Zentrale)
25/19 VS-Vertr.		Tgb.-Nr.	Durchwahl: - 268
		2/20 VS-Vertr.	Telefax:
			(040) 3667-222

Betrifft: Geheimschutz in der Wirtschaft;
hier: VS-Auftrag ‘Entwicklung K 2“

Bezug: Schreiben des BAAINBw vom 3.12.2018
- ZA 13 - 06-20-01 - Tgb.-Nr. 186/18 - VS-Vertr.

Anrede,

- T e x t - (eingestuft)

Mit freundlichen Grüßen

[1] Geheimhaltungsgrade in der vorgeschriebenen Farbe

Kennzeichnung unterschiedlich eingestufter Verschlusssachen (VS)

1. Unterschiedliche VS-Einstufungen sind auf dem Deckblatt, auf der ersten Seite der VS oder in einem gesonderten Inhaltsverzeichnis zu dokumentieren. Die Gesamteinstufung der VS richtet sich nach dem höchsten VS-Einstufungsgrad. Dieser ist auf der ersten Seite zu vermerken. Bei der Gesamtzahl der Seiten sind auch die als OFFEN eingestuften Teile der VS mitzuzählen.
2. Anfang und Ende unterschiedlich eingestufter Teile einer VS müssen klar erkennbar sein. Elektronische Datenträger erhalten insgesamt immer den höchsten Einstufungsgrad, die eine Information hat, die auf ihnen gespeichert ist.

Beispiel für eine unterschiedlich eingestufte VS[1]

GEHEIM
auf amtliche Veranlassung geheimgehalten

Die Verschlusssache umfasst mit / ohne Anschreiben insgesamt 20 Seiten.
Punkt 1: 5. 1-3 GEHEIM
Punkt 2: 5.4-8 VS-VERTRAULICH
Punkt 3: 5. 9-20 Offen

Niederschrift

über die Besprechung am:

Punkt 1: Seite 1-3	Text	GEHEIM auf amtliche Veranlassung geheimgehalten
Punkt 2: Seite 4-8	Text	VS-VERTRAULICH auf amtliche Veranlassung geheimgehalten
Punkt 3: Seite 9-20	Text	Offen

GEHEIM
auf amtliche Veranlassung geheimgehalten

[1]Geheimhaltungsgrade in der vorgeschriebenen Farbe

Leitfaden für unternehmensinterne VS-Vervielfältigungsanweisungen

Unternehmensinterne VS-Vervielfältigungsanweisungen müssen auf der Grundlage der Bestimmungen des GHB und dieser Rahmenvorschrift erstellt werden.

Die VS-Vervielfältigungsanweisungen müssen mindestens folgenden Grundforderungen entsprechen:

1. Geltungsbereich der unternehmensinternen VS-Vervielfältigungsanweisung

Angabe der Abteilungen/Betriebsstätten/Werke, für die die unternehmensinterne VS-Vervielfältigungsanweisung gilt.

2. Anwendungsbereich

(1) Vervielfältigungen im Sinne dieser Rahmenvorschrift sind Druckerzeugnisse und sonstige Abdrucke, Fotokopien, Abschriften, Auszüge oder Vervielfältigungen von VS-Schriftgut (einschließlich VS-Zeichnungen o.ä.).

(2) Die Vervielfältigungsanweisung gilt nicht für die Mikroverfilmung von VS, für die erforderlichenfalls eine besondere unternehmensinterne Anweisung herausgegeben werden muss.

(3) Die Weitergabe und das Vervielfältigen von VS im Rahmen der Fernübertragung ist unverschlüsselt nicht zulässig. Im übrigen wird auf 6.10. GHB hingewiesen.

3. Hinweis auf die Zulässigkeit der Vervielfältigung von VS

(1) VS der Geheimhaltungsgrade GEHEIM oder VS-VERTRAULICH dürfen ohne Einwilligung des amtlichen VS-Auftraggebers vervielfältigt werden, soweit dies zur Durchführung des VS-Auftrages notwendig ist und der amtliche VS-Auftraggeber nichts anderes verfügt hat. Bei der Beurteilung der Notwendigkeit der VS-Vervielfältigung und bei der Festlegung der Anzahl der zu erstellenden Kopien ist restriktiv zu verfahren und der Grundsatz „Kenntnis nur, wenn nötig“ zu beachten.

(2) Die Vervielfältigung von STRENG GEHEIM ist nicht gestattet, es sei denn, der VS-Herausgeber hat eingewilligt.

4. Anordnungsbefugte Personen

Anordnungsbefugte Personen müssen VS-ermächtigt und sollen grundsätzlich nur Angehörige der fachlich zuständigen Stellen in leitender Funktion sein, z.B. Projektleiter, Leiter der Entwicklungsabteilungen, der/die SiBe bzw. dessen/deren Vertreter/in.

Der/die SiBe führt über anordnungsbefugte Personen ein Verzeichnis in mindestens zweifacher Ausfertigung. Je ein Exemplar muss bei dem/der SiBe und in der VS-Registratur aufbewahrt werden.

Das Verzeichnis muss enthalten: Name und Vorname der anordnungsbefugten Personen und deren Unterschriftsprobe.

5. Antragsverfahren für VS-Vervielfältigungen

(1) Vervielfältigungen von VS sind schriftlich bei der zuständigen anordnungsbefugten Person zu beantragen. Hierbei ist die Verwendung eines dem Muster der Anlage 46 GHB entsprechenden Formulars vorzusehen. Anzahl und Empfänger der Vervielfältigungen sind auf der vervielfältigten VS oder auf dem Auftragsformular zu verfügen.

(2) VS-Vervielfältigungsaufträge dürfen der VS-Vervielfältigungsstelle grundsätzlich nur über die VS-Registratur oder den/die SiBe zugeleitet werden, falls der/die VS-Verwalter/in diese Arbeiten nicht selbst erledigt.

Alle VS-Unterlagen (Original, Vervielfältigungen, Über- und Fehldrucke) sowie des VS-Zwischenmaterials (z.B. Folien usw.) sind - nach Registrierung auf dem VS-Vervielfältigungsauftrag - an die VS-Registratur zu geben.

6. Genaue Orts-/Raumbezeichnung und Öffnungszeiten der für die VS-Vervielfältigung zugelassenen Vervielfältigungsstellen

(1) VS-Vervielfältigungsarbeiten dürfen nur mit Kopiergeräten/Vervielfältigungsautomaten und in Räumen durchgeführt werden, die für die VS-Vervielfältigung in der unternehmensinternen Anweisung zugelassen sind. Bei allen anderen Vervielfältigungsgeräten, die in Gebäuden oder in der Nähe von Stellen stehen, in denen VS bearbeitet werden, ist durch Aushänge darauf hinzuweisen, dass die Vervielfältigung von VS nicht gestattet ist.

(2) Vervielfältigungen von VS dürfen nur in Gegenwart von mindestens zwei VS-Ermächtigten durchgeführt werden (Vier-Augen-Prinzip). Während der Dauer der Vervielfältigung von VS dürfen sich nur entsprechend VS-Ermächtigte an der Vervielfältigungsstelle aufhalten. Bei häufiger oder länger andauernder Vervielfältigung von VS ist die Vervielfältigungsstelle für die Dauer der VS-Vervielfältigung zur VS-Kontrollzone zu erklären.

(3) Für die Vervielfältigung von VS dürfen nur Geräte benutzt werden, bei denen gewährleistet ist, dass nach Beendigung der VS-Vervielfältigung eine Reproduktion der vervielfältigten VS oder ein sonstiges Lesbarmachen nicht mehr möglich ist.

7. Hinweise für die Behandlung der VS-Vervielfältigungen

7.1 Kennzeichnung der VS-Vervielfältigungen

Vervielfältigungen sind von der VS-Registratur vorschriftsmäßig so zu kennzeichnen, dass sich die VS-Ausfertigungsnummern der einzelnen Kopien bei unternehmenseigenen VS deutlich von der Ausfertigung des Originals unterscheiden. Unternehmensfremde VS erhalten bei Ablichtungen als Unterscheidungskriterien eine zweite arabische Zahl nach der Ausfertigungsnummer (z.B. 4.1.) oder eine fortlaufende römische Zahl als Hochzahl (z.B. $4.^{I.}$). Bei Vervielfältigungen von VS der Einstufung GEHEIM oder STRENG GEHEIM ist jede Seite oben und unten mit dem entsprechenden zusätzlichen Stempelaufdruck in roter Farbe zu versehen.

7.2 Registrierung der VS-Vervielfältigungen

Unmittelbar nach Eingang in der VS-Registratur sind die VS-Vervielfältigungen in das VS-Bestandsverzeichnis bzw. in den VS-Ausfertigungs-/VS-Vervielfältigungsnachweis einzutragen. Im VS-Bestands-

verzeichnis ist die Anzahl der erstellten Kopien und ggf. die Nummer und die Seite des evtl. benutzten VS-Ausfertigungs/VS-Vervielfältigungsnachweises zu vermerken.

7.3 Weitergabe der VS-Vervielfältigungen

Erst nach Eintragung in das VS-Bestandsverzeichnis bzw. in den VS-Ausfertigungs- / VS-Vervielfältigungsnachweis dürfen die vervielfältigten VS dem/der Antragssteller/in durch die VS-Registratur gegen Empfangsquittung (VS-Quittungsbuch) übergeben werden.

7.4 Vernichtung von VS-Zwischenmaterial

Bei der Durchführung von Vervielfältigungsarbeiten anfallendes VS-Zwischenmaterial (z.B. Fehl- oder Überdrucke) ist auf dem VS-Vervielfältigungsauftragsformular zu vermerken und an die VS-Registratur zur unverzüglichen vorschriftsmäßigen Vernichtung zu geben.

7.5 Sammlung der VS-Vervielfältigungsaufträge

Nach Erledigung der Vervielfältigungsarbeiten sind die angefallenen VS-Vervielfältigungsaufträge von der VS-Registratur fünf Jahre aufzubewahren.

7.6 Manuelle VS-Vervielfältigungen

Sofern im Einzelfall VS manuell vervielfältigt werden (abschreiben, abzeichnen usw.), regelt der/die SiBe das Verfahren in sinngemäßer Anwendung dieser Rahmenvorschrift.

8. Kontrolle durch den/die SiBe

Der/die SiBe kontrolliert nachweisbar in unregelmäßigen Zeitabständen stichprobenweise die Einhaltung dieser Rahmenvorschrift.

GHB – Anlage 46

....den.....
(Name u. Abteilung des/der Antragsstellers/in)

VS—Vervielfältigungsauftrag Nr.:...../.....

für Ausfertigungen / Vervielfältigungen von VS

(bitte vollständig ausfüllen und Nichtzutreffendes streichen)

1. An die
   VS-Vervielfältigungsstelle
   - über VS-Registratur –

   Ich bitte, die beigefügte Verschlusssache zu vervielfältigen.

   .....
   (genaue Bezeichnung der VS)
   Tgb.-Nr.:...../..... Ausf.-Nr.:..... Seitenzahl.....

Gewünschte Kopierart und Anzahl:

Kopienart	Vervielfältigung DIN A 3 / 4 / 5	(Blau-)Pause / Transparent	Sonstige Kopienart:.....
Anzahl der Kopien			

.....
Unterschrift des/der Anordnungsbefugten

2. Die Kopie(n) wurde(n) wie oben angegeben gefertigt.
3. Es ist/sind.....Blatt Über-/Fehldruck(e) angefallen.

   ....
   Unterschrift des / der Vervielfältigers/in Unterschrift des / der Zeugen/in

4. Kopie(n) ist - sind - ordnungsgemäß gekennzeichnet und im VS-Tagebuch sowie ggf. im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis registriert worden. In Ziffer 3. aufgeführte Über-/Fehldrucke wurden vernichtet.

   .....
   (Unterschrift des/der VS-Verwalters/in)

Hinweise zum VS-Vervielfältigungsauftrag

1. Vervielfältigungen sind nur an den durch den/die SiBe hierfür bestimmten, gegebenenfalls in einer VS-Vervielfältigungsanweisung bezeichneten Stelle und in Gegenwart eines weiteren entsprechend VS-Ermächtigten zulässig (Vier-Augen-Prinzip). Die Anzahl der VS-Vervielfältigungen und die Vernichtung von gegebenenfalls entstandenem VS-Zwischenmaterial ist durch Unterschrift der Beteiligten auf dem VS-Vervielfältigungsauftrag zu bestätigen.

2. Vervielfältigungen von STRENG GEHEIM eingestuften VS sind nicht zulässig. Ausnahmen bedürfen der Einwilligung des VS-Herausgebers.

3. Soweit der VS-Herausgeber nicht anders verfügt hat, entscheidet der/die zur Anordnung von VS-Vervielfältigungen Befugte über die Anzahl der nötigen VS-Vervielfältigungen von GEHEIM oder VS-VERTRAULICH eingestuften VS und unterschreibt den VS-Vervielfältigungsauftrag. Gegebenenfalls ist eine Verfügung des VS-Herausgebers, die die VS-Vervielfältigung von seiner Zustimmung abhängig macht, zu beachten.

4. Das Original einer VS darf nur einmal erstellt werden, wird als Ausfertigung nicht gezählt und ist im VS-Bestandsverzeichnis zu registrieren.

5. VS-Vervielfältigungen sind unverzüglich im VS-Tagebuch zu registrieren und werden nur über die VS-Registratur ausgehändigt. Wird neben dem VS-Tagebuch ein VS-Ausfertigungs-/VS-Vervielfältigungsnachweis geführt, ist darauf im VS-Tagebuch hinzuweisen.

6. Im VS-Vervielfältigungsauftrag muss die VS und der Umfang der VS-Vervielfältigungen genau bezeichnet werden und verbleibt bei der VS-Registratur.

7. Angefallene Über- bzw. Fehldrucke sind in Ziffer 3 des VS-Vervielfältigungsauftrags zu vermerken und der VS-Registratur bzw. dem/der VS-Verwalter/in zuzuleiten. Dort sind sie sofort ohne Vernichtungsverhandlung zu vernichten.

8. Vervielfältigte VS, die GEHEIM eingestuft sind, sind rot nachzustempeln.

9. VS-Vervielfältigungen (auch auszugsweise) von nicht mittels elektronischer Medien hergestelltem VS-Schriftgut (Kopien, Abdrucke, Abschriften) sind vom/von der SiBe in einer BMWi zur vorherigen Genehmigung vorzulegenden VS-Vervielfältigungsanweisung zu regeln. Für VS-Vervielfältigungen mittels elektronischer Medien (z. B. Fax, Scanner, PC) gelten die VS-IT-Richtlinien.

10. Für alle VS-Vervielfältigungen gilt der Grundsatz „Kenntnis nur, wenn nötig“.

11. Die VS-Vervielfältigungsaufträge sind fünf Jahre aufzubewahren und im VS-Tagebuch unter b) in den Spalten 3 bzw. 4 einzutragen.

GHB - Anlage 47

Deckblatt VS-Tagebuch

Unternehmen: .....

VS-Tagebuch

Nummer:.....

für

Verschlusssachen der Geheimhaltungsgrade

VS-VERTRAULICH und GEHEIM

Dieses VS-Tagebuch umfasst 50 Doppelseiten.
Bei der Führung des VS-Tagebuches sind die Allgemeinen Hinweise zum Führen von VS-Tagebüchern und die Erläuterungen zu beachten.

....

(Angefangen am) (Unterschrift des/der Sicherheitsbevollmächtigten)

Geführt:

von - bis	von (Name)	Unterschrift

.....

(Abgeschlossen am[1])

[1] Es ist das Datum einzutragen, an dem die letzte in diesem VS-Tagebuch noch nicht durchgestrichene Verschlusssache versandt, herabgestuft oder vernichtet worden ist.

Linke Seite VS-Tagebuch

Eingang

Tgb. Nr. / Jahreszahl Geheim-haltungs-grad	Lfd. Nr. der Anlagen	a)Ausferti-gungs-Nr.	a) Vervielfältigungs-Nr. b) Vervielfältigungsauftrags-Nr.	VS-Ausferti-gungs- /VS-Vervielfälti-gungsnach-weis Nr. und Seite	a) Datum b) Ein-gang der VS (bzw. der Anlagen)	a) Einsender / Abteilung b) Tgb. Nr. bei Anlagen: c) Ersteller d) Tgb. Nr. des Erstellers	Gesamtsei-tenzahl, davon GEHEIM, VS-Vertr. VS-NfD, offen, Leerseiten	Bezeich-nung der VS Inhaltsanga-be
1	2	3	4	5	6	7	8	9

Rechte Seite VS-Tagebuch

Ausgang

Weitergabe				a) Höher-/ Herabstufungsverfügung b) Nr. der VS-Vernichtungsverhandlung c) Fristen	Bemerkungen
Ausgangs-Datum	Extern		Intern		
	Empfänger	VS-Empfangsschein a) Nr. b) zurück am	Nr. des VS-Quittungsbuches und lfd. Nr. bzw. Nr. des internen VS-Empfangsscheins		
10	11	12	13	14	15

Allgemeine Hinweise zur Führung von VS-Tagebüchern

1. Auf der ersten Seite ist zu vermerken: Unternehmensname, lfd. Nr. des VS-Tagebuches, von wem und für welchen Zeitraum das VS-Tagebuch geführt wurde bzw. wird. Der/die Sicherheitsbevollmächtigte (SiBe) muss auf der ersten Seite des VS-Tagebuches, bei Karteikarten auf jeder Seite, unterschreiben, bevor Eintragungen vorgenommen werden. Der/die VS-Verwalter/in muss den Empfang der VS-Tagebücher gegenüber dem/der SiBe quittieren.
2. Die Seiten der VS-Tagebücher sind fortlaufend nummeriert. VS-Tagebücher dürfen nach vorheriger Einwilligung des Bundesministeriums für Wirtschaft und Technologie (BMWi) auch in Karteiform geführt werden. Die Karteikarten müssen fortlaufend nummeriert werden (fest eingedruckt), den Unternehmensnamen tragen und vor Ausgabe von dem/der SiBe einzeln unterschrieben worden sein.
3. In den VS-Tagebüchern sind Ein- und Ausgang, Verbleib, Vervielfältigung, Herabstufung und Vernichtung von GEHEIM oder VS-VERTRAULICH eingestuften VS nachzuweisen. In den Nachweisen zu VS-Tgb.Nrn. sind Eingang, Zugang, Bestand, Verbleib und Vernichtung von einzelnen eingestuften Seiten zu VS-Tgb.Nrn. nachzuweisen. STRENG GEHEIM eingestufte VS sind in einem getrennten VS-Tagebuch zu dokumentieren.
4. Jede VS ist mit einer eigenen fortlaufenden VS-Tgb.Nr. und mit allen Ausfertigungen im VS-Tagebuch zu registrieren. Anlagen zu einer VS sind unter der gleichen VS-Tgb.Nr. mit einer zusätzlichen Anlagennummer (z.B. 1/93-1-) oder mit einer eigenen VS-Tgb.Nr. einzutragen.
5. Änderungen der Eintragungen in VS-Tagebüchern müssen erkennbar sein. Sie sind mit Datum und Unterschrift zu versehen. Bei Streichungen muss der ursprüngliche Text lesbar bleiben. Es ist unzulässig, Eintragungen unkenntlich zu machen sowie Blätter zu entfernen oder einzufügen. VS-Tagebücher sind nach Austragung der letzten VS fünf Jahre aufzubewahren.
6. Der/die SiBe führt einen schriftlichen Nachweis über alle im Unternehmen geführten VS-Tagebücher. Wenn für VS-Material, Patente, spezielle Projekte o.ä. gesonderte VS-Tagebücher geführt werden, erhalten die VS-Tgb.Nrn. dieser VS-Tagebücher aus Unterscheidungsgründen einen Zusatzbuchstaben vor der VS-Tgb.Nr. (z.B. P 1/90 für Patente).
7. Der Nachweis von VS kann auch IT-gestützt nach Einwilligung des BMWi erfolgen.

Erläuterungen zum VS-Tagebuch

1. Es ist zweckmäßig, zwischen den einzelnen VS-Tgb.Nrn. mehrere Zeilen freizulassen, damit nachträgliche Ergänzungen möglich sind. Im Regelfall sollten auf einer Seite nicht mehr als zwei VS-Tgb.Nrn. eingetragen werden. Im VS-Tagebuch sind auf der linken Seite (Spalte 1-9) alle Eingänge (von anderen Unternehmen und von Behörden sowie von im eigenen Unternehmen erstellten VS) und auf der rechten Seite (Spalten 10-15), sofern kein VS-Ausfertigungs-/ VS-Vervielfältigungsnachweis geführt wird, alle Ausgänge (einschließlich Herabstufungen und Vernichtungen sowie die Weitergabe im eigenen Unternehmen) einzutragen.
2. Wenn Eintragungen im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis wegen des Umfangs der zu fertigenden Kopien erforderlich sind, werden die Ausgänge der im eigenen Unternehmen hergestellten Ausfertigungen bzw. Vervielfältigungen, die im VS-Tagebuch in Spalte 3 bzw. 4 zusammengefasst einzutragen sind, nicht auf der rechten Ausgangsseite des VS-Tagebuches, sondern nur im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis nachgewiesen. In Spalte 5 des VS-Tagebuches wird vermerkt, in welchem VS-Ausfertigungs/VS-Vervielfältigungsnachweis (lfd. Nr.) und auf welcher Seite die Eintragungen erfolgt sind.
3. Bei Unternehmen mit geringem VS-Aufkommen (weniger als 50 VS-Tgb.Nrn. pro Jahr) empfiehlt es sich, pro Seite nur eine VS-Tgb.Nr. einzutragen. Die im eigenen Unternehmen hergestellten VS-Ausfertigungen oder VS-Vervielfältigungen können dann (ohne dass ein besonderer VS-Ausfertigungs- / VS-Vervielfältigungsnachweis geführt wird) einzeln untereinander (in einer freien Zeile) in Spalte 3 bzw. 4 des VS-Tagebuches eingetragen werden. Ihr Ausgang wird in diesem Fall auf der rechten Seite des VS-Tagebuches in derselben Zeile nachgewiesen.
4. Ausfertigungsnummern werden grundsätzlich bei eigenen, d.h. in dem Unternehmen erstellten VS, Vervielfältigungsnummern bei unternehmensfremden VS vergeben.
5. VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) sind nicht in das VS-Tagebuch einzutragen.
6. Anschreiben, die „ohne Anlagen offen“ sind und von der VS-Registratur keine eigene VS-Tgb.Nr. erhalten, müssen nicht im VS-Tagebuch eingetragen werden.

Spalte 1 Tgb.Nr. / Jahreszahl; Geheimhaltungsgrad:

- In Spalte 1 ist (jährlich mit Nummer 1 beginnend) die lfd. VS-Tgb.Nr. und - getrennt durch einen Schrägstrich - die Jahreszahl einzusetzen. Darunter ist der abgekürzte Geheimhaltungsgrad (geh. oder VS-Vertr.) anzugeben. NATO-VS sind mit NS für NATO SECRET oder NC für NATO CONFIDENTIAL zu registrieren.
- VS-Tgb.Nr. von zusätzlich geführten VS-Tagebüchern erhalten aus Unterscheidungsgründen einen Zusatzbuchstaben vor der VS-Tgb.Nr. (z.B. M 1/90, wenn ein VS-Materialtagebuch geführt wird).

Spalte 2 Lfd. Nr. der Anlagen:

- Jede zu einer VS gehörende eingestufte Anlage erhält eine eigene fortlaufende Nummer, die unter derselben VS-Tgb.Nr. wie die VS, jedoch in Spalte 2 des VS-Tagebuches eingetragen wird (Beispiel: -1- für die erste Anlage; im VS-Eingangsstempel wird z.B. 1/94-1-geh. vermerkt).
- Die Spalte 1 wird bei Anlagen nicht ausgefüllt.
- Anlagen können jedoch auch, wenn es aus Arbeitsgründen zweckmäßig erscheint, mit einer eigenen VS-Tgb.Nr. in das VS-Tagebuch eingetragen werden.

Spalte 3 a) VS-Ausfertigungs Nr.; b) VS-Vervielfältigungsauftrag Nr.:

- In Spalte 3 müssen alle im eigenen Unternehmen erstellten VS erfasst werden, z.B. O (Original/Aktenexemplar) und alle davon hergestellten VS-Ausfertigungen, die jeweils in eine eigene Zeile in Spalte 3 einzutragen sind, falls kein VS-Ausfertigungs-/VS-Vervielfältigungsnachweis geführt wird. Wird ein VS-Ausfertigungs-/VS-Vervielfältigungsnachweis geführt, können die VS-Ausfertigungen bzw. VS-Vervielfältigungen im VS-Tagebuch in einer Zeile eingetragen werden (z.B. 1-20). Der technische Ablauf bei der Herstellung von Kopien ist bei der Erläuterung zu Spalte 4 beschrieben. Die laufende Nr. des VS-Vervielfältigungsauftrages mit der Jahreszahl ist unter b) anzugeben (z.B. 2/94).
- Sollen von VS-Ausfertigungen (nicht vom Original) weitere VS-Vervielfältigungen notwendig werden, sind diese in Spalte 4 einzutragen.
- Ferner ist die VS-Ausfertigungsnummer der von anderen Unternehmen oder Behörden eingegangenen VS (und zugehörigen Anlagen) in dieser Spalte unter a) zu vermerken. Gehen mehrere Ausfertigungen ein, so ist jede Ausfertigung mit ihrer Ausfertigungsnummer untereinander in einer eigenen Zeile einzutragen. In diesem Fall ist b) nicht auszufüllen.
- Fehlt z.B. bei einer von Behörden eingegangenen VS des Geheimhaltungsgrades VS-VERTRAULICH die Ausfertigungsnummer, ist eine unternehmensinterne und als solche kenntlich gemachte Ausfertigungsnummer zu vergeben und entsprechend einzutragen (Beispiel: 1. Ausfertigung – firmenintern oder 1.-f-).

Spalte 4 a) VS-Vervielfältigungs Nr.; b) VS-Vervielfältigungsauftrag Nr.:

- VS-Vervielfältigungen dürfen grundsätzlich nur von bzw. über die VS-Registratur hergestellt werden. VS-Vervielfältigungen erhalten als Unterscheidungskriterium eine fortlaufende arabische Zahl oder eine römische Hochzahl hinter der Ausfertigungsnummer (z.B. 4.1. oder $4.^{I}$) und sind in dieser Spalte unter a) in einer freien Zeile einzutragen.
- Wenn von VS Vervielfältigungen benötigt werden, ist ein VS-Vervielfältigungsauftrag auszufüllen, der von einer anordnungsbefugten Person zu unterschreiben ist. Die Nummer des VS-Vervielfältigungsauftrages mit der Jahreszahl ist unter b) einzutragen (z.B. 2/94). Der Verbleib (Absendung, Vernichtung usw.) ist auf der Ausgangsseite (Spalten 10-14) in derselben Zeile nachzuweisen.

Spalte 5 VS-Ausfertigungs-/VS-Vervielfältigungsnachweis Nr. und Seite:

- Besteht wegen des erheblichen Umfangs der herzustellenden Ausfertigungen oder Vervielfältigungen die Notwendigkeit, einen VS-Ausfertigungs-/VS-Vervielfältigungsnachweis zu führen, so sind im VS-Tagebuch in den Spalten 3 bzw. 4 die erstellten Ausfertigungen bzw. Vervielfältigungen zusammengefasst einzutragen

(z.B. 1.- 40. oder $1.^{I}$. - $1.^{X}$.). In Spalte 5 ist die lfd. Nr. und die Seitenzahl des VS-Ausfertigungs-/VS-Vervielfältigungsnachweises einzutragen (z.B. 2/3 für den 2. Nachweis und die Seite 3). In diesem Fall ist die Ausgangsseite nicht auszufüllen (Spalten 10-14).

Spalte 6 a) Datum; b) Eingang der VS (bzw. der Anlagen):

- In dieser Spalte sind das Ausstellungsdatum und das Eingangsdatum der VS einzutragen. Anlagen können unter einem anderen Datum erstellt sein als die VS, mit der die Anlage übersandt wurde. In diesem Fall ist das Erstellungsdatum der Anlage gesondert zu vermerken.

Spalte 7 a) Einsender/Abteilung; b) Tgb.Nr.; c) Ersteller; d) Tgb.Nr. des Erstellers:

- In Spalte 7 sind der Einsender (Unternehmen oder Behörde) und die Tgb. Nr. des Einsenders sowie bei Anlagen der Ersteller und die Tgb.Nr. des Erstellers zu vermerken.
- Bei VS, die im eigenen Unternehmen erstellt werden, ist als Einsender die Abteilung, in der die VS gefertigt wurde, einzutragen. Die Eintragung der Tgb.Nr. in Spalte 7 entfällt, weil sie in Spalte 1 bereits vermerkt ist.

Spalte 8 Gesamtseitenzahl, davon GEHEIM / VS-VERTRAULICH / VS—NfD / offen / Leerseiten:

- In Spalte 8 ist die Gesamtseitenzahl der jeweiligen VS und gesondert für jede Anlage die Seitenzahl der einzelnen Anlage einzutragen. Bei unterschiedlich eingestuften VS ist die Gesamtseitenzahl entsprechend aufzuschlüsseln. Die Eintragungen im VS-Tagebuch müssen mit den Eintragungen im VS-Eingangsstempel identisch sein.

Spalte 9 Bezeichnung der VS, Inhaltsangabe:

- Hier ist die VS (bzw. die Anlage) mit ihrer Bezeichnung oder ihrer Inhaltsangabe (ggf. stichwortartig) einzutragen.

Genereller Hinweis zu den Spalten 10 bis 13:

- Diese Spalten sind für Eintragungen bei der Weitergabe von VS (Spalte 11 und 12, wenn VS versandt werden; Spalte 13, wenn sie innerhalb des Unternehmens weitergegeben werden) bestimmt.

Spalte 10 Ausgangsdatum:

- Es ist das Versanddatum der VS einzusetzen. Das Versanddatum ist nur bei der externen Weitergabe anzugeben.

Spalte 11 Empfänger:

- Der Empfänger ist anzugeben.

Spalte 12 **VS-Empfangsschein; a)Nr.; b) zurück am:**

- Beim Versand von VS ist die Nummer des der VS-Sendung beizufügenden VS-Empfangsscheines einzusetzen. Nach dem Rücklauf des unterschriebenen VS-Empfangsscheines ist das Datum des Eingangs im Unternehmen zu vermerken. Mindestens einmal wöchentlich ist zu prüfen, ob alle VSEmpfangsscheine zurückgesandt worden sind.

Spalte 13 **Nummer des VS-Quittungsbuches und lfd. Nr. der Eintragung im Quittungsbuch bzw. Nr. des internen VS-Empfangsscheins:**

- Sofern im eigenen Unternehmen die VS länger als einen Tag weitergegeben wird, ist in Spalte 13 die Nummer des VS-Quittungsbuches (falls mehrere VS-Quittungsbücher verwendet werden) und die lfd. Nummer im VS-Quittungsbuch zu vermerken (z.B. 3/13). In diesem Fall muss der Empfänger über ein zugelassenes VS-Verwahrgelass verfügen.
- Wird innerhalb des Unternehmens die VS mit VS-Empfangsschein weitergegeben, so ist die Nummer des **VS-Empfangsscheins** einzutragen. Die Eintragung in Spalte 13 kann entfallen, wenn der Rücklauf der VS an den/die VS-Verwalter/in noch am gleichen Tag erfolgt.
- Wenn der Rücklauf der VS an die VS-Verwaltung noch am gleichen Tag erfolgt oder die VS nur eingesehen wird, ist in Spalte 13 einmalig ein “A“ einzutragen und die jeweilige Ausleihe bzw. Einsichtnahme in einem VS-Quittungsbuch zu vermerken.

Spalte 14 a) **Höher-/Herabstufungsverfügung: Veranlasser und Datum; b) Nummer der VS-Vernichtungsverhandlung; c) Fristen:**

- In dieser Spalte ist unter a) der Veranlasser, der die Höher-/Herabstufung verfügt hat, sowie das Datum und das Geschäftszeichen der Herabstufungsverfügung zu vermerken. Weiterhin sind in dieser Spalte unter c) die auf der 1. Seite einer VS verfügten Fristen der VS-Einstufung einzutragen.
- Bei der Vernichtung einer VS des Geheimhaltungsgrades VS-VERTRAULICH und höher sind schriftliche VS-Vernichtungsverhandlungen anzufertigen. Die Nummer der VS-Vernichtungsverhandlung ist in dieser Spalte unter b) einzutragen (z.B. 2/91 = 2. VS-Vernichtungsverhandlung im Jahre 1991).

Spalte 15 **Bemerkungen:**

- In Spalte 15 können Bemerkungen eingetragen werden (Hinweise auf andere Tgb.Nrn., sachliche Zusammenhänge usw.).

- ♦ Eintragungen in den Spalten 1 - 15 sind diagonal durchzustreichen, wenn alle unter dieser VS-Tgb.Nr. registrierten VS versandt, herabgestuft oder vernichtet worden sind.
- ♦ Zuvor müssen alle Eintragungen über den Verbleib dieser VS (Versendung, Herabstufung, Vernichtung usw.) geprüft werden.
- ♦ Am Ende eines jeden Kalenderjahres ist das VS-Tagebuch für das zurückliegende Jahr abzuschließen.

Unternehmen: .....

VS-Ausfertigungs-/VS-Vervielfältigungsnachweis

Nummer:

über die in dem eigenen Unternehmen hergestellten VS-Ausfertigungen und VS-Vervielfältigungen von Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH und GEHEIM. Dieser Nachweis umfasst 100 Doppelseiten.

....
(Angefangen am) (Unterschrift des/der Sicherheitsbevollmächtigten)

Dieser Nachweis wurde/wird geführt:

von - bis	Name	Unterschrift

.....
(Abgeschlossen am[1])

[1]Es ist das Datum einzutragen, an dem die letzte in diesem Nachweis noch nicht durchgestrichene Verschlusssache versandt, herabgestuft oder vernichtet worden ist.

VS-Ausfertigungs- und VS-Vervielfältigungsnachweis Tgb.-Nr.: Titel:					Externe Weitergabe		Weitergabe im Unternehmen		Seite: Bemerkungen: a) Höher-/ Herabstufungs-verfügung b) Nr. der VS-Ver-nichtungs-verhandlung c) Fristen
Vervielfältigungs-Auftrag-Nr.	Ausfertigungs-Nr.	Vervielfältigungs-Nr.	Empfänger Abteilung	Ausgangsdatum	E-Schein		Quittungs-buch-Nr. und lfd.Nr.	Rückgabe	
					Nr.	zurück am			

Hinweise zum VS-Ausfertigungs-/VS-Vervielfältigungsnachweis

1. Der VS-Ausfertigungs-/VS-Vervielfältigungsnachweis kann für im eigenen Unternehmen hergestellte VS-Ausfertigungen und VS-Vervielfältigungen von VS-VERTRAULICH und GEHEIM eingestuften VS geführt werden.
2. Der Nachweis kann im Einzelfall nach Einwilligung des Bundesministeriums für Wirtschaft und Technologie auch in Karteiform geführt werden. In diesem Fall sind die Karteikarten fortlaufend zu nummerieren; sie müssen die Unterschrift des/der Sicherheitsbevollmächtigten und den Unternehmensstempel aufweisen.
3. Wird eine VS-Ausfertigung bzw. VS-Vervielfältigung mehrfach intern oder extern weitergegeben, dann ist sie jeweils erneut in den VS-Ausfertigungs-/VS-Vervielfältigungsnachweis einzutragen (auch wenn der Empfänger bereits früher dieselbe Kopie in Besitz hatte).
4. Ist eine VS-Tgb.Nr. im VS-Bestandsverzeichnis durchzustreichen, so ist bei der entsprechenden Eintragung im VS-Ausfertigungs-/VS-Vervielfältigungsnachweis analog zu verfahren. Gleiches gilt auch für Karteikarten, deren Führung gesondert zugelassen wurde.
5. Der VS-Ausfertigungs-/VS-Vervielfältigungsnachweis ist fünf Jahre, nachdem die letzte dort nachgewiesene VS versandt, herabgestuft oder vernichtet worden ist, zu verwahren.
6. In der ersten Spalte ist die Nr. des VS-Vervielfältigungsauftrags einzusetzen.
7. In der zweiten Spalte sind die hergestellten VS-Ausfertigungen (von einer im Unternehmen erstellen VS) untereinander (jeweils in einer eigenen Zeile) einzutragen. Wenn von vornherein feststeht, dass ein Empfänger eine bestimmte Anzahl von VS-Ausfertigungen erhält, können die für diesen Empfänger bestimmten VS-Ausfertigungen auch zusammengefasst eingetragen werden (z. Bsp. 1.-20.)
8. VS-Vervielfältigungen von unternehmensfremden und evtl. eigenen VS erhalten eine fortlaufende zweite arabische Zahl hinter der vorgegebenen Ausfertigungsnummer oder eine römische Zahl als Hochzahl (z.B. 4.1. oder 4.$^{I.}$**).** Fehlt bei von Behörden (weil dort nicht zwingend vorgeschrieben) eingegangenen VS die Ausfertigungsnummer und / oder die Angabe der Seitenzahl, so ist im VS-Tagebuch eine als unternehmensintern kenntlich gemachte Ausfertigungsnummer (z.B. 1-f-) zu vergeben und / oder die tatsächliche Zahl der Seiten einzutragen. Die Anzahl der Seiten ist auf der ersten Seite der VS zu vermerken. Entsprechendes gilt für die Anlagen. Unterschiedliche VS-Einstufungen innerhalb einer VS sind detailliert, entsprechend den Vorgaben im VS-Eingangsstempel aufzuführen.
9. Für eine VS-Tgb.Nr. können auch mehrere Seiten des VS-Ausfertigungs-/VS-Vervielfältigungsnachweises verwendet werden.
10. Wird innerhalb eines Unternehmens nicht nur ein VS-Quittungsbuch geführt, so ist bei Weitergabe einer VS sowohl die Nummer des VS-Quittungsbuches als auch dessen laufende Nummer anzugeben (z.B. 1/7)

    Sofern innerhalb des Unternehmens die VS mit einem internen VS-Empfangsschein weitergegeben wird, ist die Nummer des VS-Empfangsscheines einzutragen.

    Die Eintragung für die Weitergabe innerhalb des Unternehmens kann unterbleiben, wenn der Rücklauf der VS an den/die VS-Verwalter/in noch am gleichen Tage der Ausgabe anhand eines VS-Quittungsbuches oder VS-Empfangsscheines nachgewiesen wird. In diesem Fall ist in der Spalte „Weitergabe im Unternehmen“ einmalig ein großes „A“ einzutragen.

GHB - Anlage 49

Kennzeichnung einer eingehenden Verschlusssache (VS) mit dem VS-Eingangsstempel

1. Alle in einem Unternehmen eingehenden VS sind mit einem Aufdruck des VS-Eingangsstempels zu versehen. Ein solcher VS-Eingangsstempel muss daher in jeder VS-Registratur vorhanden sein.
2. Der VS-Eingangsstempel muss folgende Angaben enthalten:
   a) Name des Unternehmens,
   b) Hinweis "VS-Registratur",
   c) Eingangsdatum,
   d) VS-Tgb. Nr. mit Jahreszahl und Abkürzung des Geheimhaltungsgrades "VS-Vertr." oder "geh.",
   e) Ausfertigungsnummer,
   f) Gesamtzahl der Seiten (ggf. auch der Anlagen) und deren (ggf.) Aufteilung auf verschiedene Geheimhaltungsgrade.
3. Auf allen Anlagen ist ein eigener Aufdruck des Eingangsstempels für VS anzubringen.
4. Erhalten Anlagen die VS-Tgb.Nr. des Anschreibens, ist aus Unterscheidungsgründen zusätzlich hinter der VS-Tgb.Nr. (in Beistrichen) eine arabische Zahl (z.B. die 1. Anlage: 1/03-1- geh.) hinzuzufügen.

Beispiel eines Eingangsstempels

Name des Unternehmens	
-VS-Registratur -	
Eing.-Datum:.....	
Tgb. -Nr.:.....	
Ausf.-Nr.:	
Anlagen:.....	
Diese Verschlusssache umfasst:	
insges.	.....Seiten
davon	.....Seiten GEHEIM
	.....Seiten VS-VERTRAULICH
	.....Seiten VS-NfD
	.....Seiten offen
	.....Seiten Leerseiten
.....	.....
Datum	Unterschrift des/der VS-Verwalters/in

Deckblatt VS-Quittungsbuch

Unternehmen:	
Ort:	Datum:

VS-Quittungsbuch

Nummer...../Jahr.....

Geführt von:

Name:	von:	bis:
Name:	von:	bis:
Name:	von:	bis:
Name:	von:	bis:
Name:	von:	bis:

Vollständigkeitsprüfung wurde gemäß 6.6.3 Absatz 4 GHB durchgeführt von:

Name:	am:
Name:	am:
Name:	am:
Name:	am:
Name:	am:

Dieses Buch hat 25 Doppelseiten

Anmerkung:

Linke Seite VS-Quittungsbuch

Lfd. Nr.	VS-Tgb.Nr. Geheimhaltungsgrad	Ausfertigung Seitenzahl	Bezeichnung der Verschlusssache

Rechte Seite VS-Quittungsbuch

erhalten am	Unterschrift des Empfängers	Rückgabe Datum	Unterschrift des/der VS-Verwalters/in

Hinweise zum Quittungsbuch

1. Bei der Weitergabe von VS-VERTRAULICH und höher eingestuften VS innerhalb des Unternehmens ist ein VS-Quittungsbuch (oder ein interner VS-Empfangsschein) zu verwenden.
2. Die Rückgabe einer VS ist auch von dem/der VS-Verwalter/in durch Unterschrift zu bestätigen.
3. Weiterhin hat der/die VS-Verwalter/in Vollständigkeitskontrollen der VS durchzuführen.
4. Das VS-Quittungsbuch ist fünf Jahre nach Rückgabe der letzten ausgeliehenen VS zu verwahren.

GHB - Anlage 51

Adresse absendendes Unternehmen
Zusatz - VS-Registratur-

Name/ Anschrift des Empfängers
gem. Sicherheitsbescheid

Sofort

offen zurück

VS-Empfangsschein Nr. ...../.....

VS-Tgb. Nr.	**Datum der VS**	**Ausf.-Nr. und Seitenzahl der VS**	**Anlagen**		**Seitenzahl insgesamt**
			Nr. der Anlage	**Ausf. u. Seitenzahl**	
Versandart: zugelassenes Transportunternehmen/Kurier **.....** **Abgesandt am:**			**Empfangen am:**		

.....
(Unternehmensstempel der VS-Registratur des Absenders, an die der VS-Empfangsschein zurückgesandt werden soll)

.....
(Unterschrift und Unternehmens-stempel/Dienstsiegel des Empfängers; der Name ist in Maschinenschrift zu wiederholen)

Hinweise zum VS-Empfangsschein

1. Bei der Versendung von VS der Geheimhaltungsgrade GEHEIM und VS-VERTRAULICH ist im inneren Umschlag ein ausgefüllter VS-Empfangsschein beizufügen. Adressat ist der / die im Sicherheitsbescheid genannte Empfangsberechtigte/r (VS-Verwalter/in), über dessen/deren Anwesenheit sich die abgebende Stelle vor der Versendung zu vergewissern hat, der / die Geheimschutzbeauftragte in einer Behörde (Zusatz: o.V.i.A.) oder der Sicherheitsoffizier bei Dienststellen der Bundeswehr.
2. Der VS-Empfangsschein ist in dreifacher Ausfertigung auszustellen. Die 1. und 2. Ausfertigung erhält der Empfänger. Er quittiert den Empfang der VS und sendet die 1. Ausfertigung an den Absender zurück. Die 2. Ausfertigung behält der Empfänger. Sobald die quittierte 1. Ausfertigung des VS-Empfangsscheines beim Absender eingegangen ist, vernichtet der Absender die bis dahin zu Kontrollzwecken bei ihm verbliebene 3. Ausfertigung. Das Datum des Eingangs des VS-Empfangsscheins ist im VS-Tagebuch in Spalte 12 b) einzutragen.
3. Der/Die VS-Verwalter/in hat die eingegangene VS mit den Angaben auf dem VS-Empfangsschein zu überprüfen. Festgestellte Abweichungen sind entsprechend kenntlich zu machen (mit Namenszeichen und Datum). Er/Sie vermerkt auf dem VS-Empfangsschein das Datum des Empfangstages und unterschreibt ihn. Der VS-Empfangsschein ist ferner mit dem Unternehmensstempel zu versehen und unverzüglich an den Absender offen zurückzusenden. Die quittierte Gesamtzahl der erhaltenen VS ist im VS-Eingangsstempel und im VS-Tagebuch zu vermerken.
4. Geht der VS-Empfangsschein beim Absender der VS nicht innerhalb einer angemessenen Frist (im Inland sieben Arbeitstage) nach Versendung nicht ein, hat er/sie den VS-Empfangsschein anzumahnen. Notfalls ist der/die SiBe einzuschalten, der/die die notwendigen Maßnahmen zu treffen und ggf. das Bundesministerium für Wirtschaft und Technologie zu unterrichten hat.
5. Zurückgegebene VS-Empfangsscheine sind in der VS-Registratur als Nachweis für versandte VS fünf Jahre aufzubewahren.

Unternehmen:	
Ort:	Datum:

VS-Übergabeprotokoll

Heute wurde die VS-Verwaltung von

Name

an

Name

übergeben.

Die VS-Tagebücher, VS-Quittungsbücher und alle sonstigen Nachweise des/der VS-Verwalters/in sowie die Schlüssel zu den VS-Verwahrgelassen, Gefahrenmeldeanlagen und VS-Schlüsselbehältern waren vollzählig vorhanden.

☐ Der Verbleib der VS und ihrer Anlagen wurde vollständig geprüft.
oder
☐ Folgende Eintragungen im VS-Tagebuch und ggf. im VS-Ausfertigungs- / VS-Vervielfältigungsnachweis wurden stichprobenweise geprüft.

(Zutreffendes ankreuzen)

(Fortsetzung s. ggf. Anlage 1)

Beanstandungen (Fortsetzung s. ggf. Anlage 2)

.....
Unterschrift des/der übergebenden VS-Verwalters/in und/oder Zeugen/in (Name)

.....
Unterschrift des/der übernehmenden VS-Verwalters/in (Name)

.....
Gesehen (Unterschrift des/der Sicherheitsbevollmächtigten mit Datum)

Hinweise zum VS-Übergabeprotokoll

1. Beim Wechsel des/der VS-Verwalters/in ist ein VS-Übergabeprotokoll zu fertigen. Dabei ist der/die SiBe einzuschalten. Das VS-Übergabeprotokoll ist von dem/der SiBe oder einem von ihm/ihr Beauftragten/e, der/die nicht an der Verwaltung der VS beteiligt sein darf, in Verwahrung zu nehmen; es ist fünf Jahre aufzubewahren.
2. Es sind alle Unterlagen des/der VS-Verwalters/in (z.B. auch VS-Vernichtungsprotokolle, VS-Empfangsscheine) zu übergeben.
3. Das VS-Übergabeprotokoll ist fünf Jahre zu verwahren.

GHB - Anlage 53

Unternehmen:	
Ort:	Datum:

VS-Vernichtungsverhandlung Nummer Jahr

Heute wurden auf Vollständigkeit geprüft und vernichtet:

Lfd. Nr.	**Heraus-geber**	**Tgb.-Nr. der herausgeben-den Stelle**	**Datum der VS**	**Tgb.-Nr. des eigenen Unternehmens**	**Ausf.-Nr.**	**Seitenzahl**
Vernichtet aufgrund der Anordnung des						**Vom:**

....

(Unterschrift des/der zuständigen VS-Verwalters/in)

(Unterschrift des/der Zeugen/in)

Hinweise zur VS-Vernichtungsverhandlung

1. Bei der Vernichtung von VS ist stets eine VS-Vernichtungsverhandlung zu fertigen. Bei der Austragung der VS im VS-Tagebuch ist in Spalte 14 die Nr. der VS-Vernichtungsverhandlung einzusetzen (z.B. 3/96). Bei allen Arbeiten im Zusammenhang mit der Vernichtung von VS ist das "Vier-Augen-Prinzip" zu beachten, d.h. es müssen stets zwei VS-ermächtigte Unternehmensangehörige anwesend sein und die VS-Vernichtungsverhandlung anschließend unterschreiben.
2. Für jede VS-Tgb.Nr. einer VS ist eine eigene Zeile der VS-Vernichtungsverhandlung zu verwenden. Anlagen einer VS erhalten ebenfalls jeweils eine eigene Zeile. Der Vordruck kann auch erweitert werden. Freibleibende Zeilen sind mit einem Diagonalstrich so zu überziehen, dass nachträgliche Eintragungen erkennbar sind.
3. Die VS-Vernichtungsverhandlung ist fünf Jahre aufzubewahren.

VS-Quittungsbuch für VS-Zwischenmaterial

Genaue Bezeichnung oder Inhaltsangabe des VS-Zwischenmaterials (ggf. Nr. des Auftrags / Projekts)	Seitenzahl oder sonst. Beschreibung	Weitergabe am	Empfänger	Unterschrift des Empfängers	Vermerke (z.B. Hinweis auf die Tgb. -Nr. der endg. VS)

Fortsetzung Seite:

Hinweise zum VS-Quittungsbuch für VS-Zwischenmaterial

1. Wenn VS-Zwischenmaterial auch nach Erstellung der eigentlichen VS noch aufbewahrt werden soll, dann ist es wie die VS von der VS-Registratur ordnungsgemäß zu registrieren. Ab diesem Zeitpunkt darf das “VS-Quittungsbuch für VS-Zwischenmaterial“ nicht mehr verwendet werden.
2. VS-Quittungsbücher für VS-Zwischenmaterial sind fünf Jahre zu verwahren.

Berichtigungsnachweis zu VS-Tgb.Nrn.:............ Ausfertigung vom.....................

Eingang-/ Zugang Abgang / Bestand	Seitenzahl GEHEIM	Seitenzahl VS-Vertr.	Seitenzahl VS-NfD	Seitenzahl offen	Gesamt-seitenzahl	Bemerkungen
Eingang						Grundwerk
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						
Zugang						Berichtigung
Abgang						Vern.Verh.Nr.
Bestand						

. . .

Hinweise zum Berichtigungsnachweis

1. Jedem Grundwerk einer Loseblatt-Sammlung ist der Berichtigungsnachweis vorzuheften. In dem Berichtigungsnachweis sind alle Ergänzungen des Grundwerks zu dokumentieren.
2. Der Berichtigungsnachweis ist zu kennzeichnen wie die VS, jedoch mit dem Zusatz „ohne Anlage offen“.
3. In die 1. Zeile ist der Gesamtbestand des Grundwerks einzutragen, ab Zeile 2 die jeweilige Berichtigung/Ergänzung.
4. Bei herausgenommenen Seiten ist im Falle ihrer Vernichtung die Nummer der VS-Vernichtungsverhandlung in der letzten Spalte einzutragen.
5. Bei der VS-Tgb.Nr. des Grundwerks ist auf den Berichtigungsnachweis hinzuweisen (Spalte 15).
6. Wird das Grundwerk mit den Ergänzungslieferungen insgesamt vernichtet, ist im VS-Tagebuch bei der VS-Tgb.Nr. des Grundwerks diese VS-Vernichtungsverhandlung einzutragen.
7. Die vorhandenen Berichtigungsnachweise müssen als Leerdruck fortlaufend nummeriert werden, den Unternehmensnamen tragen und vor Ausgabe von dem / der Sicherheitsbevollmächtigten einzeln unterschrieben worden sein.
8. Bei den VS-Tgb.Nrn. der Ergänzungslieferungen ist auf den Berichtigungsnachweis beim Grundwerk zu verweisen.

Unternehmen:	
Ort:	Datum:

Inhaltsverzeichnis zum VS-Datenträger

Der VS-Datenträger

Tgb.-Nr. der versendenden Stelle/ Geheimhaltungsgrad	Ausf.-Nr.	Ersteller des VS-Datenträgers	Bezeichnung des VS-Datenträgers

hat folgenden Inhalt:

Anzahl der enthaltenen Dateien		**..... Dateien**			
Bezeichnung der VS	Dateinamen	Größe der Datei in KB	Dateityp	Erstellungs-/Änderungs-Datum	Geheimhaltungs-grad der Datei

..... (Unterschrift des/der zuständigen VS-Verwalters/in)

..... (Unterschrift des/der Erstellers/in des VS-Datenträgers)

Das Inhaltsverzeichnis ist zusammen mit dem VS-Datenträger zu verwahren. Die auf dem VS-Datenträger gespeicherten Daten dürfen nach Erstellung des Inhaltsverzeichnisses nicht mehr gelöscht oder verändert werden. Es dürfen auch keine Daten hinzugefügt werden. Technische Möglichkeiten des Dokumentenschutzes sind für den VS-Datenträger zu nutzen.

Hinweise zum Inhaltsverzeichnis für VS-Datenträger

1. Das Inhaltsverzeichnis zum VS-Datenträger ist dann zu erstellen, wenn dieser versandt werden soll. Die Beförderung von VS-Datenträgern erfolgt entsprechend den Bestimmungen für VS-Schriftgut. Dem VS-Datenträger ist neben dem Inhaltsverzeichnis ein VS-Empfangsschein beizufügen.
2. Abgebende und empfangende Stellen haben den Datenträger im VS-Tagebuch nachzuweisen.
3. Das Inhaltsverzeichnis zum VS-Datenträger ist zusammen mit dem VS-Datenträger solange zu verwahren, bis dieser vernichtet werden kann.

Beschaffung von Stahlschränken, die zur Aufbewahrung von VS geeignet sind

1. Allgemeines

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat technische Anforderungen (BSI 7565, BSI 7566 und BSI 7567) an Stahlschränke zur Aufbewahrung von VS festgelegt. Nur Stahlschränke, die diesen Anforderungen entsprechen, dürfen zur Aufbewahrung von VS verwendet werden und werden von durch das BSI zugelassenen Unternehmen hergestellt und sind als Stahlschränke der Sicherheitsgrade I und II mit der Bezeichnung SG I VS (nach BSI 7566) und SG II VS (nach BSI 7567) lieferbar.

Die allgemeinen Festlegungen sind in den technischen Anforderungen BSI 7565 enthalten. Jeder einzelne Stahlschrank gemäß diesen Anforderungen wird durch den Güteprüfdienst der Telekom vor Auslieferung an den Besteller „gütegeprüft".

Hinsichtlich Größen und Facheinteilung bestehen zwischen der Normalausführung (SG I und SG II) und der Ausführung für VS (SG I VS und SG II VS) keine Unterschiede. Die Ausführung für VS unterscheidet sich jedoch von der Normalausführung insbesondere durch höherwertige Schlösser und ein aufwändigeres Riegelwerk (höherer Sicherheitswert). Außerdem sind die Fachböden eingeschweißt. Verstellbare Einlegeböden sind nicht vorgesehen.

Die lieferbaren Größen und die verschiedenen Möglichkeiten der Facheinteilung ergeben sich aus Anhang 1 und 2.

2. Hersteller von Stahlschränken SG I VS und SG II VS

Die Anschriften der vom BSI zugelassenen Hersteller von Stahlschränken zur Aufbewahrung von VS nach BSI 7566 bzw. BSI 7567 teilt BMWi auf Anfrage mit.

3. Verfahren bei der Bestellung

Die zur Aufbewahrung von VS zugelassenen Stahlschränke SG I VS und SG II VS können bei einem der vom BSI zugelassenen Hersteller bestellt werden. Die Bestellung muss folgende Angaben enthalten:

- Bauausführung (SG I VS oder SG II VS nach BSI 7566 bzw. BSI 7567 in Verbindung mit BSI 7565),
- Größe (Größe 0, Größe 1 oder Größe 2 nach BSI 7565, Abschnitt 2), bei Größe 0: Art der Verankerung (Boden oder Rückwand),
- Facheinteilung (Ausführung A, B, C, D, E nach BSI 7565, Abschnitt 3), Sondereinrichtungen (bei Fachböden müssen die gewünschten Abstände angegeben werden),
- Stückzahl,
- Anschlag für Tür (links oder rechts).

Außerdem muss der Besteller sich bereit erklären, die Kosten der Güteprüfung zu übernehmen.

Die erfolgte Lieferung des Stahlschrankes muss BMWi angezeigt werden.

4. Abnahme eines gelieferten Stahlschrankes nach BSI 7566 / BSI 7567

Der Besteller muss sich nach Lieferung eines Stahlschrankes gemäß BSI 7566 /BSI 7567 davon überzeugen, dass die unter Abschnitt 3 aufgeführten Voraussetzungen erfüllt sind, bevor er darin erstmalig VS deponiert.

5. Veränderungen am SG I VS und SG II VS

Sicherheits- und Kombinationsschlösser dürfen nur durch Fachunternehmen instandgesetzt oder ausgetauscht werden.

Bei Veränderungen genügt der Stahlschrank SG I VS und SG II VS nicht mehr den Anforderungen zur Aufbewahrung von VS, es sei denn BMWi hat diese Veränderungen ausdrücklich gestattet.

6. Stahlschränke, die nicht der BSI 7566 / BSI 7567 entsprechen

Wenn ein Stahlschrank für die Aufbewahrung von VS beschafft werden soll, der nicht der BSI 7566/BSI 7567 entspricht, ist dieser von BMWi dahingehend zu prüfen, ob die „Technischen Anforderungen an VS-Stahlschränke“ erfüllt sind, und ggf. zu genehmigen.

7. Sonderausführungen der Stahlschränke

Für Sonderausführungen von Stahlschränken (z.B. Datensicherungsschränke) ist vor Bestellung die Zustimmung von BMWi einzuholen.

8. VS-Schlüsselbehältnisse

Die Aufbewahrung von Schlüsseln zu VS-Behältnissen erfolgt – vorbehaltlich abweichender Regelungen durch BMWi - in zugelassenen VS-Schlüsselbehältnissen. Hersteller und Typen der zugelassenen Schlüsselbehälter sind bei BMWi zu erfragen.

Die Durchführung einer Güteprüfung liegt im Ermessen des VS-Auftraggebers. Die Lieferung der Schlüsselbehältnisse muss BMWi mitgeteilt werden.

Größen der Stahlschränke SG I VS und SG II VS (BSI 7565, Abschnitt 2)

Sicherheits-grad	Bezeichnung	Größe	Abmessungen[1] Höhe/Breite/Tiefe[2] außen mm	innen mm[3]	Leergewicht (kg) [4]
I[5]	Stahlschrank SG I VS nach BSI 7566 in Verbindung mit BSI 7565	0[6]	550.510.430	450.504.352	65
		1	1350.680.520	1235.670.435	200
		2	1850.840.520	1735.830.435	310
II[7]	Stahlschrank SG II VS nach BSI 7567 in Verbindung mit BSI 7565	0[6]	620.580.560	450.410.355	105
		1	1500.840.685	1300.670.480	460
		2	1850.840.685	1650.670.480	500

1. Toleranzen bei SG I VS und SG II VS: Höhe +/- 5 mm; Breite + 10 mm, Tiefe - 5 mm.
2. Tiefenmaß erhöht sich durch vorstehende Teile (Griffe usw.) um etwa 65 mm (zu beachten bei Schrankbeförderung durch Türen usw.).
3. Innenmaße: In der Breite und Höhe zwischen Innenwandungen gemessen; in der Tiefe zwischen Rückwand und Innenseite der Haupttür gemessen; Tiefe der abschließbaren Innenfächer etwa 35 mm weniger.
4. Gewicht bei Ausführung C (Größe 0 bei Ausführung A).
5. Sicherheitsgrad I: Einwandiger Stahlschrank, Sicherheitsschloss (bei VS-Ausführung zusätzliche Ausstattung u.a. mit einem Kombinationsschloss).
6. Stahlschränke SG I VS bzw. SG II VS der Größe 0 sind nur in Ausführung A (siehe Anhang 2) vorgesehen. Sie müssen mit ihrem Stand- und Anbringungsort (massive Fußböden oder Wände) starr verbunden oder in schwere (mindestens ca. 150 kg!) Möbel fest eingebaut sein (Verschraubung 5 x M 10, Verschweißung oder gleichwertige Verbindung). Die Art der Verankerung ist anzugeben (siehe „Verfahren bei der Bestellung“).
7. Sicherheitsgrad II: Doppelwandiger Stahlschrank, feuerhemmend, Sicherheitsschloß (bei VS-Ausführung zusätzliche Ausstattung u.a. mit einem Kombinationsschloß).

Inneneinrichtung der Stahlschränke SG I VS/ SG II VS
Facheinteilung der unterschiedlichen Ausführungen

Ausführung A		
Stahlschrank	SG I VS, Größe 0	1 Fachboden
und	SG II VS, Größe 1	
Stahlschrank	SG I VS, Größe 1	2 Fachböden
Stahlschrank	SG II VS, Größe1	3 Fachböden
Stahlschrank	SG I VS, Größe 2	4 Fachböden
und	SG II VS, Größe 2	
Ausführung B		
Stahlschrank	SG I VS, Größe 1	2 Fachböden, 1 Innenfach
Stahlschrank	SG II VS, Größe 1	3 Fachböden, 1 Innenfach
Stahlschrank	SG I VS, Größe 2	4 Fachböden, 1 Innenfach
und	SG II VS, Größe 2	
Ausführung C		
Stahlschrank	SG I VS, Größe 1	2 Fachböden, 3 Innenfächer
und	SG II VS, Größe 1	
Stahlschrank	SG I VS, Größe 2	5 Fachböden, 6 Innenfächer
und	SG II VS, Größe 2	
Ausführung D		
Stahlschrank	SG I VS, Größe 1	2 Fachböden, 2 Innenfächer
Stahlschrank	SG II VS, Größe 1	3 Fachböden, 2 Innenfächer
Stahlschrank	SG I VS, Größe 2	4 Fachböden, 2 Innenfächer
und	SG II VS, Größe 2	
Ausführung E		
Stahlschrank	SG I VS, Größe 1	2 Fachböden, 6 Innenfächer
und	SG II VS, Größe 1	
Stahlschrank	SG I VS, Größe 2	5 Fachböden, 12 Innenfächer
und	SG II VS, Größe 2	

Leitfaden
zur Erstellung einer betriebsinternen
Fotografier- und Filmanweisung

A: Allgemeines

Fotografier- und Filmtechnik war lange Zeit ein „teures Hobby“, solange mit aufwendiger Technik Bildmaterial belichtet und anschließend entwickelt werden musste. Bauweisebedingt waren die eingesetzten Geräte von gewisser Größe und Gewicht.
Nachrichtendienste entwickelten vor langer Zeit technische „Kleinstwunderwerke“, um Spionen beispielsweise das Fotografieren von wichtigen Informationen unbemerkt zu ermöglichen. Das belichtete Bildmaterial wurde dann meistens über „tote Briefkästen“ oder bei konspirativen Treffen weitergegeben.

Die Digitaltechnik hat diesen Bereich revolutioniert. Für wenig Geld kann heute jeder im Computer- oder Fotofachmarkt Fotoapparate oder Filmkameras erwerben, von denen früher Spione nur träumen konnten. Kleinstfotoapparate mit Speicherchips haben eine scheinbar unbegrenzte Aufnahmekapazität und Filmkameras verfügen über eine Zoomtechnik (hundertfache Vergrößerungskapazität), die unbemerkt kleinste Details aus größter Entfernung erkennbar machen. Die Geräte können anschließend an den eigenen oder auch firmeneigenen PC/Notebook angeschlossen, das Bildmaterial aus den Kameras abgerufen und per E-Mail sofort in alle Welt versandt werden. Wem das noch zu aufwendig ist, der nimmt ein Fotohandy, fotografiert und sendet das Bild sofort als MMS an einen Empfänger irgendwo auf dieser Welt.

Diese moderne Technik gefährdet jedoch alle Bereiche und Bemühungen, wo Informationen (Firmen-Know-How oder VS) vor unbefugter Kenntnisnahme geschützt werden müssen.

Schutzmaßnahmen

Spezielle Technik zur Detektierung von Foto- oder Filmkameras (wie z.B. Handyfinder für Mobiltelefone) gibt es nicht. Zur Zeit kann nur durch Leibesvisitation oder Durchleuchtung das Mitführen von Fototechnik in der Kleidung oder in Aktentaschen festgestellt werden. Diese Maßnahmen sind aber aus vielen Gründen nicht praktikabel.

Aus diesem Grund haben bereits viele Unternehmen für ihr gesamtes Firmengelände ein grundsätzliches Verbot erteilt, Fotoapparate oder Filmkameras auf das Firmengelände mitzunehmen.

B: Schutz von VS gegen unbefugtes Fotografieren

1. Für VS gilt:

   - das Einbringen von Fotoapparaten oder Filmkameras (auch Fotohandys) ist grundsätzlich untersagt

     in VS - Registraturen,
     in VS-Sperrzonen,
     in VS-Kontrollzonen und an sonstigen Arbeitsplätzen während der Bearbeitung von VS,
     in Besprechungsräumen, wenn über VS gesprochen wird.

   Diese Regelung gilt für alle Personen (Mitarbeiter, Besucher, Lieferanten, Dienstleistende usw.) und ist in einer innerbetrieblichen Anweisung festzulegen.

   Verdächtige Wahrnehmungen oder Verstöße sind sofort dem/der SiBe zu melden, der/die der Meldung sofort nachgeht, unberechtigt eingebrachtes Gerät sicherstellt und Bildmaterial auswertet sowie die weiteren Maßnahmen (z.B. arbeitsrechtlicher Art, ggf. Meldung an BMWi oder Landesverfassungsschutzbehörde, Mitteilung an SiBe einer entsendenden Firma, Maßnahmen des Hausrechtes, Rückgabe des sichergestellten Gerätes nach dessen Auswertung bzw. dessen weitere Behandlung, wenn VS darauf gespeichert sind) einleitet. Hierbei ist darauf zu achten, dass bei Fotoapparaten mit selbstentwickelndem Bildmaterial nur die belichteten Bilder geprüft werden müssen. Zu belichtendes Filmmaterial ist durch Dauerbelichtung unbrauchbar zu machen.

   Der/die SiBe hat die Einhaltung dieser Regelung in geeigneter Weise zu kontrollieren.

   Sollten deutsche VS, ausländische VS oder VS von zwischenstaatlichen Organisationen unberechtigt abgelichtet worden sein oder der Verdacht nahe liegen, ist das BMWi in jedem Einzelfall sofort zu unterrichten.

2. **Ausnahmen**

   Zur Auftragsabwicklung (z.B. Qualitätssicherung usw.) und Öffentlichkeitsarbeit kann es erforderlich werden, offenes Bildmaterial auch in VS-Bereichen (VS-Sperrzonen usw.) zu erstellen. Hierfür ist innerbetrieblich folgendes anzuordnen:

   Die Erstellung von Bildmaterial in VS-Bereichen ist rechtzeitig bei dem/der SiBe zu beantragen. Der Antrag muss die Begründung der Notwendigkeit für die Aufnahmen, die Anzahl der vorgesehenen Aufnahmen, die hierfür vorgesehene/n Kamera/s, den genauen Zeitraum und die vorgesehene Person (die die Aufnahmen erstellt) enthalten.

   Der/die SiBe genehmigt unter Beteiligung des/der zuständigen Projektleiters/in schriftlich die Erstellung der Aufnahmen, wenn diese notwendig sind und die Person, die die Aufnahmen erstellt, zum Zugang zu den in den aufzunehmenden Lokalitäten vorhandenen VS ermächtigt ist oder die dortigen VS entfernt wurden.
   Weiterhin enthält die Genehmigung eine Regelung, ob die Person, die die Aufnahmen

erstellt, von ihm/ihr oder einem anderen zum Zugang zu VS ermächtigten Firmenangehörigen begleitet werden muss. Ist die Personen, die die Aufnahmen erstellt, nicht Mitarbeiter/in des eigenen Unternehmens, ist grundsätzlich eine Begleitung vorzusehen.

Abschließend ist in der Genehmigung festzulegen, dass vor einer weiteren Verwendung, aber spätestens arbeitstäglich, die erstellten Aufnahmen von dem/der SiBe oder einem ermächtigten fachkundigen Firmenangehörigen (Projektleiter/in) dahingehend ausgewertet werden, ob VS auf den Aufnahmen zu erkennen sind. Ist dies der Fall, ist die Aufnahme, das Speichermedium mit der Aufnahme und bei Kameras ohne Wechselspeichermedien sogar die ganze Kamera als VS zu behandeln.

Auch wenn auf einem Speichermedium irrtümlich VS gespeichert wurden, ist dieses sofort der VS-Registratur zu übergeben. Hier gelten die gleichen Regelungen, die für Speichermedien bei der VS-IT-Bearbeitung gelten. Speichermedien, auf denen VS gespeichert waren, dürfen für die offene Nutzung nur wieder freigegeben werden, wenn sämtliche gespeicherten Daten zuverlässig gemäß den Vorgaben des BSI gelöscht wurden. Informationen hierzu können beim IT-Berater des BMWi angefordert werden. Über die Freigabe für die offene Nutzung entscheidet der SiBe in Abstimmung mit dem IT-Berater des BMWi.

Die schriftliche Genehmigung ist während der Erstellung der Aufnahmen mitzuführen. Die in den vorgesehenen Bereichen tätigen Mitarbeiter sind über die beabsichtigten Aufnahmen zu informieren.

Müssen für den Auftraggeber berechtigterweise Fotos von VS erstellt werden, gelten die allgemeinen Regelungen für die Erstellung einer VS und die vorstehenden Regelungen entsprechend.

Leitfaden
zur Erstellung einer betriebsinternen
Telefonanweisung (Festnetz)

A: Allgemeines

Wer kennt nicht diese Situation, Sie sitzen in der Bahn oder im Bus, beim Arzt im Wartezimmer, im Restaurant; stehen in einem Geschäft oder gehen über die Straße oder anderswo und jemand unterhält sich lautstark mit einem Telefon (Handy) und nimmt nicht mehr wahr, dass alle Umherstehenden mitbekommen, wie schlecht es der Oma geht usw...
„Solche oder noch sensiblere Themen sollte man doch lieber in den eigenen vier Wänden am Festnetztelefon erörtern, das ist doch viel sicherer“, werden viele jetzt sagen. Aber ist das Festnetztelefon wirklich sicher?
Diese Rahmenvorschrift soll ein Leitfaden sein zur Beurteilung ihrer modernen betrieblichen Telekommunikationsanlage (TK-Anlage) im Hinblick auf den Schutz von VS; ihnen und ihren Mitarbeitern/Innen aber auch Anregungen und Denkanstöße vermitteln zum Thema Vertraulichkeit Ihrer Telefongespräche. Die verwandten Themen wie Gebührenbetrug, Konkurrenzausspähung oder Sabotage werden hier nicht speziell behandelt.

1. Digitale Technik

Mit der Ablösung der analogen Technik im Bereich privater TK-Anlagen durch die Digitaltechnik sowie durch die zunehmende Verbreitung intelligenter Endgeräte ist weitgehend unbemerkt eine veränderte Gefährdungslage entstanden.
Während bei der Analogtechnik in erster Linie die Hardware des Systems (z.B. Leitungsnetz und Endgeräte) als Angriffspunkte für illegales Abhören gesehen werden mussten, steht bei digitalen Systemen die missbräuchliche Verwendung vorhandener Funktionalitäten im Vordergrund.
Ihr modernes Telefon auf ihrem Schreibtisch ist auch die ideale „Wanze“ zum Mithören aller Ihrer Gespräche – es ist unauffällig, es besitzt ein Mikrofon, es besitzt Energie (Strom) und es ist über die Telefonleitung mit der ganzen Welt verbunden.
Damit dieses Telefon nicht als „Wanze“ missbraucht werden kann, müssen entsprechende Vorkehrungen geschaffen werden.

2. Schutzmaßnahme Konfiguration

Moderne digitale TK-Anlagen enthalten optional mehrere hundert Leistungsmerkmale. Viele von Ihnen kennen und nutzen die geläufigsten Merkmale wie z.B. Freisprechen (Führen eines Telefonates ohne Abheben des Hörers), Konferenz (Führen eines Telefonates zwischen drei Personen gleichzeitig) oder Makeln (Führen von zwei gleichzeitigen Telefonaten im Wechsel).
Ein Missbrauch dieser Merkmale kann eine ungewünschte Raumüberwachung ermöglichen.
Daher ist die ordnungsgemäßen Konfiguration der TK-Anlage und ihrer umfangreichen Sicherheitsmechanismen von größter Bedeutung.
Die meisten Unternehmen lassen die Installation und Konfiguration ihrer TK-Anlage von ei-

ner Fremdfirma durchführen. Dabei ist die Auswahl einer Firma Ihres Vertrauens besonders wichtig, da Sie die Einstellungen Ihrer TK-Anlage aus der Hand geben. Sie sollten sich zumindest von dieser Fremdfirma genau erklären und demonstrieren lassen, wie die Leistungsmerkmale und Sicherheitsmechanismen geschaltet sind. Dies sollte auch in einer Beschreibung der Anlage (nicht nur Bedienungsanleitung) festgehalten werden und ihre Mitarbeiter/Innen sollten über die Nutzung der TK-Anlage geschult sein, hier sollte insbesondere auch auf mögliche Warnanzeigen, -symbole und -töne eingegangen werden. Im Alltagsbetrieb nicht benötigte Leistungsmerkmale werden deaktiviert.
In vielen Fällen kann sogar die Geheimschutzbetreuung dieser Fremdfirma erforderlich sein.

3. Schutzmaßnahme Zugriff

Der Zugriff auf TK-Anlagen kann über die Administrationsschnittstelle des zu Ihrer TK-Anlage gehörenden Rechners (Wartungs-, Diagnose- und Steuereinheit) oder über die Fernwartung (siehe Nr. 5) erfolgen. In diesem Rechner werden die Leistungsmerkmale und die Sicherheitsmechanismen für Ihre TK-Anlage ein- oder ausgeschaltet. Manipulationen an den TK-Anlagen selbst und ihren Komponenten sollen verhindert werden.
Der Raum, in denen dieser Rechner steht, aber auch alle Haupt- und Zwischenverteilerkästen sind gegen unbefugtes Öffnen zu schützen.
Sämtliche zur TK-Anlage gehörenden Kabel und Leitungen sind möglichst zugriffssicher zu verlegen.
Lagehinweise auf schützenswerte Gebäudeteile sind zu vermeiden.
Haben Fremdpersonen Zugriff auf Rechner, Verteilerkästen und Leitungen, sollten sie begleitet werden.
Der Zutritt zum Raum des Rechners der TK-Anlage sowie der Zugriff auf Verteilerkästen sind zu regeln und zu kontrollieren.
Bedienplätze größerer TK-Anlagen sind zugriffssicher unterzubringen und der Zugang ebenfalls entsprechend zu regeln.
Die Abläufe von Wartungs- und Reparaturarbeiten sind genau zu regeln.
Alle Administrationsarbeiten an der TK-Anlage sind genauestens zu protokollieren.
Zusätzlich sind die Regeln des Passwortschutzes einzuhalten.

4. Fernwartung

Aus Gründen der Wirtschaftlichkeit und der Verfügbarkeit der Anlage wird gern auf den Fernwartungsservice der Hersteller zurückgegriffen. Da der Wartungsport Ihrer TK-Anlage dafür amtsberechtigt sein muss, kann er ohne zusätzliche Maßnahmen weltweit angewählt werden. Die möglichen Schutzmaßnahmen um nachzuvollziehen, wer wann welche Änderungen vorgenommen hat (z.B. automatischer Rückruf, Auswertung der im ISDN übermittelten Rufnummern, Sperrung des Fernwartungszuganges im Normalfall und Aktivierung nur auf spezielle Nachfrage, lückenlose Protokollierung aller Administrationstätigkeiten), können jedoch nicht gegenüber den unter Nummer 3. genannten Schutzmaßnahmen als gleichwertig angesehen werden.

5. Schutzmaßnahme Vertraulichkeit

Die Kommunikation über elektronische Medien ist für unsere Gesellschaft unverzichtbar geworden. Einrichtungen wie Telefon, Telefax, lokale Netze, Datenfernübertragung, E-Mail sind für ein effizientes Arbeiten nicht mehr wegzudenken; die Zeit der "reitenden Boten" ist längst vorbei.
Fast allen elektronischen Informations-Übertragungsverfahren ist gemeinsam, dass der In-

formationsfluss über Leitungen erfolgt. Ob es sich hierbei um Koaxial-, Zweidraht-, Twisted-Pair- oder Glasfaser-Leitungen handelt, bleibt dem Anwender meistens verborgen, sofern nur die Übertragung einwandfrei funktioniert. Dazu gehört auch, dass ca. 50 % aller Telefonverbindungen im Laufe ihrer Strecke teilweise über eine Richtfunkstrecke geführt werden und somit von entsprechenden Empfangseinrichtungen mitgehört werden.
Ebenso verborgen bleibt dem Anwender vielfach die Tatsache, dass auf Leitungen übertragene elektrische Signale auf andere Leitungen überkoppeln (Frequenzen auf der einen Leitung werden auf andere Leitungen übertragen bei schlechter Isolierung der Leitungen) können und damit ein Verlust der Vertraulichkeit droht.
Dabei ist der physikalische Effekt, dass elektrische Signale auf benachbart verlegte Leitungen überkoppeln, vielen aus eigener Erfahrung unbewusst bekannt. Beim Telefonieren mit herkömmlichen, analog arbeitenden Telefonapparaten hört man mitunter leise Stimmen im Hintergrund, die nicht dem angewählten Gesprächspartner zuzuordnen sind. Wer hier eine Fehlschaltung irgendwo auf dem langen Übertragungsweg vermutet, denkt nicht an das Nächstliegende, dass nämlich beispielsweise ein Nachbar, dessen Telefonleitung im selben Kabelbündel wie das eigene geführt ist, ebenfalls telefoniert. Dass ein einigermaßen versierter Elektronikbastler in der Lage ist, das "übergekoppelte" Gespräch mit geringem Aufwand aufzubereiten und so einwandfrei mithörbar zu machen, ist fast selbstverständlich.

Schutzmaßnahmen gegen Verlust der Vertraulichkeit lassen sich aus den physikalischen Effekten folgern, die zum Überkoppeln auf Leitungen führen.

Geeignete Schutzmaßnahmen sind:

- Verwendung von Kabeltypen, deren Aufbau so gestaltet ist, dass nur ein geringes elektromagnetisches Feld freigesetzt wird, z.B. Koaxial- oder Twisted-Pair-Kabel.

- Verwendung von Kabeltypen mit hochwertiger, vorzugsweise doppelter Schirmung. Als sehr wirksam und kostengünstig hat sich eine Kombination aus Folien- und Geflechtschirm erwiesen.

- Verlegung der bedrohten Leitungen mit ausreichendem Abstand zu anderen, parallel geführten Leitungen (Von einem Arbeitsplatzcomputer werden Informationen beispielsweise zu einem Hostrechner oder Netzserver übertragen. Die Übertragungsleitung befindet sich in einem vor Zugriff durch Unbefugte gesicherten Bereich, ist jedoch zusammen mit anderen Leitungen im selben Kabelkanal verlegt. Eine der anderen Leitungen, beispielsweise eine Telefonleitung, verlässt den gesicherten Bereich. Dort ist es mit verhältnismäßig geringem Aufwand möglich, das übergekoppelte Informationssignal von der Leitung abzugreifen, aufzubereiten und darzustellen bzw. für eine spätere Auswertung zu speichern. Bezüglich digitaler, auf Leitungen übertragener Signale (z.B. ISDN) ist anzumerken, dass die von einer parallel verlegten Leitung übergekoppelte Signalamplitude meist so gering ist, dass die eigentliche Funktion der Leitungen nicht beeinträchtigt wird und so das Überkoppeln von den Nutzern dieser Leitungen nicht bemerkt wird. Erst eine geeignete Aufbereitung des übergekoppelten Signals erlaubt eine Rekonstruktion der Information).

- Verringerung des Signal-Oberwellengehalts durch elektrische Filterung bei digitaler Übertragung von Informationen.
  Die Oberwellen, für deren Intensität die Flankensteilheit des digitalen Signals ein Maß ist, sind für die eigentliche Informationsübertragung nicht notwendig, koppeln aber

besonders stark auf parallel geführte Leitungen über.

- Verwendung von Lichtwellenleiterkabeln (Glas- oder Kunststofffasern). Lichtwellenleiter erzeugen kein elektromagnetisches Feld, können jedoch unter Umständen optisch überkoppeln, wenn sich zwischen den einzelnen Fasern keine optisch undurchlässige Ummantelung befindet.

B: Verbindliche Regelungen zum Schutz von VS-Gesprächen

Bedingt durch die Möglichkeit der Manipulation von TK-Anlagen und der Gefährdungen durch die Übertragung auf Telekommunikationswegen einschließlich Überkoppeln gilt für die Übermittlung von staatlichen Verschlusssachen:

- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Telefongespräche
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Faxe
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Emails
- keine nicht den Vorgaben des BMWi entsprechend verschlüsselte Datenübertragungen.

Ist in Ihrem Unternehmen eine Besprechung (auch unter Mitarbeitern im kleinen Kreise) über VS-eingestufte Inhalte geplant, so sind vorhandene Telefonapparate durch Entfernung des Leitungssteckers vom Netz zu trennen. Sollte dies aus technischen Gründen nicht möglich sein, sind vorhandene Telefonapparate von der Zentrale aus zu deaktivieren oder andere gleichwertige Maßnahmen vorzusehen.

Bei Unternehmen mit größerem VS-Bestand, Sperr- und Kontrollzonen oder häufig stattfindenden Besprechungen mit VS-Inhalten ist eine Fernwartung nicht zulässig.
Hier ist mit Einwilligung des BMWi das Personal, dass die Installation, Instandsetzung, Wartung und Betrieb der TK-Anlage und aller ihrer Komponenten durchführt, entsprechend der vorhandenen VS sicherheitsmäßig zu überprüfen und zum Zugang zu VS zu ermächtigen. Werden diese Aufgaben nicht von eigenem Personal durchgeführt, können andere Firmen hierzu auch in die Geheimschutzbetreuung des BMWi aufgenommen werden.

Die weiteren unter Abschnitt A Nr. 3 „Schutzmaßnahmen Zugriff“ enthaltenen allgemeinen Empfehlungen sind für den Schutz von staatlichen VS zu beachten und hier verbindlich. Sollte eine dieser Forderungen nicht erfüllt werden können, ist in Abstimmung mit dem BMWi ein gleichwertiger Schutz sicherzustellen (z.B. sind vorhandene bauliche Kabelführungen nicht zugriffssicher verlegt, so müssen sie in offen zugänglichen Bereichen auf Unversehrtheit in regelmäßigen Abständen geprüft werden. Nicht offen zugängliche Bereiche sind dabei unter Verschluss des SiBe oder einer von ihm beauftragten Person zu halten).

Leitfaden
zur Erstellung einer betriebsinternen
Telefonanweisung (Mobilfunk)

Die moderne Mobilfunktechnik beinhaltet auch ein immenses Gefährdungspotential im Bereich der illegalen Ausspähung von Unternehmen und Behörden. In diesem Zusammenhang wird auf die umfassenderen Hintergrundinformationen für die Erstellung einer betriebsinternen Telefonanweisung (Moblifunk) auf dem Geheimschutzserver (www.bmwi-sicherheitsforum.de - Bibliothek) verwiesen.

Nachfolgend soll nur auf die Schutzmaßnahmen gegen die bekannten Gefährdungen eingegangen werden, die in zwei Bereiche aufgeteilt wurden. Die allgemeinen Schutzmaßnahmen, die jeder Mobilfunkteilnehmer zum Schutz seiner Privatsphäre oder auch von firmenvertraulichen Angelegenheiten beachten sollte und die verbindlichen Regelungen für den Schutz von Verschlusssachen.

A: Allgemeine Schutzmaßnahmen

1. Allgemeines

Grundsätzlich gilt, dass Art und Umfang der Schutzmaßnahmen abhängig sind von der Gefährdungslage. Welche Maßnahmen im Einzelfall umgesetzt werden, liegt in der Verantwortung des Einzelnen.
Da aber oft auch leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Sicherheitsverantwortliche prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen.
Für den VS-Bereich müssen jedoch höhere Schutzmaßnahmen ergriffen werden.

2. Schutz vor Abhören von Telefonaten

Ein wirksamer Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Solange eine solche Verschlüsselung nicht realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden.
Folgende Maßnahmen werden zur Verringerung der Gefährdung empfohlen:

- Grundsätzlich sollten ohne besondere Schutzmaßnahmen keine Telefongespräche mit sensiblem Inhalt geführt werden.
- Es sollten Geräte verwendet werden, die eine fehlende Verschlüsselung auf dem Display anzeigen.
- Im Bedarfsfall ist geschlossenen Benutzergruppen die Verwendung von speziellen kryptierenden Mobiltelefonen anzuraten. Für behördliche Benutzerkreise sei an dieser Stelle auf Kryptomobiltelefone mit VS-Zulassung hingewiesen.
- Einzelverbindungsnachweise sollten auf unbekannte Rufnummern hin überprüft werden.
- Ferner sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden; fehlende Gebühren für bestimmte Verbindungen können auf Abhören hindeuten.

3. Schutz vor Abhören von Raumgesprächen

Schutz vor Abhören von Raumgesprächen mittels handelsüblicher Mobiltelefone

Das Abhören von Raumgesprächen mittels Mobiltelefonen kann nur dann sicher ausgeschlossen werden, wenn das Einbringen von Mobiltelefonen in den zu schützenden Raum verhindert wird.

Auf dem Markt sind passive Warngeräte (GSM-Mobiltelefon-Detektoren) verfügbar, die Mobiltelefone, die sich im Sendebetrieb befinden oder neu in Sendebetrieb gehen, melden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, solche Warngeräte zu installieren und diese bei Gesprächen mit sensitivem oder vertraulichem Inhalt zu aktivieren.

Es gibt aktive Mobiltelefon-Detektoren, die alle in Reichweite befindlichen Mobiltelefone auffordern, in den Sendebetrieb zu gehen. Diese können wegen der fehlenden Betriebserlaubnis für Deutschland nicht empfohlen werden. Auch für Störsender, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist, gibt es in Deutschland keine Betriebsgenehmigung.

Schutz vor Abhören von Raumgesprächen mittels manipulierter Mobiltelefone

Zusätzlich ist zu beachten, dass das Ausschalten des Mobiltelefons als Schutz nicht ausreicht, da bei manipulierten Mobiltelefonen ein unbemerkter Übergang in den Sendebetrieb nicht mit hinreichender Sicherheit ausgeschlossen werden kann.

Das Risiko einer Manipulation kann vermindert werden, wenn der Kauf von Mobiltelefonen bei vertrauenswürdigen Stellen erfolgt, damit nicht schon beim Erwerb mit einer Manipulation gerechnet werden muss. Bei der Beschaffung größerer Stückzahlen sollte der Auftrag auf mehrere Anbieter aufgeteilt werden. Bei Manipulationsverdacht sollte das betroffene Mobiltelefon aus dem Verkehr gezogen werden.
Hardware-Manipulationen können sicher mit Röntgenprüfverfahren oder auch per Sichtprüfung nach Zerlegen des Gerätes erkannt werden. Derzeit existiert kein Prüfwerkzeug, mit dem die Software von Mobiltelefonen auf Manipulationen hin überprüft werden kann.

4. Schutz vor missbräuchlicher Datenweitergabe über GSM-Endgeräte

Schutz vor unberechtigter Datenweitergabe

Einen absoluten Schutz gegen Innentäter gibt es nicht. Daher ist es ratsam, die Mitnahme von Mobiltelefonen in sensitive Bereiche zu untersagen; die Umsetzung dieses Verbotes sollte überprüft werden.

Schutz vor ungewollter Datenweitergabe

Da Fälle von manipulierten Card-Phones nicht auszuschließen sind, sollten in PCs, auf denen sensitive Daten verarbeitet werden beziehungsweise die mit einem Rechner-Netzwerk verbunden sind**,** keine Mobilfunkkarten zugelassen werden.

Schutz vor SIM-Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte sollten stets sicher aufbewahrt werden. Die persönliche Geheimzahl PIN sollte aktiviert bleiben und darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden.
Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch - und damit auch einen persönlichen Schaden - abzuwehren.
Es ist empfehlenswert, Einzelverbindungsnachweise regelmäßig auf unerklärliche Gebühren und Zielrufnummern zu prüfen.

Schutz vor Erstellen von Bewegungsprofilen

Wird die Erstellung von Bewegungsprofilen als Gefährdung angesehen, dann sollten - falls umsetzbar - die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert. Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte auch der Akku entfernt werden.

Schutz vor Rufnummernermittlung

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer beziehungsweise Gerät und Nutzer möglich. Die Zuordnung zum Beispiel zu einer Firma bleibt aber bestehen. Weitere Möglichkeiten sind die Nichtveröffentlichung der Rufnummern im öffentlichen Telefonbuch und die Nichtveröffentlichung der Rufnummern im internen Telefonbuch.

5. Schutzmaßnahmen für die Nutzung zusätzlicher Dienste

Kurznachrichten-Dienste

Da es keine Möglichkeit gibt, den Empfang von SMS zu unterbinden, kann an dieser Stelle nur die Empfehlung ausgesprochen werden, die eigene Rufnummer nur vertrauenswürdigen Personen mitzuteilen.

M-Commerce und M-Payment sowie Virenproblematik

Hier gelten die allgemeinen Schutzmaßnahmen bei Nutzung des Internets und des Homebankings.

B: Regelungen für den Schutz von Verschlusssachen

Folgende Regelungen sind in einer betriebsinternen VS-Anweisung zu regeln

1. Die Nutzung von Phone-Cards für VS-zugelassene Notebooks bedarf der Genehmigung des BMWi. Voraussetzung der Genehmigung wäre in jedem Fall eine Verschlüsselung der Informationen nach vom BMWi zugelassenen Verfahren zwischen Sender und Empfänger.

2. Das Führen von Telefongesprächen, übermitteln von SMS, MMS oder anderer Daten mit VS-eingestuften Inhalten bedarf der Genehmigung des BMWi. Voraussetzung der Genehmigung wäre in jedem Fall eine Verschlüsselung der Informationen nach vom BMWi zugelassenen Verfahren zwischen Sender und Empfänger.

3. Das Einbringen von Handys in VS-Sperrzonen oder VS-Registraturen ist grundsätzlich untersagt. Ausnahmen sind in der jeweiligen Sperrzonenanweisung festzulegen, die der Einwilligung des BMWi bedarf. Die Einhaltung der Maßnahme ist vom SiBe durch Verwendung eines passiven Warngerätes (GSM-Mobiltelefon-Detektoren) regelmäßig zu überwachen. Zuwiderhandlungen stellen die Ermächtigung zum Zugang zu VS in Frage und sollten auch arbeitsrechtlich geahndet werden.

4. Zu Besprechungen von Mitarbeitern in Kontrollzonen oder Arbeitsräumen mit VS-eingestuften Inhalten dürfen keine Handys mitgenommen werden. Das Personal ist entsprechend zu belehren und zu verpflichten. Die Einhaltung ist ebenfalls zu kontrollieren (siehe vorstehende Nummer 3).

5. Zu Besprechungen mit größerem Personenkreis und externen Teilnehmern über VS-eingestufte Inhalte gilt ebenfalls das Verbot zur Einbringung von Handys in den Besprechungsraum. In der Besprechungseinladung und bei Empfang der Teilnehmer muss hierauf hingewiesen werden.

   Es empfiehlt sich eine Belehrungsanweisung für die Teilnehmer an der Besprechung zu erstellen.

   Es muss eine Aufbewahrungsmöglichkeit für mitgeführte Handys außerhalb des Besprechungsraumes vorgesehen (Sekretariat, Schließfächer usw.) und die Einhaltung der Maßnahme durch Verwendung eines passiven Warngerätes (GSM-Mobiltelefon-Detektoren) überwacht werden. Bei festgestellten Verstößen ist sofort der SiBe einzuschalten.
   Sind vorgesehene Teilnehmer nicht bereit, auf die Mitnahme ihres Handys zu verzichten, sind sie von der Besprechung auszuschließen. Der SiBe und das BMWi sind hierüber zu unterrichten.

6. Die vorstehend zu 2. bis 5. genannten Regelungen gelten insbesondere für Fotohandys, die u.U. auch bereits von der VS-Fotografieranweisung oder des betrieblichen Fotografierverbotes erfasst werden. Im Jahr 2003 wurden weltweit 55 Millionen Fotohandys verkauft. Diese Zahl ist gleich groß wie die der weltweit verkauften analogen oder digitalen Fotoapparate. Wegen der Möglichkeiten, die diese Technik mit sich bringt, verbieten viele Unternehmen weltweit aus Angst vor Industriespionage das Einbringen solcher Handys auf das Unternehmensgelände.
   Wegen der zusätzlichen besonderen Gefährdung durch solche Fotohandys ist deren Einbringung zu allen VS-Arbeitsplätzen grundsätzlich untersagt.

Leitfaden zur Verpackung von VS-Schriftgut

1. Briefsendungen

1.1 Äußere Briefhüllen

Standardbriefhüllen in handelsüblicher Papierqualität nach Bedarf.

1.2 Innere Briefhüllen

Briefhüllen in handelsüblicher Papierqualität.

Die Briefhüllen sind mit Scotch-Siegelband 820 und dem Scotch-Schnellsiegler TSZ 2240 mit Anwenderlogo zu versiegeln. Die dafür erforderliche Ausstattung kann im Bürofachhandel bezogen werden:

- Scotch-Siegelband 820 von 3M
- Scotch-Handabroller H 315 von 3M
- Scotch-Schnellsiegler TSZ 2240 von 3M

Der spezielle Siegelaufsatz, der das Anwenderlogo trägt, gehört nicht zum Lieferumfang des Schnellsieglers und kann durch örtliche Klischeehersteller hergestellt werden.

Alternativ können die Briefhüllen mit Sicherheitsetiketten versiegelt werden. Vom BSI sind folgende Etiketten zugelassen:

- Advantage Transfer der Firma Schreiner
- Sico Tra-Klebesiegel der Firma Trautwein Security

Als innere Briefhülle können auch DEBASAFE-Taschen aus PE-Folie der Firma Anton Debatin verwendet werden. Für den Versand von GEHEIM eingestuften VS werden die DEBASAFE-Taschen wegen ihrer höheren Sicherheit empfohlen.

DEBASAFE-Taschen des Formats 195 x 265 mm können bei der Firma Debatin ab Lager beschafft werden.

Die DEBASAFE-Taschen haben als Verschlusselement das Scotch-Siegelband 820, das ebenfalls mit dem Schnellsiegler TSZ 2240 zu versiegeln ist.

Die DEBASAFE-Taschen sind mit einer fortlaufenden Nummerierung versehen. Die jeweilige Nummer ist auf dem VS-Empfangsschein aufzuführen.

2. Paketsendungen

2.1 Äußere Verpackung

Versandkartons in handelsüblicher Qualität, Format je nach Bedarf.

2.2 Innere Verpackung

Vorzugsweise Versandkartons in handelsüblicher Qualität. Eine Verpackung mit Packpapier (Natronkraftpapier) sollte nur ausnahmsweise erfolgen.

Die innere Verpackung ist mit dem Scotch-Siegelband 820 oder mit Sicherheitsetiketten (siehe Abschnitt 1.2) zu versiegeln. Das Siegelband oder die Etiketten sind auf der inneren Verpackung so aufzukleben, dass ein Öffnen nur möglich ist, wenn die Verpackung selbst oder die Siegel zerstört werden. Die einzelnen Siegelbänder oder Etiketten dürfen sich dabei nicht überlappen.

Alternativ kann eine Sicherung der inneren Verpackung durch Verschnüren erfolgen. Die Verschnürung muss aus einem Stück bestehen und so um die Sendung gelegt werden, dass sie nicht abgestreift werden kann. Als Schnur wird Polyamidschnur (dreischäftig gedreht aus Endlosfaser, Durchmesser 1,5 mm) empfohlen. Die Verschnürung darf nur an einer Stelle verknotet werden. Der Knoten ist mit einer SNAPLOCK-Plombe der Firma UNISTO zu sichern.

Die SNAPLOCK-Plomben sind innen mit einer fortlaufenden Nummerierung versehen, die im VS-Empfangsschein anzugeben ist.

Anstelle der SNAPLOCK-Plomben kann auch mit Siegellack und Petschaft versiegelt werden.

3. Anschriften

- Anton Debatin GmbH
  Postfach 1420
  76604 Bruchsal
  Tel.: 07251/80090
  Fax: 07251/8009 199

- Schreiner GmbH & Co. KG
  Bruckmann Ring 22
  85764 Oberschleißheim
  Tel.: 089/31 584—135
  Fax: 089/31 584-317

- Trautwein Security GmbH & Co.
  Am Trimbuschhof 8
  44628 Herne
  Tel.: 02323/95 39—0
  Fax: 02323/95 39—20

- Unisto GmbH
  Max-Stromeyer-Str. 35
  78467 Konstanz
  Tel.: 07531/8107—0
  Fax: 07531/50 474

Versendung durch private Zustelldienste

Das Bundesministerium für Wirtschaft und Energie (BMWi) lässt die Versendung GEHEIM oder VS-VERTRAULICH eingestufter VS durch private, auch nicht geheimschutzbetreute Zustelldienste unter den nachfolgenden Voraussetzungen zu.

1. Privater Zustelldienst

Der private Zustelldienst und dessen Versandangebot müssen folgenden Anforderungen genügen:

a) Sitz in Deutschland;

b) lückenlose DV-gestützte Verfolgung der Sendung von der Annahme bis zur Auslieferung („Track and Trace“);

c) Nachweis der Annahme der Sendung durch den privaten Zustelldienst und der Auslieferung der Sendung an den Empfänger und

d) Auslieferung der Sendung binnen 24 Stunden.

2. Absender und Empfänger

Absender und Empfänger haben den VS-Versand unter Achtung der allgemeinen Vorgaben des Geheimschutzhandbuchs für die Wirtschaft (GHB) sorgfältig vorzubereiten, zu beobachten und zu dokumentieren. Folgende spezifische Anforderungen sind zu beachten:

a) Vorbereitung des Versands

(1) Der Absender hat sich zu vergewissern, dass der private Zustelldienst und dessen Versandangebot den Anforderungen gemäß Ziff. 1. genügen.

(2) Eine Absendung ist nur am Tage vor Werktagen, nicht jedoch vor Wochenenden und Feiertagen zulässig. Maßgeblich sind die Feiertagsregelungen im jeweiligen Bundesland des Empfängers.

Vor Absendung hat der Absender den Empfänger über die Versendung in Kenntnis zu setzen und sich zu vergewissern, dass die Sendung am Empfangstage beim Empfänger eingehen kann. Regelmäßig sind für diese Abstimmung die VS-Verwalter/innen von Absender und Empfänger oder deren Vertreter/innen zuständig.

(3) Der Absender hat die VS gemäß dem GHB für den Versand ordnungsgemäß zu verpacken.

Auf dem im inneren Umschlag beizufügenden VS-Empfangsschein hat der Absender neben dem Datum der Absendung zusätzlich die geplante Übergabezeit an den privaten Zustelldienst zu vermerken.

Der innere Umschlag, auf dem der Geheimhaltungsgrad anzubringen ist, ist mit den Firmenanschriften des Empfängers aus dem Sicherheitsbescheid des BMWi zu adressieren an

- den/die Sicherheitsbevollmächtigte(n) oder dessen/deren Stellvertreter/in vor Ort und/oder
- an den/die VS-Verwalter/in oder dessen/deren Vertreter/in.

Der äußere Umschlag, der den VS-Inhalt nicht erkennen lassen darf, ist neutral an die Poststelle des Empfängers zu adressieren.

Sofern der genutzte Zustelldienst Versandtaschen zur Verfügung stellt, wird zusätzlich deren Verwendung empfohlen. Die Versandtasche ist in diesem Fall als dritter Umschlag zu verwenden und wie der vorstehend genannte äußere Umschlag neutral zu adressieren.

(4) Der Absender darf die Sendung nur gegen Nachweis der Annahme an den privaten Zustelldienst übergeben. Erfolgt die Übergabe nicht bei dem Absender, sind bis zur Übergabe zusätzlich die Regelungen über die Beförderung durch Kuriere (Ziff. 6.10.3.2 GHB) zu berücksichtigen.

b) Beobachtung des Versands

(1) Unverzüglich nach Annahme der Sendung durch den privaten Zustelldienst hat der Absender den Empfänger über die tatsächliche Übergabezeit zu unterrichten. Ziff. 2 a) (2) Satz 4 gilt entsprechend.

(2) Der/die VS-Verwalter/in des Empfängers oder dessen/deren Vertreter/in hat den Zeitpunkt des Eingangs der Sendung in der Poststelle bei Quittierung des VS-Empfangsscheins auf diesem zu vermerken.

(3) Der/die VS-Verwalter/in des Empfängers oder dessen/deren Vertreter/in und der/die Sicherheitsbevollmächtigte(r) des Empfängers oder dessen/deren Stellvertreter/in vor Ort haben sich unverzüglich wechselseitig zu unterrichten, wenn die Sendung nicht am angekündigten Empfangstage beim Empfänger eingeht. Der Absender ist zeitnah hierüber zu informieren. Der Absender hat den Sachverhalt unter Einbindung des privaten Zustelldienstes unverzüglich aufzuklären.

(4) Bei Ungewissheit über den Verbleib der Sendung oder bei Verdacht des Verlustes oder einer Kompromittierung der VS hat der Absender sofort das BMWi zu unterrichten.

c) Dokumentation

Der Absender hat die unter Ziff. 1. c) genannten Nachweise entsprechend Ziff. 6.6.2. GHB zu behandeln.

Leitfaden für die Beförderung bzw. Mitnahme von geheimhaltungsbedürftigen Dokumenten der Einstufung VS-Vertraulich oder höher innerhalb Deutschlands

1. Der Kurier, der geheimhaltungsbedürftige Dokumente befördert oder befördern soll, muss

   - zum Zugang zu Verschlusssachen (VS) des entsprechenden Geheimhaltungsgrades ermächtigt sein,
   - sich verpflichten, die VS in ständigem persönlichen Gewahrsam zu halten, insbesondere sie nicht in Verkehrsmitteln, Hotelzimmern, Garderoben usw. unbeaufsichtigt zu lassen bzw. sie nicht in Hotelsafes, Gepäckschließfächern oder sonstigen Gepäckaufbewahrungen abzugeben und die Verpackung der geheimhaltungsbedürftigen Dokumente unterwegs nicht zu öffnen,
   - über seine Pflichten von dem/der SiBe vor der Abreise nachweisbar belehrt werden. Die Belehrungsnachweise sind zwei Jahre aufzubewahren.

   Dem Kurier ist eine Bescheinigung entsprechend dem nachstehenden Muster mitzugeben.
   Ist der persönliche Gewahrsam während der Reise nicht zu gewährleisten, so muss der Kurier durch einen weiteren entsprechend VS-Ermächtigten begleitet werden.

2. Kuriere, die geheimhaltungsbedürftige Dokumente der Einstufung STRENG GEHEIM befördern, haben einen Firmenwagen mit entsprechend VS-ermächtigtem Fahrer zu benutzen. Ist dies nicht möglich, ist ein zweiter Kurier zur Begleitung einzusetzen.

3. VS können von Unternehmensangehörigen zu Verhandlungen und Besprechungen bei anderen Unternehmen bzw. Dienststellen mitgenommen und anschließend zurückgebracht werden, die auf der Reise die Aufgaben des Kuriers mit anderen Aufgaben vereinen, wenn die Mitnahme der VS zur Erledigung des mit der Reise bezweckten Geschäfts notwendig ist.

   Über die Notwendigkeit der Mitnahme von VS auf Geschäftsreisen entscheidet in jedem Einzelfall der/die SiBe nach Abstimmung mit dem/der Arbeitsvorgesetzten.
   Bei der Mitnahme ist folgendes zu beachten:

   - Die geheimhaltungsbedürftigen Dokumente sind in doppeltem Umschlag (oder entsprechendem Material) zu verpacken. Die Umschläge müssen aus festem undurchsichtigem Papier bestehen.
   - Auf dem Außenumschlag oder der äußeren Verpackung muss die Anschrift des/der SiBe des absendenden Unternehmens stehen.
   - Ein Kurierausweis ist erforderlich.

4. Dem Kurier ist in jedem Fall eine vorbereitete Empfangsquittung auszuhändigen, in denen die mitgeführten Briefe/Päckchen/Pakete aufgeführt sind.

   Werden die geheimhaltungsbedürftigen Dokumente dem besuchten Unternehmen oder der besuchten Dienststelle übergeben (z.B. im Anschluss an einer dort stattgefundenen Erörterung), hat sich der Kurier die Übergabe der Sendung auf dem VS-Empfangsschein quittieren zu lassen und den VS-Empfangsschein nach seiner Rückkehr unverzüglich der VS-Registratur des absendenden Unternehmens zu seiner Entlastung zuzuleiten. Eine Durchschrift dieser VS-Empfangsscheine verbleibt in der VS-Registratur des absendenden Unternehmens.

Wird die Sendung vom Kurier zum absendenden Unternehmen wieder zurückgebracht, erfolgt seine Entlastung dadurch, dass er sich anhand der VS-Empfangsscheine die Rückgabe durch die VS-Registratur des absendenden Unternehmens bestätigen lässt. Der Kurier bleibt bis zu dieser Entlastung für die ordnungsgemäße Behandlung der geheimhaltungsbedürftigen Sendung verantwortlich.

5. Der/die SiBe des absendenden Unternehmens unterrichtet den/die SiBe des zu besuchenden Unternehmens oder den/die Geheimschutzbeauftragte/n der zu besuchenden Dienststelle über den vorgesehenen Zeitpunkt der Ankunft des Kuriers und bittet um sofortige Benachrichtigung für den Fall, dass dieser nicht zeitgerecht eintrifft. Erforderlichenfalls vereinbart er/sie mit dieser Stelle die ordnungsgemäße Unterbringung der VS nach der Ankunft und während einer etwaigen Besuchszeit.

6. Kurierfahrten sind auf dem kürzesten Weg auszuführen.

7. Die Benutzung öffentlicher Nahverkehrsmittel (außer Taxi) ist möglichst zu vermeiden, bei STRENG GEHEIM verboten.

8. Gehen VS bei der Beförderung oder Mitnahme - auch nur zeitweise - verloren, ist unverzüglich BMWi und das zuständige Landesamt für Verfassungsschutz zu unterrichten. Falls es sich um NATO-Dokumente oder Dokumente ausländischen Ursprungs handelt, ist dies unter genauer Bezeichnung des betreffenden Programms anzugeben.

Für VS-Material ist diese Richtlinie sinngemäß anzuwenden.

GHB - Anlage 63b

KURIERAUSWEIS NR: ..... gültig bis: .....
(Für Kurierlieferung von Verschlusssachen - Dokumente, Material -)

Hiermit wird bestätigt, dass der/die Ausweisinhaber/in:

Herr/Frau (Name/Vorname):.....

geboren am : ..... in.....

Staatsangehörigkeit: .....

Inhaber/in des Passes/Personalausweises Nr. .....

ausgestellt in ..... am .....

dazu ermächtigt ist, die folgende Sendung auf der nachstehend beschriebenen Reise mit sich zu führen:

REISEROUTE/-N

Von: .....

Nach: .....

Durch (Länder): .....

Genehmigte Zwischenstationen: .....

Reisebeginn (Datum): .....

(Unterschrift des/der Sicherheitsbevollmächtigten, Unternehmensstempel)

Polizeibeamte werden auf folgendes hingewiesen:

(1) Diese Sendung ist im Interesse der nationalen Sicherheit eingestuft.
(2) Es wird darum gebeten, dass die Sendung nur von ordnungsgemäß VS-Ermächtigten oder von Personen mit einer Sondererlaubnis inspiziert wird.
(3) Falls eine Inspektion für notwendig erachtet wird, so wird darum gebeten, dass diese in Anwesenheit des Kuriers durchgeführt wird. Darüber hinaus sollten nur die unter (2) bezeichneten Personen Kenntnis von der Sendung erhalten.
(4) Es wird darum gebeten, dass die Sendung, wenn sie für eine Inspektion geöffnet wird, nach Verschluss gekennzeichnet wird, so dass das Öffnen durch Siegel und Unterschrift und durch Vermerk über das Öffnen der Sendung in den Frachtpapieren (falls solche vorliegen) belegt wird.
(5) Die Polizeibeamten der Länder, durch die die Sendung geführt wird oder die betreten oder verlassen werden, werden gebeten, gegebenenfalls bei der erfolgreichen und sicheren Zustellung der Sendung behilflich zu sein.

ERKLÄRUNG (Nach Abschluss der Reise zu unterschreiben):

Ich erkläre hiermit, dass ich während der von diesem Kurierausweis abgedeckten Reise/n keine Begebenheit oder eine durch mich oder andere hervorgerufene Handlung wahrgenommen habe, die diese Sendung gefährdet haben könnte.

.....
(Unterschrift des Kuriers)

.....
(Abgabedatum des Kurierausweises)

Hinweise zur Versendung von VS an Empfänger im Ausland durch diplomatischen Kurier

1. Die Weitergabe von VS der Geheimhaltungsgrade VS-VERTRAULICH und GEHEIM oder von nicht-deutschen VS mit vergleichbaren Geheimhaltungsgraden an oder über Auslandsvertretungen (z.B. Botschaften, Generalkonsulate) erfolgt entsprechend den Vorschriften des Abschnittes 6.10 GHB und dieser Anlage. Die Richtlinien für die Beförderung von Kuriersendungen können bei der VS-Kurierstelle des Auswärtigen Amtes erfragt werden. Tel.: +49 30 50002100; Email: 115-500@auswaertiges-amt.de

2. Die Unternehmen beantragen bei BMWi die Versendung von VS der Geheimhaltungsgrade VS-VERTRAULICH und GEHEIM oder von nicht-deutschen VS mit vergleichbaren Geheimhaltungsgraden unter Beifügung einer Kopie von Versand- und Begleitschein nach Anlage. BMWi bestätigt der Kurierstelle des Auswärtigen Amtes, dass es sich um ein geheimschutzbetreutes Unternehmen handelt, und teilt dem Unternehmen mit, dass die Sendung der Kurierstelle des Auswärtigen Amtes zugeleitet werden kann.

3. Die VS ist gemäß 6.10.2 GHB zu verpacken. Der Begleitschein nach Anlage ist auf dem inneren Umschlag anzubringen. Auf dem Begleitschein sind Ansprechpartner und Telefonnummer des Empfängers vor Ort anzugeben. Die Sendung ist für den weiteren Transport möglichst kompakt zu halten.

4. Die VS sind verschlossen der Kurierstelle des Auswärtigen Amtes mit Versandschein nach Anlage zuzuleiten. Für jede Auslandsvertretung ist ein gesonderter Versandschein zu fertigen. Der Versandschein dient der Kurierstelle des Auswärtigen Amtes als Unterlage für die Abfertigung und trägt deshalb keinen Geheimhaltungsgrad.

5. Die Sendungen sind gegen Empfangsbestätigung der Kurierstelle des Auswärtigen Amtes zu übergeben bzw. zu übermitteln.

   Sofern VS durch einen privaten Zustelldienst übersandt werden, sind sie der Kurierstelle des Auswärtigen Amtes mit Versandschein in einem weiteren Umschlag entsprechend des Abschnittes 6.10.3 GHB zuzuleiten.

   Die Anschrift lautet: Auswärtiges Amt; VS-Kurierstelle; Kurstr. 36; 10117 Berlin. Die Sendung muss unter 115-500@diplo.de oder unter Telefon: 030-50002100 angekündigt werden. Ist die Sendung termingebunden, so ist auf dem Begleit- und Versandschein zu vermerken, bis zu welchem Zeitpunkt die Sendung dem Empfänger vorliegen muss.

6. Sofern die Auslandsvertretung nicht selbst Endempfänger ist, ist die Sendung von dem im Begleitschein angegebenen Empfänger in der Auslandsvertretung abzuholen.

Begleitschein

Absender

Bezeichnung der Auslandsvertretung, Ort, Land

Begleitschein

Datum

Es wird gebeten, die beiliegende Verschlusssache

☐ GEHEIM ☐ VS-VERTRAULICH (oder nicht-deutsche VS mit vgl. Geheimhaltungsgraden)

sicher weiterzuleiten an

Empfänger

Unterschrift

Versandschein

Absender

Auswärtiges Amt
VS-Kurierstelle
Kurstr. 36

10117 Berlin

Versandschein

Datum

Es wird gebeten, die beiliegende Verschlusssache

mit der Bitte ☐ den beiliegenden Umschlag ☐ die beiliegenden Umschläge

Anzahl

(verschlossen)

durch persönlichen Kurier weiterzuleiten an

Bezeichnung und Ort der Auslandsvertretung

Haftungsausschluss- und Kostenübernahmeerklärung:

Unter Bezugnahme auf die mir bekannten Richtlinien für die Beförderung von Kuriersendungen erkläre ich mich hiermit damit einverstanden, dass das Auswärtige Amt im Falle von Verlust, Beschädigung oder verzögerter Zustellung der Sendung(en) keine Haftung übernimmt.

Die Transportkosten für diese Sendung(en) sollen mir unter folgender Adresse in Rechnung gestellt werden:

Unternehmen

Vollständige Anschrift

Unterschrift

Federal Ministry
for Economic Affairs
and Energy
German Designated Security
Authority
Industrial Security
D-53107 Bonn / Germany

INTERNATIONAL COURIER CERTIFICATE

For a Single International Hand Carriage or Transport of Classified Documents or Material at the level of CONFIDENTIAL or SECRET by Contractor Personnel

Project:	**Courier Certificate No.:**

This is to certify that the bearer

Name:		**First Name:**	
DoB:	**PoB:**		**Nationality:**
Passport / Identity Card No:			
Issued by (issuing authority)**:**			**Date of Issue:**
Employer (company)**:**			

is authorised to carry or accompany on the travel a consignment containing documents or material classified at the level of CONFIDENTIAL or SECRET as detailed in the attached "Description of Shipment".

The attention of Customs, Police, and / or Immigration Officials is drawn to the following:

1. **The material comprising this consignment is classified in the security interests of the following countries or International Organisations:**
2. **It is therefore requested that**
   - **a) This courier certificate and other shipping documents are recognised as official documents and priority is given to the shipment;**
   - **b) The consignment will not be inspected by persons other than duly authorises government officials or persons having a special government permission;**
   - **c) In case an inspection of the consignment is deemed necessary, it is requested that the inspection is carried out in the presence of the courier and in an area that is out of sight of unauthorised individuals;**
   - **d) A consignment, which has been opened for inspection must be closed again by showing evidence of the opening through sealing and signing, and by annotating on the shipping documents, if available, that the consignment has been opened;**
   - **e) Customs, Police, and/or Immigration Officials of the country of origin or destination of the consignment, or countries to be crossed, give necessary assistance to assure successful and secure delivery of the consignment.**

Name (Issuing government representative) Stamp:

Signature

Name: (Issuing company security officer) Stamp:

Signature

Federal Ministry
for Economic Affairs
and Energy

German Designated Security
Authority
Industrial Security
D-53107 Bonn / Germany

INTERNATIONAL MULTI-TRAVEL COURIER CERTIFICATE

For International Hand Carriage or Transport of Classified Documents or Material at the level of CONFIDENTIAL or SECRET by Contractor Personnel

Project:	**Courier Certificate No.:**
Issuing Date	**Expiry Date:**

This is to certify that the bearer

Name:		**First Name:**
DoB:	**PoB:**	**Nationality:**
Passport / Identity Card No:		
Issued by (issuing authority)**:**		**Date of Issue:**
Employer (company)**:**		

is authorised to carry or accompany on the travel a consignment containing documents or material classified at the level of CONFIDENTIAL or SECRET as detailed in the attached "Description of Shipment".

The attention of Customs, Police, and / or Immigration Officials is drawn to the following

1. **The material comprising this consignment is classified in the security interests of the following countries or International Organisations:**
2. **It is therefore requested that**
   a) **This courier certificate and other shipping documents are recognised as official documents and priority is given to the shipment;**
   b) **The consignment will not be inspected by persons other than duly authorises government officials or persons having a special government permission;**
   c) **In case an inspection of the consignment is deemed necessary, it is requested that the inspection is carried out in the presence of the courier and in an area that is out of sight of unauthorised individuals;**
   d) **A consignment, which has been opened for inspection must be closed again by showing evidence of the opening through sealing and signing, and by annotating on the shipping documents, if available, that the consignment has been opened;**
   e) **Customs, Police, and/or Immigration Officials of the country of origin or destination of the consignment, or countries to be crossed, give necessary assistance to assure successful and secure delivery of the consignment.**

Name (Issuing government representative)

Stamp

Signature

Name (Issuing company security officer)

Stamp

Signature

Appendix 1
to Courier Certificate No:

Shipment No.:

DESCRIPTION of SHIPMENT & ITINERARY

Kind of Classified Consignment / Freight:					
Documents / Data Storage Media	☐	**Components / Equipment**	☐		
Total Number of Packages / Envelopes / Components		**Size or Weight** (if appropriate)			
Sender: (name, address)					
Sender's Classified Reference / Serial Numbers					
Recipient: (name, address)					
Duration of Carriage / Transport (dates)	**From:**		**To:**		
Itinerary (countries)	**Country of Origin:**		**Destination Country:**		
	Countries Crossed:				
	Authorised Stops: (locations)				
Courier(s) (list further individuals accompanying the transport, if appropriate)	**Name(s):**				
Issuing Company Security Official	**Name:**	**Function:**			
	Date: **Place:** **Signature:** **Stamp:**				

GHB – Anlage 65

ERKLÄRUNG (NACH ABSCHLUSS DER REISE ZU UNTERSCHREIBEN)

Ich erkläre hiermit, dass ich während der von Kurierausweis Nr. _____ abgedeckten Reise/n keine Begebenheiten oder eine durch mich oder andere hervorgerufene Handlung wahrgenommen habe, die diese Sendung gefährdet haben könnte, außer der nachfolgend genannten Vorkommnisse (falls erforderlich):

Ort und Datum der Erklärung:

Unterschrift des Kuriers: _____

Name und Unterschrift des Sicherheitsbevollmächtigten: _____

(Translation)

DECLARATION TO BE SIGNED ON COMPLETION OF (EACH) SHIPMENT

I declare in good faith that, during the journey according Courier-Certificate No. _____, I am not aware of any occurrence or action, by myself or by others, that have resulted in the compromise of the consignment, except the events related below (if needed):

Place and date of declaration:

Courier’s signature: _____

Witnessed by (name and signature of company Security Officer): _____

International Transportation Plan

(to be submitted in English only)

Please approve the following Transportation Plan:

A 1	**Consignor:** [Name, Address, Phone and Fax Number of dispatching Security Officer]	
A2	**Consignee:** [Name, Address, Phone and Fax Number of receiving Security Officer]	
B	**DSA/NSA PoC:** (Address, Emailad, Phone and Fax Number of authorised Point of Contact (PoC) in the dispatching and the receiving country as well)	
C	**Description of Consignment:**	
C 1	Contract or Tender Number:	
C 2	Export License or other applicable Export Authorization citation:	
C 3	Transport License for consignment of hazardous material:	
C 4	Consignment Description: [Description of Consignment and Classification level — if possible use abbreviation (C) (S)]	
D	**Package Description:**	
D 1	Type of package: [e.g.box, card, metal box]	
D 2	Number of packages:	
D 3	Number of enclosed classified items in each package:	
D 4	Package dimensions:	
D 5	Package weight:	

Cont'd

E	**Routing of Consignment:**		
E 1	Date/time of Departure:		
E 2	Date/estimated time of arrival:		
E 3	Routes to be used between point of origin, point of export, point of import and ultimate destination: [Locations of Transfer — if possible encode locations]		
E 4	Method of transport for each portion of the consignment: [Name and Adress of all shipment companies involved — if possible specify Flight, Train or Ship Number]		
E 5	Freight Forwarders/Transportation Agents to be used: [Name, Address, Phone and Fax Number of all commercial courier companies involved — The companies have to hold Facility Security Clearances up to the classification and safeguards level necessary]		
E 6	Customs or Port Security Contacts: [Name, Phone and Fax Number of PoC's]		
F	**Authorized courier(s):**		
F 1	Name(s) and identification of authorized Courier(s): [Name, First Name, Date of Birth, Passport-/ID-Card No. and Courier Certificate used]	1.	
G	**Security Officer's signature, date and stamp of the requesting facility:**		
H	**Signature, date and seal of the releasing NSAJDSA:**		

I	Signature, date and seal of the receiving NSA/DSA:	

GHB - Anlage 66b

Details of Hand Carriage of Classified Items by Approved Company Courier

Dispatching Facility: (gov. /mil. establishment / company, location, country)				
Destination of Consignment: (gov. / mil. establishment / company, location, country)				
Point of Contact (PoC):				
Date(s):				
Project / Programme:				
Nature of Item(s) / Material & Classification Level of Shipment: (e.g. documents, data storage media, other material)				
Itinerary: (travel route indicating main locations/cities / airports/ railway stations to be passed)				
The classified item(s) shall be:		☐ **left at the destination** ☐ **returned immediately after processing** (same courier(s), route backwards, date – see above)		
		☐ **additionally, another classified consignment shall be picked up at the destination** (same courier(s), route backwards, date and nature of item(s) as described above)		
Flight Details (where appropriate)				
		1st Flight	**2nd Flight**	**3rd Flight**
Flight No.				
Departure from:	**IATA-Code**			
	Date			
	Time			
Arrival at:	**IATA-Code**			
	Date			
	Time			
Details of Vehicle used (where appropriate)				
☐ **Complete Journey by Car**		☐ **Transfer to Airport**	☐ **Transfer from Airport**	
Car: (rental car, taxi, company car, etc.)				
Car Registration No.:				
Courier Details				
Name, First Name:				
Date of Birth:				
Nationality:				
ID Document:				
No. Courier Certificate used (serial number issued by NSA/DSA):				
Employed by: (company)				
Company PoC:				

(all times are local times)

Merkblatt zum VS-Transport per Luftfracht

(1) In Ausnahmefällen ist zu besonderen Bedingungen eine Beförderung von VS, die nach Art und Umfang einen grenzüberschreitenden Transport auf dem Luftweg erfordern, durch nicht geheimschutzbetreute Luftfrachtunternehmen möglich, mit denen BMWi eine Rahmenvereinbarung abgeschlossen hat (zugelassene Luftfrachtunternehmen). Die Beförderung darf von Deutschland aus nur in Länder erfolgen, mit denen Deutschland multi- oder bilaterale Geheimschutz-Vereinbarungen abgeschlossen hat. Luftfrachttransporte vom Ausland nach Deutschland sind nach den nationalen Geheimhaltungsvorschriften des Landes des Absenders abzuwickeln.

(2) Bisher von BMWi zugelassenes Luftfrachtunternehmen ist die Lufthansa Cargo AG, Frankfurt/Main.

(3) Allgemeine Voraussetzung für die Benutzung des Luftfrachtunternehmens ist die vorherige Unterrichtung von BMWi über
- Name und Anschrift des Absenders und Empfängers der VS,
- Flugnummer, planmäßige Abflugs- und Ankunftszeit des Fluges,
-Luftfrachtbriefnummer, die innerhalb "Safe td/1" von Lufthansa Cargo AG vergeben wird,
- genaue Bezeichnung des Abflug- und Ankunftsflughafens,
- bei planmäßigen Zwischenlandungen die Ankunfts- und Weiterflugzeiten sowie die genaue Bezeichnung des Flughafens, auf dem zwischengelandet wird,
- Namen und Anschriften der beteiligten Luftfrachtagenten und Speditionen,
- Art und Geheimhaltungsgrad der VS,
- Programm bzw. Projekt, das der Weitergabe der VS zu Grunde liegt,
- Art der Verpackung, Anzahl und Merkmale der Verpackungsstücke.

BMWi sind diese Angaben so rechtzeitig vor Transportbeginn zu übermitteln, dass sie den Sicherheitsbehörden der beteiligten Länder ausreichend lange vor dem Transport mitgeteilt werden können. Die Versendung darf erst nach Einwilligung durch BMWi erfolgen.

(4) Besondere Bedingung für die Benutzung der Lufthansa Cargo AG ist, dass die Luftfracht ausschließlich mit der Versendungsart für Wertfracht "Safe td/1" befördert wird. Die Transportverträge werden unmittelbar zwischen dem geheimschutzbetreuten Unternehmen und der Lufthansa Cargo AG geschlossen. Die Versendung hat über ein Unternehmen, im Regelfall eine Spedition mit einem von der IATA zugelassenen Luftfrachtagenten, zu erfolgen, das die Wertfracht beim geheimschutzbetreuten Unternehmen abholt, zur Lufthansa Cargo AG verbringt und die Modalitäten des Luftfrachttransports für den Kunden direkt mit der Lufthansa Cargo AG durch Erstellung eines Luftfrachtbriefes regelt. Ansprechpartner bei der Lufthansa Cargo AG ist der Manager Regulatory Affairs & Special Loads:

Herr Marc Harry Emil Müller
Lufthansa Cargo AG
FRA F/HG-P
60546 Frankfurt am Main
Tel.: 069-696 46978
Mobil: 0151-589 03441
Email: Marc.Mueller@dlh.de

GHB - Anlage 68

Grenzüberschreitender Versand von Verschlusssachen (VS) des Geheimhaltungsgrad VS-VERTRAULICH oder vergleichbar eingestufter nichtdeutscher VS durch private Zustelldienste

Die grenzüberschreitende Versendung von Verschlusssachen mit einer Einstufung bis zum Geheimhaltungsgrad VS-VERTRAULICH oder vergleichbar eingestufter nichtdeutscher VS durch private, nicht geheimschutzbetreute, Zustelldienste ist unter den nachfolgenden Voraussetzungen zulässig:

1. Diese Versandart ist für folgende Verschlusssachenarten zugelassen:

    a) VS der NATO,

    b) VS der EU,

    c) VS der ESA,

    d) VS der OCCAR,

    e) Deutsche und nichtdeutsche VS, die auf der Grundlage von bilateralen Geheimschutzabkommen ausgetauscht werden, wenn diese Versandart mit dem Partnerland vereinbart worden ist[1],

Solche VS dürfen an nicht-öffentliche Empfänger im Ausland nur dann auf diesem Weg versandt werden, wenn über den Empfänger eine FSC-Bestätigung mit Aufbewahrungsmöglichkeit für VS bis vergleichbar VS-VERTRAULICH vorliegt.

2. Anforderungen an den privaten Zustelldienst

Der private Zustelldienst und dessen Versanddienstleistungen müssen folgenden Anforderungen genügen:
Das Unternehmen muss

a) seinen Firmensitz in Deutschland oder in einem Mitgliedstaat der NATO oder der EU haben;

b) Nachweise über die Einlieferung der Sendung oder deren Annahme durch den Zustelldienst sowie über die Zustellung der Sendung an den ausländischen Empfänger erbringen;

c) ein manuelles oder elektronisches System zur Sendeverfolgung haben, welches eine lückenlosen Verbleibskontrolle der Sendung von der Versendung bis zur Zustellung ermöglicht;

d) die Zustellung der Sendung innerhalb Europas binnen 24 Stunden und außerhalb Europas binnen 48 Stunden garantieren können.

[1] Diese Versandart kann generell auch für den Versand von VS in die Teilnehmerländer des EDIR-Rahmenabkommens (Frankreich, Italien, Großbritannien, Spanien, Schweden) genutzt werden.
Die Länder, mit denen im Rahmen von bilateralen Geheimschutzabkommen eine solche Vereinbarung getroffen worden ist, können beim BMWK/ZC4 unter zc4-international@bmwk.bund.de erfragt werden.

3. Verpacken der Sendung

Die Sendung ist gem. Abschnitt 6.10.2(2) in einem doppelten Umschlag zu verpacken.

Der äußere Umschlag ist neutral an die Poststelle des Empfängers zu adressieren.

Der innere Umschlag ist i.d.R. an die *„Classified Registry*“ des ausländischen Empfängers oder im Falle der Versendung an ein Unternehmen an den in der FSC-Bestätigung genannten Facility Security Officer zu adressieren.
Auf den inneren Umschlag ist neben der Angabe des Geheimhaltungsgrades und der Tagebuchnummer des Einsenders zudem der vom BMWK zur Verfügung gestellte Aufkleber mit einem Warnvermerk in deutscher und englischer Sprache anzubringen:

Der Aufkleber hat folgenden Wortlaut:

*„**STOP***
*Der Inhalt dieser Sendung unterliegt im Interesse der Sicherheit der Bundesrepublik Deutschland, der NATO, der EU oder einer anderen internationalen Organisation, oder eines anderen Staates der **Geheimhaltung**.*
Die Sendung darf deshalb nur vom Empfänger geöffnet werden.
Die unbefugte Öffnung kann strafrechtlich verfolgt werden.
***Die Sendung ist daher ungeöffnet wieder an den Einsender zurück zu geben**."*

Die Aufkleber sind fortlaufend nummeriert und werden vom BMWK mit Dienstsiegel und Unterschrift versehen.

Auf dem Aufkleber unten rechts muss der SiBe nur das Absendedatum eintragen.

Die Aufkleber können bei BMWK/ZC4 unter zc4-international@bmwk.bund.de angefordert werden.
Für die Anforderung sind ist folgende Angaben erforderlich:

- Firmenname und BMWK-Firmennummer;
- Anzahl der benötigten Aufkleber;
- Bezeichnung des Auftrages, Projektes oder des internationalen Programmes;
- Name und Anschrift des / der Empfänger
- Bestätigung, dass für den nicht-öffentlichen Empfänger im Ausland eine FSC-Bestätigung vorliegt[2]

Nicht mehr benötigte Aufkleber sind an BMWK/ZC4 zurückzugeben.

[2] Soweit für den nicht-öffentlichen Empfänger im Ausland noch keine FSC-Bestätigung vorliegt, ist diese nach den Vorgaben des GHB beim BMWK zu beantragen.

4. Vorbereitung des Versands

Der Versender hat sich vor der Beauftragung nachweislich zu vergewissern, dass der ausgewählte private Zustelldienst sowie die spezifische Versandart die Anforderungen gemäß Abschnitt 2 erfüllen und sofern es sich bei dem Empfänger um ein Unternehmen handelt, dass ihm über dieses eine gültige FSC-Bestätigung bis zum Geheimhaltungsgrad vergleichbar VS-VERTRAULICH vorliegt.

Eine Versendung ist nur an Tagen vor Werktagen, nicht jedoch vor Wochenenden oder Feiertagen zulässig. Maßgeblich sind die Feiertagsregelungen im Sende- und Empfangsland.

Vor Versendung hat der Versender den Empfänger

a) über die Versendung in Kenntnis zu setzen,

b) den Empfänger zu bitten, ihn über den Eingang der Sendung zu informieren.

Der Absender darf die Sendung nur gegen Nachweis der Annahme an den privaten Zustelldienst übergeben.

5. Nachverfolgen der Sendung

Sobald die Sendung verschickt wurde, muss eine Rückmeldung an BMWK/ZC4 erfolgen. Diese Meldung soll folgende Daten beinhalten:

Name und Anschrift des Empfängers,
- Datum der Absendung,
- Serien-Nr. des Aufklebers.

Wird der Versender vom Empfänger darüber unterrichtet, dass die Sendung nicht am angekündigten Empfangstag dort eingegangen ist, hat der Versender den Sachverhalt unverzüglich mit dem beauftragten privaten Zustelldienstes zu klären.

Bei Unklarheit

a) über den Verbleib der Sendung,
b) der Rücksendung einer vom Zustelldienst geöffneten VS-Sendung,
c) bei Verdacht des Verlustes oder einer möglichen anderweitigen unbefugten Öffnung der Sendung oder
d) bei sonstigen Unregelmäßigkeiten während der Beförderung der VS,

ist umgehend das BMWK/ZC4 zu unterrichten.

Eingehende VS-Empfangsscheine sind gem. Abschnitt 6.6.2 GHB zu behandeln.

Leitfaden für den Aufbau einer „Anlagenspezifischen Daten-VS-Anweisung (ITGA)“

(Ergänzende Anforderungen des BMWi für die Bearbeitung von Verschlusssachen mit informationstechnischen (IT-) Systemen)

A. Grundsätze

1. Gegenstand der ITGA sind alle geheimschutzrelevanten Sicherheitsanweisungen, die beim Betrieb eines IT-Systems, das für VS-Bearbeitung (VS-VERTRAULICH und höher) eingesetzt wird, zu beachten sind. Im Regelfall ist die ITGA bei dem IT-System bereitzuhalten bzw. den Nutzern und Verwaltern zu Kenntnis zu geben.

2. Grundlage für die Erstellung einer ITGA sind die VSITR/U und die allgemeinen amtlichen, sowie die spezifischen Forderungen des BMWi, die projektbezogen festgelegt werden.

3. In der Regel ist für jedes IT-System, das für VS-Bearbeitung eingesetzt wird, seitens des Unternehmens eine ITGA zu erstellen. Ausnahmen gelten z.B. bei geschlossenen Netzen, die in einem räumlichen Zusammenhang stehen und für das gleiche Projekt genutzt werden. Diese ist vor Inbetriebnahme des IT-Systems mit dem BMWi abzustimmen. Die Freigabe der einzelnen Komponenten eines IT-Systems (Hardware und Software) für die VS-Bearbeitung erfolgt gesondert und ist Voraussetzung für den VS-Betrieb.

4. Soll eine übergreifende Sicherheitsanweisung für den Betrieb von IT-Systemen angewendet werden, so kann diese in den einzelnen ITGA’s referenziert werden, ohne die Regelungen im Einzelnen zu wiederholen. In einer ITGA kann ggf. auch der Betrieb mehrerer IT-Systeme zusammengefasst werden, jedoch ersetzt eine übergreifende Sicherheitsanweisung grundsätzlich nicht die systemspezifische ITGA.

5. Auszüge aus einer ITGA können bei Bedarf angefertigt und einzelnen Komponenten eines IT-Systems zugeordnet werden. Die ITGA selbst muss vollständig sein, auf Auszüge ist zu verweisen. Ebenso ist in den Auszügen die ITGA zu referenzieren. Die ITGA ist VS-NfD einzustufen und entsprechend zu behandeln.

B. Inhalt

1. Eine ITGA sollte folgende Punkte berücksichtigen:
   - Deckblatt mit den wichtigsten Angaben (s. Muster)
   - Fortschreibung der VS-Projekte / VS-Aufträge (Referenz), für die das System aktuell eingesetzt wird (ggf. Liste anfügen).
   - Beschreibung der Lokalität des Systems bzw. der Komponenten
   - Verweis auf entsprechende Kontroll-/Sperrzonenanweisungen, die für die vorgenannten Örtlichkeiten bestehen.
   - Benennung und Fortschreibung der Personen, die für die Nutzung oder Verwaltung des Systems bzw. von Komponenten autorisiert sind (ggf. Liste anfügen).
   - Beschreibung des Systems
     - Hardware
     - Software; insbesondere das Betriebssystem
     - Netzwerkverbindungen

- Systemkonfiguration in Bezug auf sicherheitsrelevante Aspekte, z. B.
  - Benutzeridentifizierung
  - Benutzerauthentifizierung
  - Verschlüsselung
  - Netzwerksicherheit
  - Zugriffsschutzmechanismen
  - Virenschutz
  - etc.

- Materielle Absicherung des Systems (neben den o. a. Kontroll-/Sperrzonenanweisungen)
  - Siegelmarken
  - Verplombung
  - etc.
- Maßnahmen gegen kompromittierende Abstrahlung
  - Sind Maßnahmen vorgeschrieben?
  - Wenn ja: (zutreffende Alternative ausführen)
    - Angaben zur Zonenbewertung der Systemkomponenten und der Räumlichkeiten
    - Angaben einer Zeitmatrix mit Vorschriften zur Erfassung der VS-Rechenzeiten
    - Angaben zum Einsatz von TEMPEST-Gerät
    - andere Maßnahmen
- Weitergehende Vorschriften zum Durchführen, Erfassung und Protokollieren von Aktivitäten, z. B.
  - Löschen von VS-Datenbeständen
  - Trennen / Herstellen von Netzwerkverbindungen
  - Datenübertragung (nach außerhalb)
  - Einrichten eines VS-Betriebsmodus / Verlassen des VS-Betriebsmodus
- Handhabung, Verwaltung und Kennzeichnung von VS-Datenträgern (neben den allgemeinen Vorschriften zur Kennzeichnung und Verwaltung von VS-Material)
- Bestimmungen für den Betrieb von Verschlüsselungssystemen
  - Schlüsselverwaltung
  - sonst.
- Vorsorge bei Störungen, Systemausfall, Datenverlust
  - Beschreibung des Back Up / Recovery Verfahrens (Zuständigkeit)
  - Bestimmungen zum Booten des Systems (Zuständigkeit)
  - Maßnahmen bei Wartung und Reparatur
    - Herstellen des Wartungsmodus
    - Entfernen der VS-Daten
    - sonst.
- Benennung der Stellen und Personen die
  - bei Systemfehlern, Problemen berechtigt sind, Hilfe zu leisten
  - Meldungen bei besonderen Vorkommnissen entgegennehmen
  - sonst.
- Weitergehende Pflichten der Nutzer, Verwalter zu
  - Anzeige von Veränderungen an der Systemkonfiguration, insbesondere bei Hardware-/Software-Updates
  - allgemeine Meldepflichten (ggf. turnusmäßig – auch Fehlanzeige)
  - sonst.

2. Beim Erstellen der ITGA sind insbesondere Vorschriften zu berücksichtigen, die sich aus Vereinbarungen in internationalen Projekten (z. B. Projekt Security Instructions) und Vorschriften internationaler/übernationaler Organisationen (z. B. NATO) ergeben.

GHB – Anlage 70

Richtlinien zur Nutzung von Telekommunikations- oder anderen technischen Kommunikationseinrichtungen für die Übermittlung von Verschlusssachen (VS) in Unternehmen (Krypto - Richtlinien)

A: Kryptomittel, die von der Bundeswehr - National Distribution Agency Germany (NDA Germany) bereitgestellt werden

Für die Erfüllung von nationalen bzw. internationalen VS-Aufträgen ist auf Veranlassung des VS-Auftraggebers gegebenenfalls die Ausstattung von Unternehmen mit Kryptomitteln der Bundeswehr, der NATO, der EU sowie von sonstigen internationalen Stellen erforderlich.

Von der Bundeswehr - National Distribution Agency Germany (NDA Germany) wurden Richtlinien zur Behandlung von Kryptomitteln herausgegeben. In diesen Richtlinien wurden die Sicherheitsmaßnahmen (einschließlich der Anwendung von materiellen Sicherheitsmaßnahmen) für Kryptomittel festgelegt.

Diese Richtlinien regeln die Behandlung, den Einsatz und die Nutzung von Kryptomitteln. Sie fassen die wesentlichen Bestimmungen des Kryptowesens der Bundeswehr, der NATO und der EU zur Handhabung, Verteilung und zur Nachweisführung von Kryptomitteln zusammen und legen Schutzmaßnahmen zur Herstellung und Erhaltung der Kryptosicherheit fest.

Diese Richtlinien gelten ausschließlich für Kryptomittel der Bundeswehr, der NATO, der EU oder sonstiger internationaler Stellen, die über die NDA Germany bereitgestellt werden.

Unternehmen, die Kryptomittel benötigen, müssen sich gegenüber dem VS-Auftraggeber verpflichten, geeignete Verfahren zu implementieren, um die Einhaltung dieser Richtlinien sicherzustellen. NDA Germany darf die Einhaltung dieser Richtlinien in den Unternehmen prüfen bzw. prüfen lassen.

Die Richtlinien zur Kryptosicherheit können bei der NDA Germany angefordert werden.

Für die Wahrnehmung der Aufgaben der Kryptoverwalterung ist ein/e Kryptoverwalter/in bzw. stellvertretende/r Kryptoverwalter/in im Rahmen einer formellen Schulung auszubilden.

Ansprechpartner:

bei Kryptomitteln der Bundeswehr und der NATO / EU das

Zentrum für Cyber-Sicherheit der Bundeswehr
NDA Germany
Münstereifeler Straße 75
53359 Rheinbach

Tel. Leiter NDA: 02226 88 1710
Tel. Leitender Kryptoverwalter: 02226 88 1711
Fax: 02226 88 1702

bei anderen Kryptomitteln das

BSI - Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183
53175 Bonn
Telefon: 0228/9582-0
Telefax: 0228/9582-400

Für die Behandlung von Kryptomitteln des Bundes, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bereitgestellt werden, sind die nachfolgend abgedruckten bisherigen Krypto-Richtlinien weiter anzuwenden, bis das BSI eigene Richtlinien für die Behandlung, den Einsatz und die Nutzung von Kryptomitteln herausgeben wird.

B: Kryptomittel, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bereitgestellt werden

§ 1 Anwendbarkeit

Diese Richtlinien sind bei der Übermittlung von VS der Geheimhaltungsgrade VS-VERTRAULICH und höher unter Benutzung von Telekommunikations- oder anderen Kommunikationseinrichtungen anzuwenden.

§ 2 Allgemeine Grundsätze

(1) Die Nutzung von Telekommunikations- oder anderen technischen Kommunikationseinrichtungen zur Übermittlung von VS bedarf der Zustimmung des BMWi.
VS sind grundsätzlich vor einer Übermittlung mittels Telekommunikations- oder anderer technischer Kommunikationseinrichtungen
- zu kryptieren oder
- durch andere gleichwertige Maßnahmen zu sichern (z.B. approved circuits). Die erforderlichen Maßnahmen werden im Einzelfall durch BMWi festgelegt.

(2) Zum Kryptieren von VS dürfen nur Kryptosysteme verwendet werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den betreffenden Geheimhaltungsgrad zugelassen oder vom amtlichen VS-Auftraggeber beigestellt sind. Eine Genehmigung für deren Einsatz erteilt BMWi in Abstimmung mit den Fachdienststellen. (vgl. § 14 VS-IT-Richtlinien/Unternehmen).

(3) Komponenten von Kryptosystemen, die für eine Kryptierung von VS zugelassen sind, sowie die dazu gehörenden systembezogenen Anweisungen sind regelmäßig VS – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) eingestuft und unterliegen neben den Richtlinien für VS– NfD zusätzlichen Behandlungsvorschriften. Diese VS-NfD-Einstufung gilt nur so lange die Komponenten keine Kryptovariablen enthalten. Sind die enthaltenen Kryptovariablen höher eingestuft, sind die Komponenten entsprechend dieser höheren Einstufung zu behandeln.

Die Komponenten erhalten zusätzlich eine Abstrahl-Prüfplakette und BSI-Manipulationserkennungs-Plaketten (MEPs).

Kryptodatenträger sind neben dem Geheimhaltungsgrad mit dem Warnvermerk ”KRYPTO” in gleicher Farbe wie der jeweilige Geheimhaltungsgrad zu kennzeichnen.

(4) Zugang zu Kryptogeräten, Kryptodatenträgern und Kryptounterlagen, die VS-VERTRAULICH oder höher eingestuft sind oder Kryptovariablen enthalten, die VS-VERTRAULICH oder höher eingestuft sind, dürfen nur ausreichend ermächtigte Personen erhalten, die von dem/der SiBe schriftlich bestellt (Kryptoverwalter/-in und Vertreter/-in gemäß § 4(1)) und/oder über die Besonderheiten des Umgangs mit Kryptomitteln nachweislich belehrt wurden (Muster 3). Sämtliches Kryptopersonal sowie dessen Unterrichtung ist in einem Nachweis (Muster 2) aktenkundig zu machen.

Für die Bearbeitung von VS-NUR FÜR DEN DIENSTGEBRAUCH KRYPTO eingestuften Unterlagen reicht eine nachweisbare Belehrung aus (Muster 3).

§ 3 Begriffsbestimmungen

Kryptieren/Dekryptieren: Klartext mittels eines Kryptosystems durch Verschlüsseln oder Codieren in unverständliche Form (Kryptotext) umwandeln bzw. Kryptotext in verständlichen Klartext rückwandeln.

Kryptobetriebsstelle: Vom BMWi zugelassene Räumlichkeit, in der Kryptomittel eingesetzt und betrieben werden.

Kryptodaten: Bestandteile der Zeichenfolge, die eine Kryptovariable bildet.

Kryptodatenträger: Datenträger, der Kryptovariable enthält.

Kryptogerät: Gerät, das nach einem kryptologischen Prinzip kryptiert.

Kryptomaterial: Oberbegriff für Kryptogerät und Zubehör.

Kryptomittel: Oberbegriff für Kryptounterlagen und Kryptomaterial.

Kryptopersonal: Personal, das zum Zugang zu und Umgang mit Kryptomitteln berechtigt ist.

Kryptoschlüssel: Kryptovariable bzw. Kryptodatenträger.

Kryptosystem: Zusammengehörige Kryptomittel, die eine bestimmte Kryptierung ermöglichen.

Kryptounterlage: Unterlage, die Kryptoinformationen oder Kryptodaten enthält.

Kryptovariable: Folge von Zeichen, die einen Kryptiervorgang einleitet oder unmittelbar zum Kryptieren benutzt wird.

Kryptoverteilerstelle: Stelle, die in ihrem Zuständigkeitsbereich für Nachweis, Lagerung und Verteilung von Kryptomitteln verantwortlich ist.

Kryptoverwalter/in: Person, der die Verwaltung, sichere Aufbewahrung und Vernichtung von Kryptomitteln übertragen wurde.

§ 4 Verwaltung von Kryptodatenträgern und Kryptounterlagen

(1) Krytodatenträger und Kryptounterlagen sind getrennt von den übrigen VS zu verwalten. Die Verwaltung von Kryptodatenträgern und Kryptounterlagen obliegt dem/der Krypto-verwalter/in und sein/ihre Vertreter/in, die auf Vorschlag des/der SiBe vom BMWi bestellt werden (Muster 1). Die Bestellung kann ohne Angabe von Gründen zurückgenommen werden.
Jeweils eine Ausfertigung der Bestellung wird vom BMWi an die Kryptoverteilerstellen weitergeleitet. Eine Ausfertigung erhält der/die SiBe.
Der/die Kryptoverwalter/in und sein/ihre Vertreter/in sind von dem/der SiBe, soweit dieser/e bereits vom BMWi kryptobelehrt ist, nachweislich über ihre Aufgaben und Pflichten zu belehren (Muster 5).
Die Aufgaben des/der Kryptoverwalters/in können auch von dem/der SiBe, VS-Verwalter/in oder Vertreter/in wahrgenommen werden.

(2) Zum Aufgabenbereich des/der Kryptoverwalters/in gehören
- das Führen von Krypto-Bestandsverzeichnissen zu Kryptodatenträgern und Kryptounterlagen,
- die Ausgabe und Rücknahme von Kryptodatenträgern und Kryptoschlüsseln,
- das Laden von Kryptodatenträgern mit Kryptodaten und Kryptoschlüsseln,
- die Vernichtung von Kryptodatenträgern und Kryptounterlagen,
- die Aufbewahrung von Kryptodatenträgern und Kryptounterlagen.

(3) Eingehende Kryptodatenträger und Kryptounterlagen dürfen nur von dem/der Kryptoverwalter/in oder dem/der Vertreter/in gegen Empfangsbescheinigung (Muster 4) entgegengenommen, ausgehende nur von diesen übermittelt werden. Kryptodatenträger dürfen nicht unbefugt hergestellt, vervielfältigt oder auszugsweise wiedergegeben werden.

(4) Kryptogeräte, die für eine Kryptierung von VS zugelassen sind, sowie Kryptodatenträger und Kryptounterlagen sind in einem eigenen Krypto-Bestandsverzeichnis nachzuweisen. Mit Zustimmung BMWi kann im Einzelfall der Nachweis auch in den allgemeinen VS-Bestandsverzeichnissen erbracht werden. In diesem Fall ist der jeweilige Eintrag mit dem entsprechenden Warnvermerk zu kennzeichnen.

(5) Kryptodatenträger und eingestufte Kryptounterlagen sind unverzüglich durch den/die Kryptoverwalter/in zu vernichten, wenn sie nicht mehr benötigt werden. Der Vernichtungsnachweis (Muster 5) ist VS-NfD einzustufen. Vernichtungsnachweise und Bestandsberichte sind gemäss den Auflagen der Kryptoverteilerstelle aufzubewahren.
Kassetten und andere Sicherheitsverpackungen von Kryptodatenträgern und Kryptounter-lagen, die nicht von der Kryptoverteilerstelle zurückverlangt werden, sind zu vernichten.

§ 5 Versendung und Transport der Komponenten von Kryptosystemen

(1) Kryptogeräte und Zubehör, Kryptodatenträger, die mit einem Kryptoschlüssel im unverschlüsselten Zustand geladen sind, sowie Kryptounterlagen sind grundsätzlich durch Firmenkurier zu versenden.

Dabei ist der innere Umschlag bzw. die innere Verpackung mit dem Namen des/der Empfangsberechtigten, dem Zusatz ”oder Vertreter/in” und dem Zusatz ”persönlich

(KRYPTO)" zu versehen. Der äußere Umschlag bzw. die äußere Verpackung ist neutral zu adressieren.

(2) Kryptodaten bzw. Kryptoschlüssel können, wenn dies die zuständige Kryptoverteilerstelle ausdrücklich zulässt, auch auf zugelassenen technischen Kommunikationswegen übermittelt werden. Diese Übermittlung erfolgt mit einer von der Kryptoverteilerstelle festzulegenden Kryptierung. Eine Übermittlung dieser Daten hat in enger Abstimmung zwischen Kryptoverteilerstelle und dem/der Kryptoverwalter/in der empfangenden Stelle zu erfolgen.

(3) Kryptogeräte dürfen nicht mit eingelegtem/aktiviertem Kryptodatenträger bzw. unkryptiert gespeicherten Kryptodaten transportiert werden.

§ 6 Installation und Sicherung von Kryptogeräten und Kryptounterlagen einschließlich Kryptodatenträgern, Freigabe und Prüfungen

(1) Kryptogeräte, Kryptodatenträger und Kryptounterlagen sind entsprechend ihrer jeweiligen VS-Einstufung, jedoch getrennt von den übrigen VS, zu verwahren. Kryptogeräte dürfen nicht mit eingelegtem oder aktiviertem Kryptodatenträger bzw. eingegebenen Kryptodaten gelagert werden.

(2) Kryptogeräte sind gemäß den Vorgaben bzw. systembezogenen Zulassungskriterien des BSI zu installieren und insbesondere gegen kompromittierende Abstrahlung zu sichern.

(3) Die Inbetriebnahme der Kryptobetriebsstelle und somit des Kryptogerätes ist erst zulässig, wenn eine schriftliche Freigabe von BMWi vorliegt. Mit Vorlage dieser Freigabebestätigung gewährt die Kryptoverteilerstelle Zugang zu Kryptomittel.

(4) Der ordnungsgemäße Betrieb der Kryptobetriebsstelle wird alle 5 Jahre durch BMWi überprüft.

(5) Kryptobetriebsstellen sind grundsätzlich als Kontroll- bzw. Sperrzonen zu betreiben. Der Zutritt ist in der Kontroll- bzw. Sperrzonenanweisung zu regeln.

(6) In Kryptobetriebsstellen darf grundsätzlich nur ermächtigtes Personal eingesetzt werden. Personal, das nicht ermächtigt ist (z. B. Wartungs-, Reinigungskräfte), darf nur kurzfristig eingesetzt werden und ist während der Tätigkeit in der Kryptobetriebsstelle ständig zu beaufsichtigen. Die Kenntnisnahme von VS muss ausgeschlossen sein.

§ 7 Kommunikationsbetrieb

(1) Das Kryptieren und Dekryptieren darf nur in Kryptobetriebsstellen durchgeführt werden.

(2) Kryptiert empfangene VS des Geheimhaltungsgrades VS-VERTRAULICH oder höher, sind unmittelbar nach Dekryptierung der VS-Registratur zur Registrierung vorzulegen. Dabei sind folgende Informationen mitzuteilen:
- Tagebuchnummer und Bezeichnung der VS,
- Übermittlungsart der VS (z. B. Fernschreiben, Telekopie, E-Mail usw.),
- Datum und Uhrzeit der Aufnahme bzw. Absendung,
- Datum und Uhrzeit der Weiterleitung,

- Empfänger, Absender.

Der Empfang von verschlüsselten VS ist dem Absender von der VS-Registratur zu bestätigen (Anlage 47).
Bei der Übermittlung anfallendes VS-Zwischenmaterial ist unverzüglich zu vernichten.

§ 8 Sicherheitsvorkommnisse

(1) Wenn beim Kommunikations- bzw. Kryptobetrieb für VS bekannt wird oder der Verdacht entsteht, dass
- Unbefugte Zugriff auf VS erhalten haben oder ihn sich verschaffen wollten,
- Komponenten von Kryptosystemen sicherheitserhebliche Mängel aufweisen, manipuliert oder entwendet wurden oder
- die Geheimhaltung von VS in anderer Weise verletzt oder konkret gefährdet wurde,
- ist unverzüglich der/die SiBe zu benachrichtigen.

(2) Der/die Sicherheitsbevollmächtigte veranlasst bei Gefahr im Verzuge die notwendigen Maßnahmen. Er hat bei Feststellung schwerwiegender Mängel bis zu deren Beseitigung den Kommunikations- bzw. Kryptobetrieb für VS einzuschränken oder zu untersagen. Die festgestellten Mängel sind dem BMWi, dem VS-Auftraggeber und der Kryptoverteilerstelle zu melden.

(3) Sicherheitsvorkommnisse und die daraufhin veranlassten Maßnahmen sind zu dokumentieren. Die Dokumentation ist mindestens zehn Jahre aufzubewahren.

§ 9 Krypto-Geheimschutzdokumentation

Ergänzend zu einem eventuellen Geheimschutzplan ist eine Krypto-Geheimschutzdokumentation zu führen, die mindestens folgendes enthält:
- aktuelle Liste des Kryptopersonals und Verzeichnis der Kryptobetriebsstellen und Kryptogeräte für die letzten fünf Jahre,
- Zulassungskriterien sowie systembezogene Anweisungen der Kryptogeräte und Freigabebestätigungen für Kryptosysteme für die gesamte Einsatzdauer des Gerätes,
- Kontroll- und Prüfberichte, Berichte über Sicherheitsvorkommnisse und bei Einsatz von IT zusätzlich die ITGA’s für die jeweils letzten zehn Jahre.

Muster 1

Bestellung des/der KRYPTO-Verwalters/in und des/der Stellvertreters/in

Firma	*Betriebsnummer*	*Datum*
Anschrift		

Mit Wirkung vom _____ werden zum KRYPTO-Verwalter/in bzw. zum/zur Stellvertreter/in vorgeschlagen:

Lfd. Nr.	*Name, Vorname*	*Funktion*	*Überprüfungsgrad*	*Unterschrift des/der KRYPTO-Verwalters/in bzw. Stellvertreters/in*
		KRYPTO-Verwalter/in		
		Stellvertreter/in		

Der/die Krypto-Verwalter/in und der/die Stellvertreter/in sind zum Empfang von KRYPTO-Unterlagen berechtigt.

SiBe	*Firmenstempel*
_____ *Unterschrift*	

Der/die oben benannte KRYPTO-Verwalter/in und der/die Stellvertreter/in werden hiermit bestellt.

_____ *Dienstsiegel BMWi*

Unterschrift

Die Bestellung kann ohne Angabe von Gründen zurückgenommen werden. Sie erlischt automatisch mit dem Ausscheiden des/der bestellten KRYPTO-Verwalters/in bzw. Stellvertreters/in aus der o. g. Firma.

Verteiler:
1. *Ausfertigung an den/die SiBe der Firma*
2. *Ausfertigung an die zuständige KRYPTO-Verteilerstelle beim BSI*
3. *Ausfertigung verbleibt bei BMWi – Referat RS 3 -*

Muster 2

Nachweis über die Bestellung und Unterrichtung des KRYPTO-Personals

Name, Vorname, Funktion	*Ich bestätige die Unterrichtung über die erforderlichen Sicherheitsmaßnahmen für die Behandlung von KRYPTO-Unterlagen (Unterschrift/Datum)*				
	1	*2*	*3*	*4*	*5*

Muster 3

Niederschrift über die Krypto-Belehrung von Kryptopersonal

Unternehmen:.....

Betriebs-Nummer:

Ort:.....

Sicherheitsbevollmächtigter/e:.....

Kryptoverwalter/in bzw. Stellvertreter/in:.....

Kryptopersonal:.....

Personalausweisnr./Reisepassnr.:.....

ausgestellt in/am:.....

ermächtigt bis:.....

1. Als Unterzeichner/in erkläre ich, dass ich heute über die nachstehenden Sicherheitsbestimmungen belehrt worden bin.

   Ich wurde darauf hingewiesen, dass

   - ich keine Abschriften, Kopien, Auszüge aus den mir anvertrauten Kryptounterlagen ohne Genehmigung des Herausgebers fertigen darf,

   - ich Kryptomittel nur an dazu ermächtigte Personen, die dienstlich Kenntnis erhalten müssen, gegen Quittung weitergeben darf,

   - Kryptomittel gemäß § 4 KryptoRL aufzubewahren und nachzuweisen sind,

   - Kryptomittel mit dem Warnvermerk Crypto/Krypto und Kryptodruckschriften/CryptoPublications mit Kurier versandt werden müssen,

   - ich über alle Angelegenheiten des Kryptowesens Stillschweigen gegenüber Unbefugten zu bewahren habe. Dies gilt auch für die Zeit nach meinem Ausscheiden aus der Tätigkeit als Kryptoverwalter/in und/oder dem Beschäftigungsverhältnis.

   - Verstöße gegen diese zusätzlichen Sicherheitsbestimmungen über den/die Sicherheitsbevollmächtigte/n umgehend dem Bundesministerium für Wirtschaft und Energie – Referat RS 3 - zu melden sind.

Ich bin belehrt worden, dass ich mich durch Verstoß gegen diese zusätzlichen Sicherheitsbestimmungen nach den §§ 93 ff und 353 b StGB strafbar machen kann.

.....
Ort, Datum

....
Unterschrift des/der Belehrten Unterschrift des/der Belehrenden

.....
Unterschrift des/der Sicherheitsbevollmächtigten

Muster 4

Empfangsschein für KRYPTO-Datenträger (sowie ggf. andere KRYPTO-Unterlagen)

Datum *Tgb.-Nr.* *Nr.*	*1. Ausf.: sofort an Absender* *2. Ausf.: Einnahmebeleg für Empfänger* *3. Ausf.: Entwurf*
Absender	*Empfänger*

Kurzbezeichnung	*Anzahl*	*Registrier-Nr. und Ausgabe oder Prüf-Nr.*	*Ausf.-Nr.*	*Bemerkungen*

Übersandt am (Datum)	*Empfangen am (Datum)*

Name, Unterschrift, Firmen-/Dienststempel	*Name, Unterschrift, Firmen-/Dienststempel*

Muster 5

Wenn ausgefüllt: VS-NUR FÜR DEN DIENSTGEBRAUCH

Vernichtungsnachweis für KRYPTO-Datenträger

Firma	*Lfd.Nr.*

Registrier-Nr. und Ausgabe	*Ausf.Nr.*

Die nachstehend aufgeführten KRYPTO-Datenträger wurden vernichtet[1].

KRYPTO-Datenträger	**Andere Kryptomittel**		
Gültigkeitstag		***Durchführender** (Unterschrift)*	***Zeuge** (Unterschrift)*
1	*2*	*3*	*4*
01.			
02.			
03.			
04.			
05.			
06.			
07.			
08.			
09.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			

[1] *Werden KRYPTO-Datenträger für einen Monat in einem Arbeitsgang vernichtet, so genügen Datum und Unterschrift in der letzten Zeile (31.). Die Zeilen 01. bis 30. sind mit einem Diagonalstrich durchzustreichen.*