

Fragen und Antworten zur VSA

Inhaltsverzeichnis

Inhaltsverzeichnis.....	1
A. Allgemeine Bestimmungen	2
B. Geheimschutzorganisation und Geheimschutzdokumentation	4
C. Handhabung von Verschlusssachen.....	5
D. Zusammenarbeit mit nichtdeutschen Stellen.....	9
E. Materielle und technische Maßnahmen.....	10
F. Einsatz von Informationstechnik.....	11
I. Freigabeprozess.....	11
II. Zulassung.....	17
G. Kryptopersonal und Handhabung von Kryptomitteln	18
H. Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH	19
I. Sonstige Fragen	22

A. Allgemeine Bestimmungen

1. **Frage:** Was sind die besonderen Bestimmungen des Geheimschutzes?

Antwort: Zu den besonderen Bestimmungen des Geheimschutzes i. S. v. § 4 Absatz 2 Satz 2 VSA gehören insbesondere das Sicherheitsüberprüfungsgesetz (SÜG), die AVV zum SÜG, die Verschlusssachenanweisung (VSA) und dazu ergangene Vorschriften sowie weitere Dienstvorschriften.

2. **Frage:** Muss jede Person mit Zugang zu einem Netz bzw. geplantem Zugang zu einem Netz, welches für die Verarbeitung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH freigegeben ist, zugelassen werden?

Antwort: Zuzulassen sind Personen, die nicht ermächtigt sind, denen aber eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften VS verschaffen können. Die Zulassung spielt daher im Zusammenhang mit VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH keine Rolle.

Gemäß § 4 Absatz 1 VSA ist eine Person, bevor sie Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhält, auf Anlage V zu verpflichten. Auch für Verschlusssachen dieses Geheimhaltungsgrades gilt, dass von einer Verschlusssache nur Personen Kenntnis erhalten dürfen, die **auf Grund ihrer Aufgabenerfüllung** Kenntnis von ihr haben müssen (Grundsatz „Kenntnis nur, wenn nötig“, vgl. § 3 Absatz 1 Satz 3 VSA). Insoweit stellt sich in diesem Zusammenhang nicht die Frage nach einem Zugang zu einem Netz, welches für die Verarbeitung dieser Verschlusssachen freigegeben ist, sondern die Frage nach dem Erfordernis zum Zugang zu solchen VS.

Da Erstellung und Handhabung von Verschlusssachen dieses Geheimhaltungsgrades grundsätzlich in der Dienststelle erforderlich sein können, empfiehlt es sich jedoch, alle Mitarbeiter entsprechend zu verpflichten.

3. **Frage:** Wie soll mit Dienstleistern, insbesondere im Rahmen der IT-Konsolidierung, bezüglich der Verpflichtung umgegangen werden?

Antwort: Für seinen Zuständigkeitsbereich ist jeder Dienstleister für die Einhaltung der geheimschutzrechtlichen Vorschriften verantwortlich. Hierzu bedarf es einer klaren Abgrenzung der Zuständigkeitsbereiche der Dienstleister und der Dienststellen. Die umzusetzenden geheimschutzrechtlichen Vorgaben sind hierbei Gegenstand von (Rahmen-)Vereinbarungen (Dienstleister gehört dem öffentlichen Bereich an) bzw. vertraglichen Regelungen (Dienstleister gehört dem nichtöffentlichen Bereich an).

4. **Frage:** Müssen alle bereits verpflichteten Mitarbeiter auch auf die neue VSA verpflichtet werden?

Antwort: Bei nachweislich vorliegender Verpflichtung wird keine zwingende Notwendigkeit einer erneuten Verpflichtung gesehen, da diese auch bei Änderung der

Vorschriftenlage bestehen bleibt. Die Bekanntmachung der Anlage V erscheint in der Praxis jedoch geboten.

5. Frage: Müssen Mitarbeiter, die sicherheitsüberprüft sind, trotzdem auf Anlage V verpflichtet werden?

Antwort: Eine Person, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll, ist vorher einer Sicherheitsüberprüfung zu unterziehen (vgl. § 2 Absatz 1 Satz 1 SÜG). Bevor sie dann Zugang zu VS-VERTRAULICH oder höher eingestuften VS erhält oder ihr eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften VS verschaffen kann, ist sie durch den Geheimschutzbeauftragten zu ermächtigen bzw. hierfür zuzulassen (vgl. § 4 Absätze 2 und 3 VSA). D. h., dass eine durchgeführte Sicherheitsüberprüfung allein nicht zum Zugang zu VS berechtigt. Hierzu bedarf es der Ermächtigung bzw. Zulassung bezogen auf die jeweilige Tätigkeit.

Erfolgte trotz durchgeführter Sicherheitsüberprüfung keine Ermächtigung oder Zulassung für die jeweilige Tätigkeit, muss eine Verpflichtung auf Anlage V erfolgen.

Die bei der Ermächtigung und Zulassung obligatorische Verpflichtung auf den Geheimschutz (vgl. § 4 Absätze 2 und 3 VSA) umfasst auch den Zugang zu VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH.

6. Frage: Müssen die Geheimschutzbeauftragten die VS-NfD-Belehrungen durchführen und wissen, wer belehrt wurde oder kann das auch durch die Personalabteilung erfolgen?

Antwort: Da Dienststellen, die ausschließlich VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte VS handhaben, Geheimschutzbeauftragte bestellen können, aber nicht müssen (vgl. § 8 Absatz 2 VSA), liegt es auf der Hand, dass der Geheimschutzbeauftragte die Belehrungen und Verpflichtungen nicht zwingend selbst durchführen muss. Die Belehrung und Verpflichtung können somit auch durch die Personalabteilung erfolgen und der Nachweis zur Personalakte genommen werden.

7. Frage: Welchen rechtlichen Hintergrund hat die Verpflichtung für VS-NfD?

Antwort: Den rechtlichen Hintergrund der Verpflichtung bilden § 4 Absatz 3 SÜG und § 4 Absatz 1 VSA. Nach § 4 Absatz 3 SÜG sind Personen, denen Zugang zu Verschlusssachen gewährt wird, gesetzlich zur Verschwiegenheit und zum Schutz der Verschlusssachen vor unbefugter Kenntnisnahme verpflichtet. Diese Verpflichtung umfasst auch Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH. Die dabei erforderlichen Schutzmaßnahmen ergeben sich aus den Vorschriften der VSA. Gemäß § 4 Absatz 1 VSA ist eine Person, bevor sie Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NfD erhält, gegen Empfangsbestätigung auf Anlage V der VSA zu verpflichten. Die Anlage V der VSA enthält das Merkblatt zur Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NfD mit einhergehenden Schutzmaßnahmen.

8. **Frage:** Ist es zwingend erforderlich, dass ein Exemplar der Anlage V nur gegen Empfangsbestätigung zugänglich gemacht werden muss?

Antwort: Ja, damit eine Kenntnisnahme des VS-NfD-Merkblatts sichergestellt ist (vgl. § 4 Absatz 1 Satz 2 VSA)

9. **Frage:** In der VSA sind für die Ausstellung von Konferenzbescheinigungen (Muster 4 Anlage VIII zur VSA) keine weiteren Vorgaben, insbesondere zur Gültigkeitsdauer, enthalten. Wie lange soll/kann die Gültigkeitsdauer auf der Konferenzbescheinigung festgelegt werden?

Antwort: Gemäß § 4 Absatz 5 VSA ist ermächtigten Personen bei Bedarf eine Konferenzbescheinigung auszustellen. Der genannte „Bedarf“ muss sich folglich an der Dauer oder Häufigkeit eines sich ggf. wiederholenden Dienstgeschäfts orientieren. Hierbei sind ggf. auch Vorgaben zu Fristen der Stellen, für die eine solche Konferenzbescheinigung benötigt wird, zu berücksichtigen. Ebenfalls ist zu berücksichtigen, dass jedes erneute Ausstellen einer Konferenzbescheinigung zwar einen „Mehraufwand“ für die Dienststelle darstellt, die Ausstellung einer möglichst langfristigen Bescheinigung aber auch das Risiko birgt, dass bei über einen langen Zeitraum ausgestellten Bescheinigungen unerwartet eintretende Ereignisse, die zu Änderungen der Grundlage der Bescheinigung führen, nicht einkalkuliert werden können.

Ergänzend ist darauf hinzuweisen, dass die allgemeinen Verwaltungsvorschriften nach § 1 Absatz 2 und Absatz 4 VSA den spezifischen Belangen Rechnung tragende Regelungen vorsehen können.

10. **Frage:** Warum werden alle, die Zugang zu VS haben oder ihn sich verschaffen können sicherheitsüberprüft, private Zusteller jedoch nicht, obwohl VS dort über Feiertage oder Sonntage liegen bleiben können?

Antwort: Grundsätzlich kommen private Zusteller nicht unmittelbar in Kontakt mit VS, da die VS von außen nicht erkennbar sind (siehe Ziffer 3.2.3, Anlage IV zur VSA). Darüber hinaus hat die Zustellung von VS nach Ziffer 3.2.3, Anlage IV zur VSA bis zum Mittag des folgenden Arbeitstages zu erfolgen. Ein Liegenbleiben über Sonn- oder Feiertage ist folglich nicht zulässig.

B. Geheimschutzorganisation und Geheimschutzdokumentation

11. **Frage:** Was ist unter Risikomanagement nach § 8a VSA zu verstehen?

Antwort: Die Art und Weise, wie ein Risikomanagement und eine Risikoanalyse in der jeweiligen Dienststelle erfolgen und welche konkreten Maßnahmen damit einhergehen können, obliegt allein der Beurteilungshoheit der zuständigen Geheimschutzbeauftragten. Die Wahl einer dafür geeigneten Methodik bleibt den Geheimschutzbeauftragten überlassen.

Weiterführende Dokumente zur Orientierung:

- Modell eines Risikomanagements für die Bundesverwaltung vom 11.04.2017, Hrsg.: Der Präsident des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung.
- Das neue Organisationshandbuch – aus der Praxis für die Praxis, Kapitel 3.10 Risikomanagement, Hrsg.: BVA, 2023, **Fehler! Linkreferenz ungültig..**
- BSI-Standard 200-3, Risikomanagement, vor allem mit Blick auf das Risikomanagement bei VS-IT (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620).

12. Frage: Wie muss man sich die Zusammenarbeit zwischen Geheimschutzbeauftragten und IT-Sicherheitsbeauftragten vorstellen?

Antwort: Die Geheimschutzbeauftragte sind für die Umsetzung der VSA zuständig und beraten die Dienststellenleitung in allen Fragen des Geheimschutzes. Die IT-Sicherheitsbeauftragten beraten und unterstützen den Geheimschutzbeauftragten gemäß § 9 VSA in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung.

13. Frage: Gibt es Regelungen für Geheimschutzbeamte?

Antwort: Ja. § 8 Absatz 3 VSA sieht die Unterstützung der Geheimschutzbeauftragten durch besonders beauftragte Mitarbeiter vor. Deren Aufgaben sind der Anlage I zur VSA zu entnehmen.

C. Handhabung von Verschlusssachen

14. Frage: Können GEHEIM und STRENG GEHEIM eingestufte VS in einem gemeinsamen Bestandsverzeichnis geführt werden?

Antwort: Grundsätzlich ja. Mögliche Abweichungen im internationalen Bereich sind zu beachten.

15. Frage: Muss bei einem Datenträger mit unterschiedlichen VS nur der Stick oder müssen auch die sich darauf befindlichen VS nachgewiesen werden?

Antwort: Gemäß § 21 Absatz 2 VSA sind VS-VERTRAULICH oder höher eingestufte VS in VS-Registaturen so zu verwalten, dass ihre Existenz, ihre Einstufung einschließlich der Einstufungsfrist, ihr Verbleib, die Kenntnisnahmen, ihreervielfältigung und deren Verbleib sowie ihre Vernichtung nachvollziehbar sind. Daraus ergibt sich, dass unabhängig von der Aufbewahrungsart immer die einzelne VS nachzuweisen ist.

16. Frage: Gibt es eine Technische Leitlinie zum Führen eines elektronischen Bestandsverzeichnisses?

Antwort: Die Nachweisführung hat bei elektronischen VS-Registratursystemen und bei elektronischer VS-Bearbeitung nach den Nummern 2.1 und 2.1.2, Anlage IV zur VSA zu erfolgen. Eine technische Leitlinie des BSI für VS-Registratursysteme wird erstellt.

17. Frage: In Muster 17 Anlage VIII zur VSA ist oberhalb der Spaltenüberschriften auf Seite 1 der Begriff „Geschäftsnummer“ für einen Eintrag vorgesehen. In den Hinweisen zum Führen des VS-Bestandsverzeichnisses ist kein Hinweis hierzu enthalten.

Antwort: In den Bestandsverzeichnissen wird für ein Geschäftszeichen jeweils eine Doppelseite geführt. Bei der Geschäftsnummer handelt es sich somit um die Seitennummer der Doppelseite. Ist die Doppelseite für ein Geschäftszeichen „befüllt“ wird der Nachweis für VS dieses Geschäftszeichens auf der nächsten freien Doppelseite fortgesetzt. Diese Fortsetzung kann dann auf der jeweils abgeschlossenen Seite vermerkt werden.

18. Frage: In der VSA 2006 war in § 15 Absatz 5 VSA das Vier-Augen-Prinzip bei der Vervielfältigung von VS gefordert. In der VSA 2018 besteht diese Forderung für die Vervielfältigung (s. § 22) nicht mehr. Ist durch die VSA 2018 das Vier-Augen-Prinzip für die Vervielfältigung von VS aufgehoben worden?

Antwort: Eine Aufhebung des Vier-Augen-Prinzips war nicht beabsichtigt. Es handelt sich hierbei um ein Redaktionsversehen, welches im Zuge einer künftigen Überarbeitung der VSA korrigiert werden wird.

19. Frage: Gemäß § 20 Absatz 3 VSA kann der Herausgeber weitere Vorgaben zum Schutz und zur Handhabung von VS durch Warn- und Sperrvermerke nach Anlage IV (Ziffer 1.3.1 und 1.3.2) festlegen.

a) Können zur einheitlichen Anwendung der Warn- und Sperrvermerke Muster in Anlage VIII zur VSA ergänzt werden?

Antwort: Nein, da dies entweder eine Anpassung der Dokumentenvorlagen oder die Schaffung einer Möglichkeit zur nachträglichen Kennzeichnung (z. B. Stempel) voraussetzt. Diese sollte beim jeweiligen Bedarfsträger erfolgen.

b) Wie sind Warn- und Sperrvermerke zu „verorten“?

Warn- und Sperrvermerke sind immer unmittelbar unterhalb des Geheimhaltungsgrades anzubringen.

c) Gemäß Ziffern 1.3.1 und 1.3.2 der Anlage IV zur VSA „können insbesondere“ die dort aufgeführten Warn- und Sperrvermerke verwendet werden. Können weitere Warn- und Sperrvermerke verwendet werden?

Die Verwendung von Warn- und Sperrvermerken ist nur dann sinnvoll, wenn diese allgemein bekannt sind. Sie können daher nur Anspruch auf Beachtung

erheben, wenn sie auf Veranlassung der für die Herausgabe der VSA zuständigen obersten Bundesbehörde erstellt und in die Liste der zugelassenen Warn- und Sperrvermerke eingefügt wurden. Eine Verwendung anderer als der in Anlage IV genannten Warn- und Sperrvermerke kann daher nur im Einvernehmen mit dem BMI erfolgen.

20. **Frage:** **Gemäß § 21 Absatz 6 VSA ist beim Wechsel eines VS-Registrators der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen. Im VS-Übergabeprotokoll (s. Anlage VIII zur VSA, Muster 20) ist vermerkt, dass der Verbleib der VS und ihrer Anlagen stichprobenartig, und zwar nach folgenden Eintragungen im VS-Bestandsverzeichnis verfolgt und festgestellt wurde. Ist der komplette Bestand zu überprüfen oder reicht eine stichprobenartige Kontrolle aus?**

Antwort: Gemäß § 21 Absatz 6 VSA ist beim Wechsel eines VS-Registrators der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen. Weiteres führt § 21 VSA nicht aus. Das VS-Übergabeprotokoll sieht eine stichprobenartige Überprüfung vor. In der Praxis werden sich Art und Umfang der Überprüfung am VS-Aufkommen innerhalb der jeweiligen VS-Registatur orientieren müssen. Wird nur eine kleine Anzahl von VS verwaltet, dürfte eine Überprüfung des Komplettbestands unproblematisch durchzuführen sein. Bei einem hohen VS-Aufkommen hingegen wird man sich auf eine stichprobenartige Prüfung beschränken müssen, die u. a. dem Geheimhaltungsgrad der VS, dem Aufkommen an VS eines Geheimhaltungsgrades u. ä. Rechnung tragen sollte.

21. **Frage:** **Nach Ziffer 3 der Anlage I zur VSA wird u. a. die jährliche Durchführung von Bestandsprüfungen und schriftliche Berichterstattung an die Geheimschutzbeauftragten als Aufgabe der VS-Registatur dargestellt. Darüber hinaus wird für die vorgenannten Tätigkeiten auf die Muster in Anlage VIII verwiesen.**

a) **Ist der gesamte Bestand der VS jährlich zu prüfen oder kann ggf. die jährliche Prüfung auch stichprobenartig erfolgen und ist der Bestand auf Dokumentenebene oder auf Vorgangsebene zu prüfen?**

b) **Werden entsprechende Muster für die Bestandsprüfung analog des VS-Übergabeprotokolls und zur Berichterstattung durch das BMI zur Verfügung gestellt?**

Antwort: Zu a) In der Praxis wird sich der Maßstab für Art und Umfang der jährlichen Bestandsprüfung am VS-Bestand innerhalb der jeweiligen VS-Registatur orientieren müssen. Wird nur ein geringer Bestand verwaltet, dürfte eine komplette Bestandsprüfung unproblematisch sein. Bei einem hohen Bestand wird nur eine stichprobenartige Bestandsprüfung praktikabel sein. Die Bestandsprüfung sollte sich darüber hinaus insbesondere auf die VS beziehen, deren Rückgabe an die VS-Registatur über einen längeren Zeitraum nicht erfolgt ist.

Zu b) Eine Ergänzung der Anlage VIII zur VSA um verbindliche Muster für die Bestandsprüfung und die Berichterstattung ist nicht vorgesehen.

22. Frage: Der in § 23 Absatz 2 VSA verwendete Begriff „VS-Arbeitsbereich“ bedarf der Erläuterung. Handelt es sich um jeden Arbeitsplatz, an dem eine ermächtigte Person sitzt oder einen solchen, an dem aufgabenspezifisch häufig VS bearbeitet werden?

Antwort: VS-Arbeitsbereiche sind VS-IT-Räume und alle anderen Räume, in denen VS-VERTRAULICH oder höher eingestufte VS gehandhabt werden (vgl. § 39 Absatz 1 VSA).

23. Frage: Die Geheimschutzbeauftragten können gemäß § 24 Absatz 5 VSA besondere Regelungen zur Weitergabe von VS innerhalb einer Gemeinschaft von Geheimnisträgern festlegen. Was ist unter einer Gemeinschaft von Geheimnisträgern zu verstehen?

Antwort: Gemäß § 3 Absatz 1 VSA dürfen nur Personen Kenntnis von einer VS erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Es gilt der Grundsatz „Kenntnis nur, wenn nötig“. Unter einer Gemeinschaft von Geheimnisträgern ist eine Anzahl von Personen innerhalb einer festgelegten Organisationsstruktur (z. B. Referat, Arbeits-/Projektgruppe o. ä.) zu verstehen, die auf Grund ihrer Aufgabenerfüllung die gleiche Kenntnis von VS haben müssen. Die Geheimschutzbeauftragten können hier zur Weitergabe besondere Regelungen wie z. B. Verzicht auf die Quittierung der Weitergabe bei Weitergabe untereinander aufgrund eines hohen VS-Aufkommens und damit verbundener unvermeidbarer Zeitverzögerungen festlegen. Hierbei ist sicherzustellen, dass der aktuelle Verbleib einer VS jederzeit feststellbar ist.

24. Frage: Nach Ziffer 7 der Anlage V zur VSA können VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH außerhalb des Dienstgebäudes oder einer Liegenschaft nur auf Dienstreisen und zu Dienstbesprechungen in einem verschlossenen Umschlag unversiegelt und ohne Kurierausweis mitgeführt werden. Ist bei der Mitnahme von VS des Geheimhaltungsgrades VS-VERTRAULICH oder höher ein Kurierausweis nötig?

Antwort: Ein Kurierausweis wird ggf. für die Mitnahme von VS-VERTRAULICH oder höher eingestuftes VS nach außerhalb des Bundesgebiets benötigt (vgl. § 28 Absatz 5 VSA). Der nach den Bestimmungen des Wiener Übereinkommens (s. BGBl. 1964 II. Seite 957) für Kuriere und Kuriergepäck vorgesehene Schutz gilt nur für diplomatische Kuriere und diplomatisches Kuriergepäck im Verkehr zwischen dem Entsendestaat und den fremden Missionen im Empfangsstaat sowie zwischen den fremden Missionen untereinander. Gemäß Artikel 27 Absatz 1 des Übereinkommens schützt der Empfangsstaat nur den freien Verkehr der Mission für alle amtlichen Zwecke. Kuriere, die amtliches Gepäck an einen anderen Ort im Ausland befördern als den Sitz der deutschen Auslandsvertretung (z. B. anlässlich von Tagungen oder Besprechungen) genießen keinen nach dem Wiener Übereinkommen gesicherten völkerrechtlichen Schutz. Jedoch lässt sich für amtliche Kuriere, die zu einem Konferenzort außerhalb des Sitzes der deutschen Auslandsvertretungen entsandt werden, aus den allgemeinen Regeln des Völkerrechts ein besonderer Rechtsstatus mit einem Mindestmaß an Schutzrechten herleiten. Nähere Auskunft erteilt bei Bedarf das Auswärtige Amt.

25. **Frage:** Was muss eine Zusicherung eines Landes gemäß § 26 Absatz 2 VSA enthalten, um die Geheimschutzanforderungen des Bundes zu erfüllen?

Antwort: Eine bestätigende Zusicherung eines Landes über die Erfüllung der Geheimschutzanforderungen ist formlos möglich, etwa durch eine Mail an die für den Betrieb verantwortliche Dienststelle ist ausreichend. Ebenfalls ist eine Zusicherung analog zum Memorandum of Understanding möglich (s. Muster 23, Anlage VIII zur VSA).
Auch zur besseren Nachweisbarkeit wäre es für eine solche Zusicherung sinnvoll, wenn die jeweiligen für den Betrieb verantwortlichen Dienststellen Formblätter für die Erklärung zur Verfügung stellen, die zugleich als Belehrung über die Geheimschutzanforderungen dienen.

26. **Frage:** Sind die Verschlusssachenanweisungen der Länder als gleichwertig zum Schutz von Verschlusssachen zu betrachten?

Antwort: BMI als Nationale Sicherheitsbehörde für den Geheimschutz bestätigt mit Stand 01.01.2023, dass gemäß den Verschlusssachenanweisungen der 16 Länder in allen 16 Ländern der VSA des Bundes entsprechende Regelungen zum Schutz von Verschlusssachen gelten.

27. **Frage:** Die Regelung des § 26 Absatz 2 bezieht sich dem Wortlaut nach nur auf VS-IT-Systeme. Fallen auch VS-IT-Verbünde darunter?

Antwort: Ja. VS-IT-System ist der Oberbegriff. Auch ein VS-IT-Verbund ist ein VS-IT-System – nämlich eines, an dem mehrere Dienststellen des Bundes beteiligt sind (vgl. § 50 Absatz 5).

28. **Frage:** Sind Prüfungen zur Einhaltung der zugesicherten Anforderungen des Geheimschutzes durch die für den Betrieb verantwortliche Dienststelle des Bundes durchzuführen (s. § 26 Absatz 2 VSA)?

Antwort: Eine Überprüfung der Einhaltung der zugesicherten Anforderungen des Geheimschutzes ist grundsätzlich nicht gefordert. Sofern im Rahmen des Betriebs von der verantwortlichen Dienststelle des Bundes Abweichungen von der Zusicherung bekannt werden, veranlasst die verantwortliche Dienststelle entsprechende Maßnahmen.

29. **Frage:** Sind ebenfalls Regelungen für Kommunen erforderlich?

Antwort: Kommunen sind staatsorganisatorisch Teile der Länder und somit ist das Rechtsverhältnis mittelbar über die VSA'en der Länder geregelt.

D. Zusammenarbeit mit nichtdeutschen Stellen

30. **Frage:** Welche Auswirkungen hat die Anpassung der VSA 2023 auf den Sicherheitsakkreditierungsprozess von VS über- und zwischenstaatlicher Organisationen?

Antwort: Die Sicherheitsakkreditierung ist eine Anforderung des Geheimschutzes für eine Freigabe von VS-IT gemäß § 50 Absatz 3 Satz 1 Nr. 9 VSA. Das BMI ist als Nationale Sicherheitsbehörde für den Geheimschutz im Sinne der nationalen Zuständigkeit Sicherheitsakkreditierungsstelle (SAA) für IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen (s. § 36 Absatz 2 VSA).

31. Frage: Gibt es das Muster 23 der Anlage VIII zur VSA auch in englischer Sprache?

Antwort: Eine englischsprachige Version der VSA liegt im BMI vor. Die Anlagen zur VSA sind teilweise übersetzt.

E. Materielle und technische Maßnahmen

32. Frage: Ist bei VS des Geheimhaltungsgrades STRENG GEHEIM auch bei geringem Umfang aufgrund der Bedeutung ein Sicherheitsbereich gerechtfertigt (§ 39 Absatz 3 VSA)?

Antwort: Gemäß § 39 Absatz 3 VSA sind in einer Dienststelle oder in einem Teil von ihr von der jeweils zuständigen obersten Bundesbehörde im Einvernehmen mit dem BMI zu bilden, sofern Umfang und Bedeutung der dort anfallenden VS es erfordern. In der Regel ist die Aufbewahrung und Sicherung von VS gemäß § 23 VSA ausreichend. Die Bildung von Sicherheitsbereichen wird erforderlich, wenn aufgrund der hohen Konzentration von VS dem Risiko der unbefugten Kenntnisnahme durch zusätzliche Maßnahmen begegnet werden soll. Hierbei sind die in dem entsprechenden Bereich vorhandenen VS des Geheimhaltungsgrades VS-VERTRAULICH oder höher in ihrer Gesamtheit zu betrachten.

33. Frage: Die Regelungen zu „Besonderen Dienststellen“ (§ 42 VSA) sind im Abschnitt VII enthalten. Die rechtlichen Vorgaben zu materiellen und technischen Maßnahmen enthalten keine Vorgaben zu VS-IT. Beziehen sich die umfassenden Beratungen und Prüfungen nach § 42 Absatz 2 Satz 2 VSA nur auf die materiellen und technischen Maßnahmen und nicht auf VS-IT-Maßnahmen?

Antwort: Die Beratungen und Prüfungen nach § 42 Absatz 2 Satz 2 VSA beziehen sich - im Rahmen der Zuständigkeit des BSI - auch auf den Einsatz von VS-IT.

34. Frage: Nach § 44 Absatz 4 VSA sind unberechtigte Zugangsversuche zu VS-Verwahrgelesen, soweit technisch möglich, zu protokollieren. Bedeutet dies, dass bisherige VS-Verwahrgelese (z. B. VS-Stahlschränke), sofern dies technisch möglich ist, auf elektronische Zahlenkombinationsschlösser umgerüstet werden müssen, oder sind künftig alle VS-Verwahrgelese (z. B. besonders gesicherte Räume, Schränke oder sonstige Behältnisse) mit elektronischen Zahlenkombinationsschlössern auszustatten?

Antwort: Vorhandene Verwahrgelese können weiter genutzt werden. Die Umsetzung von § 44 Absatz 4 VSA sollte unter Wirtschaftlichkeitsgesichtspunkten im Zuge von Neu-/ Ersatzbeschaffungen, notwendigen Instandsetzungen o. ä. umgesetzt werden.

35. **Frage:** Nach § 47 Absatz 1 VSA weisen die Dienststellen die ordnungsgemäße Funktion und Ausführung von technischen Mitteln und die Einhaltung der Anforderungen durch Abnahmeprüfungen des BSI nach. Sind sämtliche nach § 40 Absatz 1 VSA aufgeführten technischen Mittel Gegenstand bei den Abnahmeprüfungen vor Ort?

Antwort: Grundsätzlich werden die technischen Mittel nach § 40 Absatz 1 VSA durch eine entsprechende Eignungsfeststellung nach § 40 Absatz 2 VSA zum Schutz von VS geprüft. Eine nochmalige Prüfung dieser technischen Mittel vor Ort ist dementsprechend nicht erforderlich. Vor Ort erfolgt die Funktionsprüfung für Einbruch- und Überfallmeldeanlagen sowie Zutrittskontrollanlagen.

36. **Frage:** Jede Vervielfältigung von VS-VERTRAULICH oder höher eingestuften VS ist mit einer fortlaufenden Nummer und dem jeweiligen Empfänger so zu kennzeichnen, dass sie als weiteres Exemplar einer VS (Kopie) eindeutig erkennbar ist und der Original-VS zugeordnet werden kann sowie nach § 21 VSA unverzüglich zu registrieren. Wie erfolgt die Kennzeichnung von elektronischen Vervielfältigungen? Soll die fortlaufende Nummer z. B. bei einem Fax auf einem Vorblatt notiert werden?

Antwort: Sofern in einem elektronischen VS-Bearbeitungssystem elektronische Vervielfältigungen gefertigt werden sollen, ist eine VSA-konforme Handhabung innerhalb des Systems durch die Implementierung geeigneter Funktionalitäten sicherzustellen.

Bei einem Fax erfolgt die Kennzeichnung einer Vervielfältigung wie bei jeder anderen VS.

F. Einsatz von Informationstechnik

I. Freigabeprozess

37. **Frage:** Was ist unter VS-IT zu verstehen? Was ist ein VS-IT-System? Was ist ein VS-IT-Verbund?

Antwort: VS-IT ist nach der Legaldefinition des § 9 VSA „Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung“. Kommunikationssysteme sind darin eingeschlossen. In die zugehörige Betrachtung sind sämtliche für den Betrieb benötigten technischen, infrastrukturellen, personellen und organisatorischen Komponenten einzubeziehen.

Wenn VS-IT nur durch eine einzelne Dienststelle betrieben und genutzt wird, handelt es sich um ein **VS-IT-System**.

Wenn ein VS-IT-System nicht nur durch eine einzelne Dienststelle betrieben und genutzt wird, sondern mehrere Dienststellen des Bundes (am Betrieb und/oder der Nutzung) beteiligt sind, handelt es sich um einen **VS-IT-Verbund** nach § 50 Absatz 5 Satz 1 VSA. (Das bedeutet im Umkehrschluss, dass auch ein VS-IT-Verbund ein VS-IT-System ist.)

Abgrenzung zum Begriff „Verbund“ in der **ISR IKTB**: Es kann sehr viele einzelne VS-IT-Verbünde im Sinne der § 50 VSA geben (jedes VS-IT-System an

dem mehr als eine Dienststelle beteiligt ist, z.B. VS-IT-Verbund eAkte, VS-IT-Verbund PVS+, VS-IT-Verbund Fachverfahren X der Behörde Y auf BP Bund im ITZBund). In der ISR ITKB ist jedoch mit „Verbund“ der Gesamtverbund der ITKB gemeint, d.h. alle im Geltungsbereich der ISR ITKB enthaltenen Betriebsplattformen, Dienste, Netze und IT-Lösungen (unabhängig davon, ob sie VS-eingestuft sind oder nicht, Gesamt-Verbund ITKB).

- 38. Frage:** Was passiert mit bereits beantragten, aber vom BSI noch nicht erteilten Freigabevoten für VS-IT, die für VS-VERTRAULICH oder höher eingestufte Verschlussachen eingesetzt werden soll, im Zuge der Neufassung? Bleiben diese Anfragen beim BSI anhängig?

Antwort: Mit Inkrafttreten der VSA ist gemäß § 50 Absatz 4 Satz 3 VSA weiterhin ein Freigabevotum des BSI Voraussetzung für eine Freigabe. Die bereits beantragten Freigabeprüfungen werden unter Maßgabe der neuen VSA weiterverfolgt.

- 39. Frage:** Gibt es eine Übergangsregelung für 2023 bereits laufende VS-NfD-Freigabeprüfungen mit Freigabevotum durch das BSI?

Antwort: Eine Übergangsregelung gilt nur für die zum 01.04.2023 laufenden Einzelfreigabeprüfungen im Rahmen der dritten Gesamtfreigabe der E-Akte Bund. In diesen Fällen erstellt das BSI noch ein Freigabevotum auch für VS-NfD-IT. Für die übrigen Freigabeprüfungen gilt die VSA 2023.

- 40. Frage:** Welche Vorgaben sind dem BSI nach § 50 Absatz 2 Satz 2 VSA nachzuweisen?

Antwort: Die Vorgaben werden derzeit noch abgestimmt.

- 41. Frage:** Wer erbringt den geforderten Nachweis nach § 50 Absatz 2 VSA (Informationssicherheitsbeauftragte oder Geheimschutzbeauftragte)?

Antwort: Für den Nachweis der Einhaltung der Informationssicherheit sind die Informationssicherheitsbeauftragten zuständig (s. UP Bund 2017). Sie erbringen diesen Nachweis nach den Vorgaben des BSI.

Der Nachweis ist der Dienststellenleitung bzw. dem von ihr beauftragten Geheimschutzbeauftragten vor der Freigabe von VS-IT vorzulegen (s. § 50 Absatz 4).

- 42. Frage:** Was sind die Standards zur Informationssicherheit des BSI nach § 50 Absatz 2 VSA?

Antwort: Dies sind aktuell die BSI Standards 200-x und die einschlägigen Mindeststandards nach § 8 BSIG. Für den Geltungsbereich des UP Bund 2017 wird bei Anwendung des IT-Grundschutzes die darin beschriebene Standard-Absicherung als Mindestanforderung festgelegt.

43. Frage: Sind die in § 50 Absatz 3 VSA aufgeführten Anforderungen des Geheimschutzes abschließend?

Antwort: Nein; § 50 Absatz 3 VSA enthält die wesentlichen Anforderungen des Geheimschutzes gemäß VSA. Weitere Anforderungen sind etwa in den §§51 und 52 zum Einsatz von IT-Sicherheitsprodukten enthalten. Im Einzelfall können die Geheimschutzbeauftragten zudem weitere Anforderungen vorsehen.

44. Frage: Wie konkret haben die Geheimschutzbeauftragten die Umsetzung der Anforderungen des Geheimschutzes nachzuweisen und zu dokumentieren?

Antwort: Der Nachweis, ob und wie die Maßnahmen des Geheimschutzes umgesetzt sind, muss für einen sachverständigen Dritten nachvollziehbar sein. Hierzu sind u. a. Angaben zur Prüfungsdurchführung und zur prüfenden Stelle, sowie Angaben zum Prüfergebnis und zu aufgedeckten Sicherheitsmängeln erforderlich. Zur Unterstützung ist geplant eine Handreichung zur Überprüfung der wirksamen Umsetzung durch das BSI im Laufe des zweiten Halbjahres 2023 bereitzustellen.

45. Frage: Bei den Ausführungen zu § 50 Absatz 3 Satz 3 VSA wurde die Formulierung "bestimmte Softwareanwendungen" erwähnt. Welche sind damit gemeint?

Antwort: Eine technische Unterstützung zur Erstellung, Verwaltung und Fortschreibung von Informationssicherheitskonzepten nach den Standards zur Informationssicherheit des BSI ist durch sogenannte IT-Grundschatz-Tools möglich (s. <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/IT-Grundschatz-Kompendium/Alternative-IT-Grundschatztools/IT-Grundschatztools.html>). Im Rahmen der IT-Konsolidierung Bund ist eine Nutzung des Dienstes „Zentraler Dienst für Informationssicherheit (ZeDIS)“ (<https://www.itzbund.de/DE/itloesungen/standardloesungen/zedis/zedis.html>) für die Bundesverwaltung vorgesehen.

46. Frage: Wer gibt nach § 50 Absatz 4 VSA frei (Geheimschutzbeauftragte oder Dienststellenleitung)?

Antwort: Grundsätzlich gibt nach § 50 Absatz 4 VSA die Dienststellenleitung die VS-IT frei. Die Dienststellenleitung kann diese Aufgabe auf die Geheimschutzbeauftragte oder den Geheimschutzbeauftragten delegieren.

Vor dem Hintergrund der Verantwortlichkeiten (s. § 7 Satz 1 VSA) sollten die Geheimschutzbeauftragten sich die Freigabe der VS-IT von der Dienststellenleitung billigen lassen bzw. die Dienststellenleitung in geeigneter Weise über die Freigabe und insbesondere die damit verbundenen Risiken unterrichten.

47. Frage: Gibt es besondere Anforderungen an die Dokumentation der Freigabe durch die Dienststellenleitung?

Antwort: Es gibt keine besonderen Anforderungen an die Dokumentation der Freigabe (s. Ziffer 2.2, Anlage II zur VSA).

48. Frage: Ist bei Vorlage einer ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes keine separate Überprüfung mehr notwendig?

Antwort: Dies gilt nur für Freigaben für den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH, sofern der Geheimschutzbaustein des IT-Grundschutzes (CON.11.1) mit überprüft wurde. Dann ist keine weitere Prüfung erforderlich. Damit gelten die Einhaltung der Standards zur Informationssicherheit des BSI und die Anforderungen des Geheimschutzes als erfüllt.

49. Frage: Ist die ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes eine notwendige Voraussetzung?

Antwort: Die ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes inklusive der im Geheimschutzbaustein aufgeführten Anforderungen ist optional und keine Verpflichtung.

50. Frage: Wie soll der Informationsverbund abgegrenzt werden für eine mögliche ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes?

Antwort: Für eine mögliche ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes muss der zu prüfende Informationsverbund (Geltungsbereich) die vollständige VS-IT umfassen. Insbesondere ist darauf zu achten, dass die für die VS-IT relevanten zusätzlichen Rahmenbedingungen berücksichtigt werden (z. B. Umgang mit Dienstleistern, Schnittstellen zu anderen Informationsverbänden, Einschränkungen in der Risikoakzeptanz). Grundsätzlich grenzt sich die VS-IT insbesondere mittels IT-Sicherheitsprodukten mit Zulassungsaussage (Zulassung oder Einsatzerlaubnis) zu anderen Informationsverbänden ab.

51. Frage: Wenn eine Behörde auf mehrere Standorte verteilt ist, fällt sie bzw. ihre VS-IT dann unter die Voraussetzungen des § 50 Absatz 5 VSA?

Antwort: Da es sich nur um eine Dienststelle an mehreren Standorten handelt, wird dies nicht als VS-IT-Verbund gesehen.

52. Frage: Wer ist Betreiber nach § 50 Absatz 5 VSA? Wer ist für die Gesamtfreigabe verantwortlich, wenn es mehrere Betreiber gibt?

Antwort Nach § 50 Absatz 5 Satz 2 VSA obliegt die Gesamtfreigabe des Betriebs für den VS-IT-Verbund der verantwortlichen Dienststelle (Betreiber). Betreiber sind Dienststellen, die für die beteiligten Dienststellen zentrale IT-Dienstleistungen zur Verfügung stellen. Falls es mehrere Teil-Betreiber gibt und daher Zweifel bestehen, wer der für die Gesamtfreigabe verantwortliche (Gesamt-)Betreiber ist, „bestimmt bei ressortinternen VS-IT-Verbänden die zuständige oberste Bundesbehörde und bei ressortübergreifenden VS-IT-Verbänden das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz den Betreiber des VS-IT-Verbundes. (§ 50 Absatz 5)“ Falls ein Teil-Betreiber allen anderen Teil-Betreibern als Dienstleister eine IT-Leistung anbietet und dafür zentrale Nutzungsbedingungen erstellt, ist dieser Teil-Betreiber als (Gesamt-)Betreiber für die Gesamtfreigabe verantwortlich.

53. Frage: Ist die Annahme richtig, dass für Dienste der IT-Konsolidierung in der Regel das ITZBund als Betreiber auftreten wird? Beispielsweise für die E-Akte Bund?

Antwort: Bei Diensten im Rahmen der Dienstekonsolidierung ist das ITZBund i. d. R. Betreiber i. S. d. VSA. Der Betreiber ist u. a. verantwortlich für die Erstellung von Nutzungsbedingungen und ggf. Festlegung von Auflagen für die beteiligten Dienststellen.

54. Frage: Was gilt für den Zeitraum, bis die Arbeitshilfen (Handreichungen, Technische Leitlinien, Umsetzungshinweise, IT-Grundschutzbausteine etc.) zur Verfügung stehen?

Antwort: Die Arbeitshilfen des BSI sollen die Umsetzung und Anwendung der VSA erleichtern. Grundsätzlich ergeben sich alle Anforderungen des Geheimschutzes aus der VSA.

55. Frage: Können bzw. müssen Dienststellen mit besonderem Geheimschutzbedarf nach § 42 VSA (weiterhin) im Vorfeld von VS-NfD-Freigaben nach § 50 VSA das BSI im Vorfeld um Beratung/Unterstützung bitten?

Antwort: Besondere Dienststellen nach § 42 VSA müssen im Vorfeld von VS-NfD-Freigaben nicht um Beratung/Unterstützung bitten. Diese Dienststellen können wie die übrigen Dienststellen im Prozess der VS-IT-Freigabe einschließlich der Erfüllung seiner Vorgaben durch das BSI auf Antrag beraten und unterstützt werden.

Nach § 42 Absatz 2 VSA sind die besonderen Dienststellen allerdings verpflichtet, mindestens alle vier Jahre umfassende Beratungen und Prüfungen durch das BSI in Anspruch zu nehmen.

56. Frage: In welchen regelmäßigen Abständen hat eine Wiederholung der Überprüfung der Umsetzung der Anforderungen des Geheimschutzes zu erfolgen (s. § 50 Absatz 8 VSA)?

Antwort: Grundsätzlich liegt eine Wiederholung der Überprüfung der Umsetzung der Anforderungen des Geheimschutzes in der Verantwortung der Geheimschutzbeauftragten. In der Regel sollte alle drei Jahre eine Wiederholung der Überprüfung der Umsetzung der Anforderungen des Geheimschutzes stattfinden, sofern vorher keine anlassbezogene Prüfung erfolgt ist. Dies hat sich auch in anderen Prüfschemata bewährt und ist mit vertretbarem Aufwand zu bewältigen.

57. Frage: Durch wen ist die Freigabe nach § 50 Absatz 8 Satz 3 VSA zu widerrufen?

Antwort: Erfolgte die Freigabe nach § 50 Absatz 4 VSA ist die Freigabe durch die Dienststellenleitung zu widerrufen (s. Antwort zur Freigabe nach § 50 Absatz 4 VSA). Bei einer Gesamtfreigabe nach § 50 Absatz 5 VSA erfolgt der Widerruf der Gesamtfreigabe durch die für den Betrieb verantwortliche Dienststelle

(Betreiber). Wird ein VS-IT-System im Auftrag des Bundes privatrechtlich betrieben (s. § 50 Absatz 6 VSA), widerruft die jeweilige zuständige oberste Bundesbehörde die Freigabe.

58. Frage: Wann besteht ein berechtigtes Verlangen für eine Auskunft für freigegebene VS-IT bzw. freigegebene VS-IT-Verbünde?

Antwort: Der Antragsteller hat sein Verlangen in der Weise darzulegen, dass ein sachlich begründbares Interesse an der Auskunft besteht. Das BSI kann im Zweifel den Antragsteller auffordern, das berechnigte Verlangen nachzuweisen. Das BSI gewährt Auskünfte nur, sofern dadurch keine nachteiligen Auswirkungen auf Belange des Geheimschutzes zu befürchten sind.

59. Frage: Welche Verantwortung trägt ein Gesamtbetreiber, wenn er eine Gesamtfreigabe für einen VS-IT-Verbund erteilt?

Antwort: Die Gesamtfreigabe eines VS-IT-Verbundes ist jetzt in § 50 Absatz 5 VSA geregelt. Die Gesamtfreigabe obliegt dem Betreiber des VS-IT-Verbundes. Er „ist für die Koordinierung der Erfüllung der in § 50 Absatz 4 VSA genannten Voraussetzungen zuständig.“ Dies bedeutet, der Betreiber des IT-Verbundes muss von jeder beteiligten Dienststelle eine Bestätigung der jeweiligen Einzelfreigabe (bzgl. des eigenen Zuständigkeitsbereich dieser Dienststelle) einholen und die Nachvollziehbarkeit der Einzelfreigaben prüfen. Jede beteiligte Dienststelle ist für ihren eigenen Zuständigkeitsbereich (und die dafür erteilte Einzelfreigabe) verantwortlich. Auf Basis dieser Einzelfreigaben spricht der Gesamtbetreiber die Gesamtfreigabe aus.

Das bedeutet im Einzelnen:

Der Betreiber von VS-IT-Verbänden

- erteilt die Gesamtfreigabe (bei VS-NfD ohne, ab VS-VERTRAULICH mit BSI-Votum)
- führt von den Teilnehmerbehörden zusammen:
- Nachweise der Einhaltung der geltenden BSI-Standards zur Informationssicherheit
- Ergebnis der Wirksamkeitsprüfung der GSB hinsichtlich der Geheimschutzanforderungen
- prüft die Plausibilität dieser Dokumente
- entscheidet über den Teilnehmerkreis
- legt Nutzerpflichten und ggf. Auflagen für die Teilnehmerbehörden fest.

Im Falle etwa der BP Bund bedeutet dies: Eine Kundenbehörde, die ihre eigene VS-IT-Anwendung auf der BP Bund selbst betreibt, bleibt für die VS-Freigabe dieser nach § 50 verantwortlich. Allerdings obliegt es dem ITZBund sicherzustellen, dass alle relevanten Freigaben im VS-IT-Verbund zeitgerecht vorliegen. Somit agiert das ITZBund als Gesamt-Betreiber des VS-IT-Verbundes.

60. Frage: Ist die Liste der Mitteilungen nach § 50 Absatz 10 VSA eingestuft und wenn ja, wie hoch?

Antwort: Die Liste der Mitteilungen nach § 50 Absatz 10 VSA ist als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

61. Frage: Gibt es eine vergleichbare Liste auch für die Länder?

Antwort: Für die Länder gibt es keine vergleichbare Liste, da eine Zusicherung durch das Land erfolgt (s. § 26 Absatz 2 VSA).

62. Frage: Welche TL ist in § 50 Absatz 11 VSA gemeint?

Antwort: Hierunter fallen z. B. Technische Leitlinien zur Absicherung von VS-IT für verschiedene Geheimhaltungsgrade. Weitere Technische Leitlinien können erstellt werden.

II. Zulassung

63. Frage: Wo kann ich die Übersicht finden, welche IT-Sicherheitsprodukte oder -komponenten über eine Zulassung verfügen müssen?

Antwort: Der vom BSI herausgegebene Katalog von Produktklassen und -typen enthält eine aktuelle und strukturierte Auflistung aller Produkttypen, die nach Maßgabe des BSI einer Zulassung oder Einsatzerlaubnis bedürfen.
(https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Katalog-der-Produktklassen-und--typen/katalog-der-produktklassen-und--typen_node.html)

Die IT-Sicherheitsprodukte sind einschließlich der zugehörigen Einsatz- und Betriebsbedingungen in der BSI-Schrift 7164 gelistet. (Fehler! Linkreferenz ungültig.).

64. Frage: Worin unterscheiden sich Zulassung von VS-IT und Zertifizierung nach § 9 BSIG??

Antwort: Die Zulassung bezieht sich nur auf IT-Sicherheitsprodukte für die Verarbeitung und Übertragung von staatlichen VS und berücksichtigt insbesondere Belange des staatlichen Geheimschutzes. Eine Zulassung wird nur durch das BSI ausgesprochen. Der Antrag auf Zulassung eines IT-Sicherheitsproduktes kann grundsätzlich nur von einem bundesbehördlichen Anwender (Bedarfsträger) gestellt werden.

Demgegenüber kann eine Zertifizierung des BSI (CC, ITSEC) für alle IT-Produkte mit Sicherheitsfunktionalität angestrengt werden, sofern sich der Hersteller entschließt, eine neutrale Prüfung durchführen zu lassen. Diese Evaluierung kann auch bei externen Prüfstellen erfolgen. Eine Zertifizierung bedeutet jedoch nicht, dass mit dem Produkt auch staatliche Verschlusssachen verarbeitet werden dürfen.

65. Frage: Welche Änderungen haben sich in den Regelungen der VSA 2023 zur Zulassung ergeben?

Antwort: Folgende Änderungen haben sich zur Zulassung ergeben:

- a) Der bisherige Begriff „Freigabeempfehlung“ wurde durch den neuen Begriff „Einsatzlaubnis“ ersetzt, um einer Verwechslung mit dem Freigabevo-tum nach § 50 VSA vorzubeugen.
- b) Gemäß § 51 Absatz 1 VSA legt das BSI fest, welche IT-Sicherheitsprodukte oder –komponenten über eine Zulassung verfügen müssen. Damit soll eine flexiblere Handhabung im Rahmen der Zulassung ermöglicht werden.
- c) Der Katalog der Produktklassen und –typen definiert insbesondere, ob eine Zulassungsaussage für einen Produkttyp erforderlich ist und welche Sicher-heitsfunktionen in einem Zulassungsverfahren für einzelne Produkttypen gelten (s. § 52 Absatz 2 VSA). Die Festlegung der Zulassungsrelevanz er-folgt unter Berücksichtigung des Geheimhaltungsgrades.

G. Kryptopersonal und Handhabung von Kryptomitteln

66. Frage: Wer belehrt die Kryptoverwalter?

Antwort: Die Geheimschutzbeauftragten oder besonders beauftragte Mitarbeiter beleh-ren die Kryptoverwalter.

67. Frage: Ist das Kryptofax (z. B. ElcroDat 6-2) auch ein Kryptomittel im Sinne von § 59 VSA?

Antwort: Ja, weil es nach der Definition von § 59 Absatz 1 VSA vom BSI als Kryptomittel zur Verschlüsselung und Übertragung von Informationen festgelegt wurde.

H. Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH

68. **Frage:** Ist aus den Vorgaben der Anlage V zur VSA zu schließen, dass eine (zugelassene) Kryptierung für Speichermedien/Datenträger auf mobiler IT bei Mitnahme nicht mehr gefordert ist?

Antwort: Gemäß Ziffer 1.4 Anlage V zur VSA ist die Verarbeitung von Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH nur mit VS-IT zulässig, die hierfür freigegeben ist. Die betrifft u. a. PC, Notebooks und Mobiltelefone. Während die Ziffer 1.4 der Anlage 7 zur VSA 2006 auf eine Verschlüsselung der in tragbaren IT-Systemen verwendeten Speichermedien durch vom BSI zugelassene Produkte abstellte, wird seit der VSA 2018 auf freigegebene VS-IT abgestellt. Der vorgenannte Rückschluss trifft daher nicht zu.

69. **Frage:** Müssen verschlüsselte Datenträger/Laptops wie Verschlussachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH behandelt werden oder können diese im Hotelzimmer verbleiben?

Antwort: Grundsätzlich sind für verschlüsselte Laptops die Einsatz- und Betriebsbedingungen zu berücksichtigen. Im Umkehrschluss zu § 54 VSA bedürfen diese keines besonderen Schutzes.

70. **Frage:** Nach Ziffer 7 Anlage V zur VSA sind VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH auf Dienstreisen und zu Dienstbesprechungen angemessen gegen unbefugte Kenntnisnahme und unbefugten Zugriff zu sichern. Gemäß § 28 Absatz 6 VSA ist eine Aufbewahrung von VS u. a. in unbesetzten Fahrzeugen grundsätzlich unzulässig. Die Polizei führt im Einsatz VS des o. a. Geheimhaltungsgrades im Fahrzeug mit. Im Einsatz sind Fahrzeuge auch unbesetzt und die VS verbleiben im Fahrzeug, weil bei möglichem körperlichem Einsatz mitgenommene Unterlagen verloren oder entwendet werden könnten. Darüber hinaus werden in diesen Fahrzeugen verschlossene Boxen mit Maschinenpistolen mitgeführt. Besteht die Möglichkeit, VS des genannten Geheimhaltungsgrades in diesen verschlossenen Boxen mit aufzubewahren, um diese vor unbefugtem Zugriff bei unbesetzten Fahrzeugen zu schützen?

Antwort: Soweit die Mitführung von VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH im Einsatz nachweislich erforderlich ist, bestehen keine Bedenken, diese VS in den verschlossenen Boxen mit aufzubewahren.

71. **Frage:** Ab § 28 Absatz 2 VSA ist unklar, welche Regelung für welchen Geheimhaltungsgrad in den nachfolgenden Absätzen gilt (insbesondere § 28 Absatz 6 VSA)

Antwort: § 28 Absatz 2 VSA verweist für die Mitnahme von VS-NUR FÜR DEN DIENSTGEBRAUCH ausdrücklich auf Ziffer 7 der Anlage V.

In § 28 Absatz 3, Absatz 4 und Absatz 5 VSA sind die Geheimhaltungsgrade ausdrücklich genannt.

Da in § 28 Absatz 2 VSA ausdrücklich auf Ziffer 7 der Anlage V verwiesen wird, findet § 28 Absatz 6 auf VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH keine Anwendung.

- 72. Frage: Gelten die Vorschriften für den Austausch von VS mit ausländischen Staaten sowie über- oder zwischenstaatlichen Organisationen und nichtöffentlichen Stellen auch für VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH?**

Antwort: Ja.

- 73. Frage: Bei der Weitergabe von VS an nichtdeutsche Stellen (§ 34 Absatz 6 VSA) kann nicht nachvollzogen werden, wie dem BMI die Weitergabe im Fall von VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH gemeldet werden soll, da diese durch die Dienststelle nicht nachgewiesen werden muss. Ist die jährliche Mitteilung an das BMI auch für VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH zwingend erforderlich oder gibt es hierzu Ausnahmen?**

Antwort: Es gibt keine Ausnahme von der Verpflichtung, die Weitergabe von deutschen VS an nichtdeutsche Stellen in jedem Fall (also auch bei VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH) zu melden.

- 74. Frage: Besitzt die mit BMI-Erlass ÖS III 3-606520/1#1 vom 23.04.2013 übermittelte Anlage zum VS-NfD-Merkblatt (Vertragsbestandteil zwischen Auftraggeber) und Auftragnehmer bei Verträgen mit Unternehmen weiterhin Gültigkeit?**

Antwort: Gemäß Ziffer 6.6 Anlage V zur VSA muss vor der Weitergabe von VS des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH an nichtöffentliche Stellen mit diesen Stellen ein Vertrag geschlossen werden, in den die Bestimmungen des VS-NfD-Merkblatts für den Geheimschutz in der Wirtschaft Eingang gefunden haben. Zu beachten ist in diesem Zusammenhang daher nur das VS-NfD-Merkblatt aus dem Geheimschutzhandbuch für die Wirtschaft (GHB). Diese Anlage 4 des GHB wurde überarbeitet und wird zum 1.9.2023 in Kraft treten (vgl. auch Antwort zu Frage 75.).

- 75. Frage: Wann erfolgt eine Aktualisierung der Anlage 4 Geheimschutzhandbuch durch das BMWK und erfolgt diese Anpassung im Einvernehmen mit dem BMI? Eine schnelle Aktualisierung wird als notwendig wegen der Firmene Mitarbeiter angesehen.**

Antwort: vgl. Antwort zur Frage 74.: Anlage 4 des GHB wurde neu konzipiert und wird zum 1.9.2023 in Kraft treten. Dies erfolgt im Einvernehmen mit BMI. Die Herstellung des Einvernehmens dient der Sicherstellung eines vergleichbaren Schutzniveaus.

Die Anlage 4 und weitere Informationen sind im öffentlichen Bereich des bmwk-sicherheitsforums unter <https://bmwk-sicherheitsforum.de/handbuch/anlagen/> abrufbar.

I. Sonstige Fragen

76. **Frage:** **Frage: Gilt § 39 Absatz 6 VSA auch, wenn Mitarbeiter in einem Büro nur VS lesen und nicht bearbeiten?**

Antwort: Sinn der Vorschrift ist, die Kenntnisnahme der VS durch Unbefugte bzw. die unerlaubte Vervielfältigung (z. B. durch das Anfertigen von Bildaufzeichnungen), den unerlaubten Mitschnitt von entsprechenden Erörterungen u. ä. zu verhindern. Insoweit gilt diese Vorschrift für alle Szenarien, in denen diese Gefahr besteht.

77. **Frage:** **Müssen die Muster der VSA genutzt werden oder können diese an die Bedürfnisse der Behörde angepasst werden?**

Antwort: Wie der Anlage VIII zur VSA zu entnehmen ist, handelt es sich um verbindliche Muster für die Umsetzung der VSA. Diese können an die Bedürfnisse der Behörde ggf. nur unter sinngemäßer Beibehaltung der formalen und inhaltlichen Bestandteile angepasst werden.

78. **Frage:** **Gelten die Regelungen der VSA auch im Deutschen Bundestag und im Bundesrat?**

Antwort: Die VSA richtet sich an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit VS arbeiten. Dienststellen wenden in der Zusammenarbeit mit dem Deutschen Bundestag und dem Bundesrat ausschließlich die VSA an (vgl. § 1 Absatz 1 VSA).

Über die Behandlung von VS in den Verfassungsorganen entscheiden diese selbst. Sie können abweichende Regelungen treffen (z. B. Geheimschutzordnung des Deutschen Bundestages). Die VSA gilt jedoch unmittelbar für die Verwaltungen des Deutschen Bundestages und des Bundesrates.

79. **Frage:** **Gibt es Prüfrechte auf die VSA-konforme Umsetzung durch die Innenrevision?**

Antwort: Die Interne Revision unterstützt die Hausleitungen bei der Wahrnehmung der Dienst- und Fachaufsicht, indem sie durch Prüfungs- und Beratungsleistungen Optimierungsmöglichkeiten der Geschäftsprozesse aufzeigt und Entscheidungshilfen erarbeitet. Sie arbeitet in der Regel mit allen Organisationseinheiten in den Dienststellen zusammen. Aufgaben und Rechte der Internen Revision ergeben sich in der Regel aus den Revisionsordnungen der Dienststellen.

Die Prüfung der ordnungsgemäßen Umsetzung der VSA obliegt den Geheimschutzbeauftragten. Die Aufgabenwahrnehmung der in der Geheimschutzorganisation beteiligten Organisationseinheiten kann durch die Interne Revision geprüft werden.