

Häufig gestellte Fragen (FAQ) zu Anlage 4 GHB – VS-NfD- Merkblatt, insbesondere zu der Nutzung von Informationstechnik (VS-NfD- FAQ)

Disclaimer

Vor der Weitergabe von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) an nichtöffentliche Stellen (u.a. Unternehmen) muss mit diesen jeweils ein Vertrag geschlossen werden, in den die Bestimmungen dieses VS-NfD-Merkblatts (Anlage 4 zum Handbuch für den Geheimschutz in der Wirtschaft, Geheimschutzhandbuch – GHB, Inkrafttreten 01.09.2023) Eingang gefunden haben. Die konkreten geheimschutzrechtlichen Anforderungen eines VS-NfD-Auftrages sind zwischen VS-NfD-Auftraggeber und VS-NfD-Auftragnehmer zu klären.

Die Inhalte dieser Fragensammlung wurden mit größter Sorgfalt und nach bestem Wissen erstellt. Adressaten dieses Dokumentes sind primär die möglichen VS-NfD-Auftragnehmer auf **abstrakt-genereller** Ebene. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte kann jedoch **keine Gewähr** übernommen werden. Maßgeblich bleibt der Text des VS-NfD-Merkblattes bzw. wie er in den jeweiligen Vertrag zwischen VS-NfD-(Unter-) Auftraggeber und VS-NfD-(Unter-) Auftragnehmer Eingang gefunden hat.

Diese FAQ dienen nicht der Erörterung von Rechtsfragen und stellen keine rechtsverbindliche Auskunft dar, sondern dienen der **rechtlich unverbindlichen** Erklärung wiederkehrender Fragemuster (**Unverbindlichkeitsklausel**). Sie stellen keine Verwaltungsvorschrift dar, und ein schutzwürdiges Vertrauen kann aus diesen FAQ nicht abgeleitet werden. Ein schutzwürdiges Vertrauen kann hieraus nicht abgeleitet werden. Sie ersetzen nicht die notwendige Klärung von Fragen zwischen VS-NfD-(Unter-) Auftraggeber und VS-NfD-(Unter-) Auftragnehmer (rechtliches Verhältnis).

Alle relevanten Regelungen bleiben unberührt.

Stand: 05/2026, Ergänzung/ Überarbeitung dieses Dokumentes erfolgt bedarfsweise.

Einführung

Der Schutz von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) in nichtöffentlichen Stellen (wie Unternehmen) ist im sog. VS-NfD-Merkblatt (Anlage 4 zum Handbuch für den Geheimschutz in der Wirtschaft, Geheimschutzhandbuch) geregelt, das zum 01.09.2023 im Einvernehmen mit dem **BMI** und dem **BSI** an den **technologischen Fortschritt** und die **veränderte Sicherheitslage** angepasst wurde. Das VS-NfD-Merkblatt stellt sicher, dass VS-NfD in Unternehmen **vergleichbar** geschützt sind wie in Behörden. Bei dieser Novellierung wurde die **Technologieoffenheit** bedacht und von Anfang an berücksichtigt, auch um Rechtsunsicherheit und ständigen Anpassungsdruck bei neuen technischen Entwicklungen durch kurze Novellierungs-Zyklen zu vermeiden. Die Geltung des VS-NfD-Merkblattes wird **vertraglich** zwischen VS-NfD-Auftraggeber (z.B. XY Behörde) und VS-NfD-Auftragnehmer (z.B. XY GmbH) vereinbart.

Die **staatliche Verpflichtung zum Schutz von Verschlusssachen** endet für die öffentliche Stelle/den amtlichen VS-NfD-Auftraggeber nicht mit der Weitergabe an eine nichtöffentliche Stelle gem. § 4 Abs. 4 S. 2 SÜG sowie gem. der SÜG-AVV zu § 4 Abs. 4 S. 2. Dies spiegelt sich auch in der Kontroll- und **Beratungspflicht** des (öffentlichen) VS-NfD-Auftraggebers gem. Teil 1a), Ziff. 4.3 VS-NfD-Merkblatt wider. Rückfragen sind daher im rechtlichen VS-NfD-Auftragsverhältnis mit dem VS-NfD-Auftraggeber zu klären.

Allgemeine Fragen

An wen wende ich mich bei Rückfragen zu VS-NfD?

Wenn Ihre Fragen nicht durch die Lektüre des VS-NfD-Merkblattes und die vorliegenden FAQ beantwortet werden können, wenden Sie sich für weitere Auskünfte an Ihren amtlichen VS-NfD-Auftraggeber. Auf die Verpflichtung des amtlichen VS-NfD-Auftraggebers gem. § 4 Abs. 4 S. 2 SÜG sowie gem. der entsprechenden Ziff. der SÜG-AVV wird hingewiesen (Schutzverpflichtung der öffentlichen Stellen/ amtlichen VS-NfD-Auftraggeber für VS-NfD auch bei Weitergabe an nichtöffentliche Stellen/ VS-NfD-Auftragnehmer). VS-NfD-Unterauftragnehmer wenden sich an ihren VS-NfD-Unterauftraggeber.

Wurden bei der Erstellung des VS-NfD-Merkblattes, das zum 01.09.2023 in Kraft getreten ist, die Belange der Wirtschaft berücksichtigt?

Ja, das BMWF hat die Wirtschaft bei der Erstellung beteiligt, damit die Belange der Wirtschaft artikuliert werden konnten. Bei der Abstimmung des VS-NfD-Merkblattes mit anderen Behörden hat das BMWF die Belange der Wirtschaft geltend gemacht. Zudem wurden die Rückmeldungen und Fragen aus der Wirtschaft in dem vorliegenden Dokument berücksichtigt.

Seitdem tauscht sich das BMWF weiterhin mit den Verbänden und Behörden aus, um einerseits für einen einheitlichen Vollzug des notwendigen Sicherheitsniveaus zu sorgen und andererseits praxiserichte Ansätze zu ermöglichen, die im Einzelfall mit dem jeweiligen VS-NfD-Auftraggeber abzustimmen sind.

Wurden die Belange von kleinen und mittleren Unternehmen (KMU) berücksichtigt?

Ja, ein sog. KMU-Check wurde durchgeführt. Insbesondere die gestuften und differenzierenden Regelungen zum BSI-IT-Grundschutz und zur Selbstakkreditierung statt einer Zertifizierung gehen hierauf zurück.

Die vorliegenden VS-NfD-FAQ sollen ebenfalls KMU und Start-Ups unterstützen und werden auch aus diesem Grund bei Bedarf überarbeitet.

Geht das VS-NfD-Merkblatt über die Anforderungen der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) hinaus?

Nein, das VS-NfD-Merkblatt stellt ein vergleichbares Sicherheitsniveau zur VSA unter Berücksichtigung der Besonderheiten des VS-NfD-Schutzes in nichtöffentlichen Stellen her. Beispielsweise bedarf es nach dem VS-NfD-Merkblatt nicht in jedem Fall einer Umsetzung des BSI-IT-Grundschutzes. Die VSA kann jedoch für einzelne Streitige Fragen ggf. eine mögliche Auslegungshilfe für das VS-NfD-Merkblatt darstellen.

Welche Vorgaben habe ich einzuhalten, wenn ich vergleichbar VS-NfD eingestufte Internationale VS (z.B. NATO RESTRICTED, OCCAR RESTRICTED, etc.) bearbeite?

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

Warum sieht das VS-NfD-Merkblatt den Hinweis auf eine mögliche Strafbarkeit nach den §§93 ff StGB vor?

Auch eine VS-NfD kann ein Staatsgeheimnis i.S.d. § 93 StGB darstellen. Auf die Einstufung kommt es dabei nicht zwingend an. Die Einstufung auf Grundlage des SÜG bzw. der VSA hat hinsichtlich des Vorliegens eines Staatsgeheimnisses lediglich Indizwirkung. Eine Strafbarkeit nach den §§ 93ff StGB ist daher auch für VS-NfD denkbar.

Gibt es eine Übersetzung des VS-NfD-Merkblattes in andere Sprachen?

Eine englischsprachige, rechtlich unverbindliche Höflichkeitsübersetzung (sog. courtesy translation) steht im Sicherheitsforum des BMW E zum Download bereit. Maßgeblich bleibt die deutschsprachige Fassung, die auch vertraglich einzubeziehen und zu zeichnen ist. Nicht-geheimschutzbetreute Unternehmen können diese Höflichkeitsübersetzung bei DSA-germany@bmwe.bund.de unter Darlegung der Notwendigkeit anfordern.

Welche Vorgaben habe ich einzuhalten, wenn ich vergleichbar VS-NfD eingestufte ausländische VS bearbeite?

Die Regelungen des VS-NfD-Merkblattes gelten für deutsche VS-NfD sowie für ausländische vergleichbar eingestufte VS, die einem Unternehmen in Deutschland zur Aufbewahrung oder Verarbeitung auf Grundlage eines bilateralen Geheimschutzabkommens (GSA) überlassen worden sind.

Ggf. sind weitere Vorgaben aus den Geheimschutzabkommen bzw. aus vertraglichen Vorgaben, z. B. aus Project Security Instructions (PSI) oder Security Aspects Letter (SAL), zu beachten.

Woher weiß ich, ob zwischen Deutschland und einem anderen Land ein bilaterales Geheimschutzabkommen besteht und ob darin eine Vergleichbarkeit mit VS-NfD vereinbart wurde?

VIII B5-International gibt auf Anfrage Auskunft zu Vorliegen und Inhalt von bilateralen Geheimschutzabkommen und kann diese bei nachgewiesener Notwendigkeit auch an Unternehmen zur Verfügung stellen (DSA-germany@bmwe.bund.de).

Geheimschutzbetreute Unternehmen finden zusätzlich im passwortgeschützten Bereich des BMW E-Sicherheitsforums eine Übersichtsliste über alle bilateralen Geheimschutzabkommen und die hierin festgelegten Äquivalenzen der Geheimhaltungsgrade

Ist eine Bearbeitung von VS-NfD in Papierform im Homeoffice möglich?

Eine Mitnahme zur Verarbeitung von VS-NfD in Papierform ist in der Privatwohnung grundsätzlich unzulässig. Jedoch kann der öffentlicher VS-NfD-Auftraggeber Ausnahmen zulassen (siehe Teil 2, Ziff. 7). Darauf bezieht sich auch der Hinweis in Teil 6, Ziff. 2.

Besteht die Möglichkeit einer Sicherheitsüberprüfung (SÜ) für VS-NfD verpflichtetes Personal (z.B. Administratoren)?

Nein. Die rechtliche Grundlage für eine SÜ ist das Sicherheitsüberprüfungsgesetz (SÜG). Dieses sieht eine SÜ erst beim Umgang mit Verschlusssachen ab dem Geheimhaltungsgrad VS-VERTRAULICH vor.

Auch eine große Anzahl an VS-NfD rechtfertigt für sich genommen keine SÜ. Erst wenn eine Gesamteinstufung durch den VS-Herausgeber zu VS-VERTRAULICH in der Einstufungsliste erfolgt, sind SÜ erforderlich. Dann sind die VS jedoch auch in materieller und IT-Hinsicht nach den strengeren Vorgaben für VS-VERTRAULICH zu schützen, was entsprechende, teils erhebliche, Folgen (Kosten, Dauer) mit sich bringen kann.

Erhalte ich für VS-NfD einen Sicherheitsbescheid?

Nein, für den Geheimhaltungsgrad VS-NfD ist kein Sicherheitsbescheid gefordert, nicht erforderlich und kann daher auch nicht ausgestellt werden.

Kann ich für VS-NfD eine Facility Security Clearance (FSC) erhalten?

Nein, für den Geheimhaltungsgrad VS-NfD wird keine FSC ausgestellt (siehe vorstehende Antwort).

Welche Person aus dem Unternehmen hat Teil 1b) des VS-NfD-Merkblattes (Vereinbarung) zu unterschreiben?

Das Unternehmen bestimmt, wer die Unterschrift leistet. Erforderlich ist, dass die unterzeichnende Person zu diesem Zeitpunkt hierfür die erforderlich Vertretungsmacht hat.

Kann der VS-NfD-Auftraggeber weitere Anforderungen, die über die im VS-NfD-Merkblatt benannten Anforderungen hinausgehen, verlangen?

Ja, der VS-NfD-Auftraggeber kann im Einzelfall auf vertraglicher Basis über das VS-NfD-Merkblatt hinausgehende Anforderungen in eigener Verantwortung vertraglich vereinbaren. Regelmäßig dürften im nationalen Kontext weitergehende Anforderungen nicht erforderlich sein, zumal zusätzliche Kosten- und Zeitaufwände zu bedenken wären.

Soll das VS-NfD-Merkblatt weiterentwickelt werden?

Eine Evaluierung des VS-NfD-Merkblattes erfolgt regelmäßig. Gleichwohl sollen neue Implementationsaufwände durch kurze Novellierungszeiträume vermieden werden. Der technische Fortschritt, insbesondere im VS-NfD-IT-Bereich, internationale Vorgaben und die sich stetig verändernde Sicherheitslage werden es erforderlich machen, das neue VS-NfD-Merkblatt daran angepasst weiterzuentwickeln.

Dürfen Personen zusätzlich auch von öffentlichen Stellen verpflichtet werden?

Ja, die Verpflichtung durch die nichtöffentliche Stelle lässt die Möglichkeit der Verpflichtung durch die öffentliche Stelle unberührt. Inwieweit dies erforderlich ist, entscheidet der amtliche VS-NfD-Auftraggeber, auch in Anbetracht des § 353b StGB (Verletzung von Dienstgeheimnissen).

Wo finde ich Informationen zur Sicherheitslage?

Neben dem jährlich erscheinendem Verfassungsschutzbericht, insbesondere dem dortigen Berichtsteil „Spionage [...]“ als Grundlagenwissen, bieten verschiedene Sicherheitsbehörden (vor allem BfV/ BSI) weiteren Informationsangebote an.

Dies betrifft zum Beispiel die Publikationsformate „Sicherheitshinweis für die Wirtschaft“ und „Sicherheitshinweis für Politik & Verwaltung“, die sog. „BfV Cyber-Briefe“, den jährlichen Bericht des BSI „Die Lage der IT-Sicherheit in Deutschland“ (Reihe), den jährlichen Verfassungsschutzbericht (Reihe) und die umfassenden Hinweise zum sog. Wirtschaftsgrundschutz. Auch das BKA unterstützt mit entsprechenden Angeboten.

Besonders hilfreich sind die „Info-Blätter“ des BfV.

Zudem wird auf die zusätzlichen Angebote der jeweiligen Landesämter für Verfassungsschutz und den jeweiligen Landesverfassungsschutzbericht hingewiesen. Weitere Informationen finden Sie zudem bei der „Initiative Wirtschaftsschutz“ zu verschiedenen Themen, die im Grundgedanken auch für den Schutz von VS-NfD übertragbar sind. Die DIN SPEC 14027 Corporate Security - Anforderungen zur Stärkung physischer Resilienz von Organisationen stellt sie eine gute Grundlage für den Schutz des Vorfeldes von VS-NfD dar, z. B. für Reisesicherheit, Pre- oder In-Employment-Screening, Sicherheitskultur, Schulung-/Sensibilisierungsmaßnahmen, sicherheitsbezogenen Dienstleistungen und Standortsicherheit.

Hinweis: Die vorstehend genannten Informationsangebote stellen eine Grundlage dar, auf der in der Folge die Maßnahmen des VS-NfD-Schutzes aufgesetzt werden können. Dadurch können Unternehmen in eigener Verantwortung einen wirksamen Schutz auch im Vorfeld des VS-NfD-Schutzes etablieren. Regelungen des VS-NfD-Merkblattes bleiben davon unberührt.

Wie kann ich prüfen, ob eine Person geeignet ist?

Eine Sicherheitsüberprüfung ist für VS-NfD gesetzlich nicht vorgesehen (s.o.). Eine Orientierung können die in § 5 Abs. 1 SÜG genannten Sicherheitsrisiken bieten. Methodisch bietet sich ein z. B. (Pre-)Employment – im gebotenen Umfang und unter Einhaltung datenschutzrechtlicher Vorschriften – an. Rückfragen können Sie an Ihren VS-NfD-

Auftraggeber richten. Ggf. können auch die Landesämter für Verfassungsschutz im Rahmen ihrer Zuständigkeit helfen.

Müssen Personen, die keinen Zugang mehr zu VS-NfD erhalten sollen, entpflichtet werden, so wie ermächtigte Personen formal entmündigt werden?

Nein, eine formale „Entpflichtung“ ist nicht vorgesehen. Es reicht aus, der Person keinen Zugang mehr zu VS-NfD zu gewähren. Es kann sinnvoll sein, bei der Beendigung des Zugangs ein Debriefing vorzunehmen.

Ist eine Wiederholungsbelehrung erforderlich?

Eine feste Frist für eine Wiederholungsbelehrung besteht nicht. Ihre Durchführung liegt im Ermessen der VS-NfD-verantwortlichen Person und bietet sich auch als Sensibilisierungsmaßnahme an, beispielsweise bei einer Änderung der Umstände (z. B. wesentlich neue Regelungen/ VS-NfD-IT/ VS-NfD-Aufträge, geänderte Sicherheitslage, nach Sicherheitsvorkommnissen, andere Lebensumstände, internationale Vorgaben, Informationen des Verfassungsschutzverbundes, etc.) oder nach Zeitlauf in einem festen Rhythmus.

Wer ist für den Schutz von VS-NfD in geheimschutzbetreuten Unternehmen zuständig?

Geheimschutzbetreeute Unternehmen unterliegen nicht nur den Regelungen des VS-NfD-Merkblattes, sondern auch den weiteren Regelungen des Handbuches für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch, GHB) und haben einen Sicherheitsbevollmächtigten gem. § 25 SÜG zu bestellen. Gem. Ziff. 3.2 Abs. 1 GHB ist der Sicherheitsbevollmächtigte bei allen VS-relevanten Entscheidungen einzubinden und gem. Ziff. 3.3.1 Abs. 2 GHB für den Schutz von VS-NfD verantwortlich.

Die unternehmensinterne Einbindung des Sicherheitsbevollmächtigten ist durch das geheimschutzbetreeute Unternehmen, z. B. durch Arbeitsanweisungen, Beteiligungs-Workflows, Schnittstellen Vergabestelle/ Personalstelle/ IT-Sicherheit/Projektmanagement etc. zu regeln und die Einhaltung sicherzustellen.

Was besagt das Prinzip „Kenntnis nur, wenn nötig“/ „Need-to-know“

Dieses Prinzip ist die zentrale Grundlage des Geheimschutzes, beschränkt die Weitergabe der Information unabhängig von ihrem Medium und ist zudem gesetzlich in § 4 Abs. 1a SÜG geregelt. Das Prinzip durchzieht das gesamte VS-NfD-Merkblatt und ist eng auszulegen („Kenntnis haben müssen“, d.h. Kenntnis muss zwingend erforderlich sein). Es muss eine Notwendigkeit spezifisch zur Aufgabenerfüllung vorliegen. In Teil 2, Ziff. 1.2 des VS-NfD-Merkblattes wird es näher beschrieben, wozu auch der zeitliche Aspekt der Kenntnis („nicht eher“) und der quantitative/ qualitative Aspekt der Kenntnis („nicht umfangreicher“) gehören. Typische beispielhafte Anwendungsfälle, die in jedem konkreten Einzelfall kritisch zu würdigen sind: Personell: IT-Administrator, Teilnehmerkreis bei Besprechungen,

projektfremde Berater, Besucher, Reinigungs-/ Sicherheitskräfte; Methodisch: begleiten, persönlicher Gewahrsam, Abdecken, wegschließen.

Daher sind technisch-organisatorische Schutzmaßnahmen immer auch am Prinzip „Kenntnis nur, wenn nötig“ (sog. Need-to-know-Absicherung) auszurichten.

Darf ich mich bei der Umsetzung der vertraglichen Vorgaben des VS-NfD-Merkblattes beraten lassen?

Ja, jedoch mit Einschränkungen. Bei Inanspruchnahme einer Beratung bleiben die Pflichten der verantwortlichen Person und die Vorgaben des VS-NfD-Merkblattes unberührt.

Die technisch-organisatorischen Schutzmaßnahmen zur Absicherung des Need-to-knows sind zu wahren, um eine Weitergabe an den Berater als Dritten (kein Need-to-know, s.o.) zu verhindern.

Anwendungsfragen zur Verarbeitung von VS-NfD auf IT

Welche Vorgaben habe ich bei Nutzung von Informationstechnik (IT) beim Umgang mit VS-NfD einzuhalten?

Bei Nutzung von IT beim Umgang mit VS-NfD ist neben den weiterhin anwendbaren Teilen des VS-NfD-Merkblattes zusätzlich Teil 3 dieses VS-NfD-Merkblattes einzuhalten.

Welcher Weg ist der derzeit wohl üblicherweise kostengünstigste zur Bearbeitung von VS-NfD auf IT?

Wenn eine VS-NfD-Bearbeitung nur in geringem Umfang mit niedriger Komplexität stattfindet, stellt ein Einzelplatzsystem (sog. Stand Alone Gerät) den derzeit kostengünstigsten Fall dar.

Ebenso ist es möglich und sogar in vielen Fällen der effizienteste Weg, die freigegebene VS-NfD-IT des VS-NfD-Auftraggebers zu nutzen. Dies ist vor-Ort beim VS-NfD-Auftraggeber oder durch zur-Verfügung-Stellung der VS-NfD-IT möglich.

Kann ich für mein VS-NfD-IT-Netzwerk beim BWME eine „Genehmigung“/ Abnahme erhalten?

Nein, da eine solche durch BMW E weder vorgesehen noch erforderlich ist. Für den Schutz von VS-NfD ist nach dem Geheimschutzhandbuch (GHB) ausschließlich die für VS-NfD benannte verantwortliche Person des Unternehmens zuständig.

Ist eine (Teil-)Auslagerung der IT-Administration im Bereich VS-NfD zulässig?

Die VS-NfD-IT-Administration ist grundsätzlich durch eigenes Personal auszuführen. Auf Teil 3 Ziff. 3.7 des VS-NfD-Merkblattes und den dortigen Verweis auf Teil 2, Ziff. 6.3 des VS-NfD-Merkblattes wird hingewiesen, insbesondere zum Erfordernis einer Weitergabeerlaubnis, je nach Fallkonstellation. Eine Weitergabeerlaubnis ist in der Regel für die VS-NfD-IT-Administration nicht erforderlich, wenn sich der VS-NfD-Administrator dauerhaft keinen Zugang zu der VS-NfD verschaffen kann.

Die Weitergabeerlaubnis kann bei mehreren amtlichen VS-NfD-Auftraggebern innerhalb eines Ressorts ressortweit erteilt werden (ressortweite Weitergabeerlaubnis). Verantwortet ein amtlicher VS-NfD-Auftraggeber mehrere VS-Aufträge, so kann er auftragsübergreifend eine Weitergabeerlaubnis erteilen (auftragsübergreifende Weitergabeerlaubnis). VS-NfD dürfen nur mit Erlaubnis des VS-NfD-Herausgebers an Dritte weitergegeben werden. Gemäß des Prinzips „Kenntnis nur wenn nötig“ darf zudem eine Weitergabe nur dann erfolgen, wenn die Person auf Grund ihrer Aufgabenerfüllung Kenntnis von der VS-NfD haben muss (§ 4 SÜG). Wenn sich die VS-NfD eingestufte Information auf einer VS-NfD-IT befindet und die VS-NfD-IT-Umgebung von einem Dritten administriert werden soll, ist die Kenntnisnahme des Administrators von der VS-NfD regelmäßig nicht erforderlich und damit technisch auszuschließen. Dies gilt auch für die Fernwartung/ Remote-Administration.

Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System das Risiko, dass darüber unbefugt auf das VS-NfD-IT-System zugegriffen wird und innerhalb des VS-NfD-IT-Systems unbefugt VS-NfD zur Kenntnis genommen werden. Spätestens bei Netzübergängen zu externen Datenverarbeitern müssen vom BSI zugelassene IT-Sicherheitsprodukte zum Schutz der VS-NfD eingesetzt werden (vgl. VS-Produktkatalog des BSI). Auch der BSI-IT-Grundschutz sieht daher umfassende Regelungen in mehreren Bausteinen dazu vor. Das Need-to-know ist einzuhalten.

Was muss ich beachten, wenn ich verschiedene VS-NfD-Projekte bearbeiten möchte?

Daten unterschiedlicher VS-NfD-Aufträge müssen jeweils in separaten und ausschließlich für die jeweiligen zugriffsberechtigten Nutzer (Need-to-know) freigegebenen Projektordnern abgelegt werden. Eine differenzierte Selbstakkreditierung ist in der Regel nicht erforderlich, da diese system- und nicht projektbezogen erfolgt. Seitens des Auftraggebers können weitergehende Anforderungen, bspw. ausschließliche Verwendung des IT-Systems für das jeweilige Projekt, gesondert gefordert werden.

Kann ich auch einen Tablet-PC oder ein Smartphone als mobiles IT-System für VS-NfD einsetzen?

Ja, grundsätzlich besteht die Möglichkeit, jedoch darf keine private Technik verwendet werden. Dies erfordert die Umsetzung der Anforderungen gemäß VS-NfD-Merkblatt.

Können die VS-NfD-IT-Systeme an beliebigen Orten im Unternehmen betrieben werden?

Räumliche Arbeitsbereiche müssen durch die VS-NfD verantwortliche Person zuvor freigegeben werden. Der Grundsatz „Kenntnis, nur wenn nötig“ muss durch geeignete Maßnahmen sichergestellt werden (z.B. abschließbare Behältnisse, Sichtschutz, Mithörschutz bei Gesprächen).

Müssen Datenserver bzw. in der Produktion verwendete Maschinen, auf denen sich Daten mit VS-NfD-Inhalt befinden, täglich ausgeschaltet werden, wie Einzelplatzsysteme gem. Teil 3, Ziff. 2.1.1?

Nein, Server müssen nicht arbeitstäglich ausgeschaltet werden, wenn die betreffenden Vorgaben nach Teil 2, Ziff. 5 eingehalten werden. Gleiches gilt für VS-NfD verarbeitende Maschinen, die aufgrund von z.B. Dauerbetrieb, Rüstzeiten etc. nicht arbeitstäglich ausgeschaltet werden können.

Mein Rechner stürzt aufgrund eines Defekts im laufenden Betrieb ab. Auf dem Datenträger befinden sich eingestufte Daten. Ich kann diese aber vor der Wartung/Reparatur nicht löschen. Was muss ich tun?

Auf Datenträgern, die VS-NfD unverschlüsselt enthalten, sind die VS-NfD gem. Teil 3, Ziff. 3.6 des VS-NfD-Merkblattes 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 VS-NfD-Merkblattes.

Ich möchte VS-NfD-Daten im Unternehmensnetz in einem separaten, passwortgeschützten Ordner ablegen. Auf diesen Ordner haben nur die VS-NfD verpflichteten Personen Zugriff. Eine Firewall wird im Unternehmensnetz eingesetzt. Entspricht dieses Vorgehen den Anforderungen?

Nein. Hier handelt es sich nicht um ein separiertes VS-NfD-IT-System („air-gapped“). Demzufolge müssen sämtliche Anforderungen zur Kopplung eines VS-NfD-Netzes mit einem Netzwerk mit niedrigerem Sicherheitsniveau umgesetzt werden.

Ich möchte private Peripheriegeräte an meinem VS-NfD- Laptop verwenden, ist dies möglich?

Nein, private Geräte dürfen nicht für die Verarbeitung von Verschlusssachen eingesetzt werden. In der Vergangenheit haben Sicherheitsvorkommnisse gezeigt, dass dies eine Schwachstelle sein kann, die bei Cyberangriffen ausgenutzt wird.

Darf ich in meinem IT-System eine Funk-Tastatur und eine Funk-Maus einsetzen?

Sofern diese über eine Zulassungsaussage des BSI verfügen, ist dies zulässig.

Darf zur Bearbeitung von VS-NfD-Daten eine WLAN-Verbindung genutzt werden?

Die WLAN-Nutzung ist bei der Bearbeitung von VS-NfD nur in Verbindung mit einer Virtual Private Network (VPN) Lösung gestattet, welche über eine Zulassungsaussage des BSI verfügt. Entsprechende Produkte finden Sie auf der Webseite des BSI.

Darf ich VS-NfD aus dem Homeoffice elektronisch bearbeiten?

Obligatorisch sind zunächst weiterhin die Anforderungen des VS-NfD-Merkblatts sowie die spezifischen Einsatz- und Betriebsbedingungen der eingesetzten Produkte mit Zulassungsaussage des BSI umzusetzen. Als zusätzliche Regeln sind einzuhalten:

- die genutzte IT (z. B. Notebooks) muss hierfür von der für VS-NfD verantwortlichen Person freigegeben sein,
- die Privatwohnung muss sich innerhalb Deutschlands befinden,

- die für VS-NfD verantwortliche Person muss ihre Zustimmung erteilt haben,
- der/ die Mitarbeiter/in muss über die spezifischen Risiken des mobilen Arbeitens belehrt sein und
- Teil 6 des VS-NfD-Merkblattes muss von dem/ der Mitarbeiter/in unterzeichnet worden und vom Unternehmen als Nachweis aufbewahrt sein.

Kann ein VS-NfD-Unterauftrag an eine ausländische nichtöffentliche Stelle gegeben und können meine Mitarbeiter dann dort beschäftigt werden, damit sie über diese nichtöffentliche Stelle im Ausland im Homeoffice arbeiten können?

Nein. Selbst wenn die Voraussetzungen (z. B. Teil 2, Ziff. 6) im Übrigen erfüllt wären, stellt die Vergabe eines VS-NfD-Unterauftrages an eine andere nichtöffentliche Stelle im Ausland zum Zwecke der Ermöglichung des Homeoffices im Ausland eine missbräuchliche Vertragsgestaltung dar. Dadurch würden Teil 2, Ziff. 7, Teil 3, Ziff. 3.5 und Teil 6 Ziff. 1 umgangen.

Was sind die spezifischen Risiken des mobilen Arbeitens?

Bei der Behandlung von VS-NfD in der Privatwohnung ist das durch das VS-NfD-Merkblatt vorgegebene Schutzniveau umzusetzen. Es ist besonders darauf zu achten, dass

- die Einsichtnahme durch Dritte durch geeignete organisatorische oder technische Maßnahmen ausgeschlossen wird,
- das eingesetzte IT-Equipment zu keiner Zeit mit privaten IT-Equipment verbunden ist (Ausnahme für Internetzugangsroutern, sofern diese durch die VS-NfD verantwortliche Person freigegeben wurden),
- die IT-Systeme nicht für private Zwecke verwendet werden dürfen,
- Systeme welche nicht über eine Festplattenverschlüsselung mit Zulassungsaussage des BSI verfügen, vor Arbeitsende auszuschalten sind und im ausgeschalteten Zustand gemäß Teil 2, Ziff. 5 aufbewahrt werden müssen,
- Wartung und Reparatur der Systeme nur auf Veranlassung der für VS-NfD im Unternehmen zuständigen Person durchgeführt werden dürfen.

In der Vergangenheit haben Sicherheitsvorkommnisse gezeigt, dass das Homeoffice zu Schwachstellen führen kann, die bei Cyberangriffen ausgenutzt werden.

Wo erhalte ich die Produktlisten über zugelassene Produkte oder die Einsatz- und Betriebsbedingungen (EuB) zu diesen Produkten?

Die Unterlagen werden über den VS-NfD-Auftraggeber bezogen. Dieser kann die Unterlagen bei BSI anfordern, sofern ihm diese noch nicht vorliegen.

BSI-IT-Grundschutz und Selbstakkreditierung

Warum wurde der BSI-IT-Grundschutz als Schutzmaßstab gewählt?

Dieser stellt ein vergleichbares Schutzniveau zu öffentlichen Stellen dar und ist ein bewährter Maßstab, der einen umfassenden Schutz gewährleistet. Zudem ist maßgeblich, dass dieser Maßstab staatlich herausgegeben wird.

Findet der IT-Grundschutz des BSI grundsätzlich Anwendung?

Die Umsetzung des IT-Grundschutzes des BSI ist abhängig von der Ausprägung des VS-NfD-IT-Systems. Einzelplatzsysteme gem. VS-NfD-Merkblatt bleiben hiervon unberührt; hier sind ausschließlich die entsprechenden technischen und organisatorischen Maßnahmen zum Schutz der VS-NfD auf IT-Systemen gemäß VS-NfD-Merkblatt anzuwenden.

Wird für mein VS-NfD Netz eine Zertifizierung (z.B. ISO 27001) gefordert?

Nein, die VS-NfD verantwortliche Person im Unternehmen bestätigt der Geschäftsleitung spätestens alle drei Jahre schriftlich die Umsetzung der Anforderungen aus Teil 3 dieses VS-NfD-Merkblattes. Dieser Prozess wird Selbstakkreditierung genannt. Dadurch sollen unnötige Bürokratielasten vermieden werden.

Welche Details muss die Selbstakkreditierung gemäß VS-NfD-Merkblatt beinhalten?

In der Selbstakkreditierung erklärt das Unternehmen die Umsetzung der IT-Anforderungen in der jeweils gültigen Fassung, sofern erforderlich, die Umsetzung der Einsatz- und Betriebsbedingungen der Produkte mit Zulassungsaussage des BSI und die Beachtung des jeweils gültigen IT-Grundschutzes des BSI mit Erstellung eines Informationssicherheitskonzepts und einer Risikoanalyse, sofern erforderlich.

Muss die Selbstakkreditierung durch einen BSI-zertifizierten BSI-IT-Grundschutz-Berater erfolgen?

Nein, weder ist eine Zertifizierung erforderlich noch müssen etwaig hinzugezogene Berater zertifiziert sein. Die Selbstakkreditierung erfolgt durch die VS-NfD-verantwortliche Person. Sollten externe Berater in Anspruch genommen werden, ist darauf zu achten, dass diese in der Regel kein „Need-to-know“ für die VS-NfD haben.

Darf ich mich bei der Umsetzung des BSI-IT-Grundschutzes beraten lassen?

Ja. Der Berater muss kein BSI-zertifizierter BSI-IT-Grundschutz-Berater sein (s. o). Auch bei Inanspruchnahme einer Beratung ist die Selbstakkreditierung durch die verantwortliche

Person vorzunehmen. Bei Inanspruchnahme einer Beratung bleiben die Pflichten der verantwortlichen Person unberührt.

Wenn ich bereits ISO 27001 zertifiziert bin, gilt dann der BSI-IT-Grundschutz als erfüllt bzw. umgesetzt?

Wenn die ISO 27001 Zertifizierung auf Basis des einschlägigen Dokumentendossiers des BSI-IT-Grundschutzes erfolgt, gilt der BSI-IT-Grundschutz als erfüllt bzw. umgesetzt. Für alle anderen Fälle muss eine Gegenüberstellung der Zertifizierungsdokumente erfolgen (Differenzanalyse, sog. Gap-Analyse, siehe ggf. unterstützende Zuordnungstabellen) und ggf. nicht erfüllte Anforderungen des BSI-IT-Grundschutzes zusätzlich umgesetzt werden.

Wo finde ich Hilfe bei der Umsetzung des BSI-IT-Grundschutzes?

Das BSI stellt auf seinen Seiten hierzu umfangreiche, anwenderorientierte Informationen zur Verfügung (u. a. Checklisten, Zuordnungstabelle, Migrations-Anleitung mit Tabellen, Hilfsmittel, fiktives Fallbeispiel zu einem mittelständischen Unternehmen, IT-Grundschutz-Profile).

Ist bei einem technisch isolierten IT-System-Verbund (Teil 3, Ziff. 2.1.2) auch eine Risikoanalyse erforderlich?

Bei einem technisch isolierten System-Verbund gemäß Teil 3, Ziff. 2.1.2 wird im VS-NfD-Merkblatt die Umsetzung der Basisanforderungen des BSI-IT-Grundschutzes nur dann gefordert, wenn ein standortübergreifendes IT-System eingesetzt wird. Ziff. 4.2 geht davon aus, dass auch in diesen Fällen ein Informationssicherheitskonzept mit Risikoanalyse zu erstellen ist. Im Übrigen sind die weiteren Vorgaben der Teil 3, Ziff. 4.2 zu beachten.

Kann ich die Anforderungen für den erhöhten Schutzbedarf des BSI-IT-Grundschutz-Kompendiums ignorieren?

Laut VS-NfD-Merkblatt ist in Teil 3, Ziff. 2.2 für „VS-NfD-Netzwerke verbunden mit Netzwerksegmenten, die nicht die VS-NfD-Anforderungen erfüllen“ nur die Umsetzung der Basis- und Standardanforderungen gefordert. Gemäß des BSI-IT-Grundschutz-Kompendiums ist bei der Vorgehensweise der Standardanforderungen eine Schutzbedarfsfeststellung vorzunehmen.

Daher ist, wie auch im VS-NfD-Merkblatt unter Teil 3, Ziff. 4.2 gefordert, eine Risikoanalyse vorzunehmen. Wenn diese Risikoanalyse zum Ergebnis kommt, dass die umgesetzten Maßnahmen nicht ausreichen und zusätzliche Maßnahmen zur Risiko-Mitigation erforderlich sind, dann sollten die im Kompendium aufgeführten Anforderungen für erhöhten Schutzbedarf in Betracht gezogen werden.

Welche VS-NfD-Sicherheitsvorkommnisse kommen häufig vor?

Unverschlüsselter E-Mail-Versand von VS-NfD: Ein häufiges Sicherheitsvorkommnis ist der nicht ausreichend verschlüsselte bzw. nicht BSI-konform verschlüsselte Versand von VS-NfD, z. B. in Emails. Ein Teil dieser Fälle würde sich dadurch vermeiden lassen, dass Tools (Data Leak Prävention Tools, o.ä.) eingesetzt werden, die eine entsprechende Warnmeldung vor dem unverschlüsselten Versand von VS-NfD anzeigen oder diesen direkt unterbinden. Auch das Entschlüsseln von VS-NfD in nicht dafür geeigneten Umgebungen stellt ein häufig vorkommendes Sicherheitsvorkommnis dar.

Cyber-Angriffe: Cyberangriffe nehmen in Art und Intensität ebenfalls erheblich zu. Auf den turnusmäßigen Bericht des BSI „Die Lage der IT-Sicherheit in Deutschland“ wird hingewiesen. Das BSI bietet mit der „Allianz für Cybersicherheit“ ein umfangreiches Informationsangebot und Hilfestellungen.

Auch die verschiedenen Produkte der Cyber-Abwehr des BfV („BfV Cyber Insight“, „(Gemeinsame) Sicherheitshinweise/ (Joint) Cyber Advisory“, BfV Cyber Brief) führen die Methodik/ Angriffsvektoren, Akteure, Gefährdungslage, aber auch Schutzmöglichkeiten, vor Augen. Im Übrigen siehe FAQ „Wo finde ich Informationen zur Sicherheitslage?“.

Software

Dürfen VS-NfD Daten im allgemeinen Unternehmensnetz in einem virtualisierten Bereich/ Umgebung abgelegt werden?

Nein. VS-NfD-Daten sind in einer VS-NfD-konformen Umgebung gemäß den Vorgaben der Anlage 4 des GHB (VS-NfD-Merkblatt) vorzuhalten. Das Maß der technischen sowie organisatorische Maßnahmen orientiert sich dabei an der Ausprägung des VS-NfD-IT-Systems, in welchem auch das Anlegen virtualisierter Bereiche möglich ist.

Welche Vorgaben gibt es bzgl. der Telemetriedaten-Übertragung?

Für Betriebssysteme und mögliche weitere Applikationen (Software-Anwendungen) gilt, dass eine Telemetrie-Datenübertragung sowie weitere ungewollte Datenabflüsse von der eigentlichen VS-NfD-IT Bearbeitung auszuschließen sind und dies als fortlaufender Prozess zu prüfen ist.

Kann ein Virens Scanner mit einer online Datenprüfung im Bereich VS-NfD eingesetzt werden?

Nein, eine solche Software darf nur eingesetzt werden, wenn sich der Upload von Daten nachweislich deaktivieren lässt. Die Funktionalität ist nach jedem Update der Software zu prüfen.

Kryptierung

Was muss verschlüsselt werden?

Verschlüsselt werden muss entweder die Hardware selbst mit einer geeigneten Festplattenverschlüsselung und/ oder die elektronische Übermittlung der Daten durch Produkte, welche über eine Zulassungsaussage des BSI verfügen.

Wir verwenden eine Verschlüsselungssoftware zum elektronischen Datenversand. Kann dieses Produkt auch zum Versand von VS-NfD eingesetzt werden?

Ja, sofern das Produkt über eine Zulassungsaussage des BSI verfügt.

Wo finde ich die Liste der Produkte, die über eine Zulassungsaussage des BSI verfügen?

Eine abschließende Auflistung aller Produkte mit BSI-Zulassungsaussage finden Sie auf der Webseite des BSI.

Wann brauche ich eine geeignete Festplattenverschlüsselung? Warum reicht es nicht aus, dass auf meinem Notebook die Dateien oder Ordner, BSI-konform verschlüsselt abgelegt sind?

Sofern auf einem Datenträger alle VS-NfD-Dateien ordnungsgemäß BSI-konform verschlüsselt sind, bedarf es keiner zusätzlichen Festplattenverschlüsselung. Diese Konstellation ergibt sich ausschließlich für den Anwendungsfall Datensicherung. Zur VS-NfD-IT-Bearbeitung benötigt man die VS-NfD-Daten jedoch im Klartext. Dabei kann es passieren, dass vom Betriebssystem VS-NfD-Daten temporär ausgelagert werden. Daher besteht auch nach mehrmaligem, nach den Vorgaben des BSI vorgenommenen Löschen keine Gewissheit, dass sich nicht doch noch VS-NfD-Daten in Klartext auf dem Notebook befinden. Demzufolge sind Notebooks im mobilen Einsatz mit einer BSI-konformen Festplattenverschlüsselung zu versehen.

Muss ich meine USB-Sticks, Wechselplatten, CDs, etc. auch verschlüsseln?

Nein. Aber: VS-NfD-Datenträger, die eingestufte Daten unkryptiert enthalten, sind entsprechend den Vorschriften zu kennzeichnen. Sie sind im persönlichen Gewahrsam zu führen oder in abgeschlossenen Räumen/ verschlossenen Behältnissen aufzubewahren. Sie sind bis zur Vernichtung als VS-NfD-Datenträger zu behandeln.

Warum ist eine kryptierte Übertragung von Daten erforderlich?

Eine kryptierte Übertragung von Daten ist immer dann erforderlich, wenn ein Zugriff durch Dritte über einen Leitungsweg bzw. Übertragungsmedium nicht ausgeschlossen werden kann. Bei einer campus- bzw. standortübergreifenden elektronischen Datenübertragung kann i.d.R. ein Zugriff durch Dritte nicht ausgeschlossen werden.

Gibt es Ausnahmen von der kryptierten Übertragung?

Ja, 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.

Ich greife von einem anderen Ort auf den Fileserver zu. Ist dies eine Übertragung?

Ja, dies stellt eine elektronische Datenübertragung dar.

Was ist bei der Übertragung zu beachten?

Die Daten sind mit Produkten zu verschlüsseln, welche über eine Zulassungsaussage des BSI verfügen.

Was ist die Alternative zur kryptierten Übertragung?

Zum einen kann eine liegenschaftsübergreifende Übertragung von VS-NfD-Daten über nachweislich geschützte Leitungswege erfolgen. Zum anderen kann die VS-NfD per VS-NfD-Datenträger oder in Papierversion ausgetauscht werden. Hierbei sind die allgemeinen VS-NfD-Kennzeichnungs- und -Schutzpflichten einzuhalten.

Ich möchte VS-NfD als Anlage zu einer Mail versenden. Was muss ich beachten?

Mailversand von VS-NfD ist nur in Form einer kryptierten Anlage erlaubt. Zur Kryptierung sind ausschließlich Produkte einzusetzen, welche über eine Zulassungsaussage des BSI verfügen. Eine aktuelle Auflistung solcher Produkte findet sich auf der Webseite des BSI. Der Versand von VS-NfD mit Verschlüsselung durch Produkte ohne Zulassungsaussage des BSI stellt ein Sicherheitsvorkommnis dar.

„Isolierte Netze“ und „Cloud“-Anwendungen

Warum sind „isolierte Netze“ wichtig?

Mit zunehmender Vernetzung werden IT-Systeme immer anfälliger für Cyberangriffe. Dies führt zu einer erhöhten Bedrohungslage für die Kompromittierung von VS-NfD. Angesichts dieser zunehmenden Bedrohungen rückt die Sicherheit von IT-Systemen immer stärker in den Fokus.

In diesem Zusammenhang wird darauf hingewiesen, dass die VS-NfD-Daten in speziell geschützten Datenbereichen vorzuhalten sind. Daher sind isolierte Netze wichtig. Als weitergehenden Schutz der VS-NfD-Daten empfiehlt es sich regelmäßig, eine Trennung der VS-NfD-Daten vom Unternehmensnetzwerk („air-gapped“) herbeizuführen. Dies führt zu einer erheblichen Reduzierung der Gefährdungslage und kann, je nach Fallkonstellation, zugleich eine Reduzierung der VS-NfD-Administrationsaufwände bewirken. Dennoch ist der Einsatz von „air-gapped“-Technologie nicht risikolos, z. B. können mit Schadcode infizierte USB-Sticks weiterhin ein Risiko darstellen.

Was ist bei der Nutzung von Cloud-Diensten zu unterscheiden?

In geheimhaltungsmäßiger Hinsicht ist grundsätzlich zwischen **Private-Cloud**-, **Community-Cloud**- und **Public-Cloud**-Modellen zu unterscheiden. Das BSI hat einen Leitfaden „Leitfaden für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung“ erstellt, auf den an dieser Stelle verwiesen wird. Auch der BSI-IT-Grundschutz enthält Vorgaben zur Cloud-Nutzung.

Ist eine Ablage BSI-konform verschlüsselter VS-NfD-Daten in einer Public-Cloud derzeit erlaubt?

Ja, sofern und soweit die VS-NfD bereits für Transport (data-in-transit) und Ablage (data-at-rest) im Vorfeld (innerhalb VS-NfD-IT-System) ausschließlich BSI-zugelassen verschlüsselt wird. Dies gilt, sofern und soweit innerhalb einer Public-Cloud keine VS-NfD-Verarbeitung (data-in-use) stattfindet. Unabhängig von dem Betriebsmodell der Cloud ist dann auch keine VS-NfD-Freigabe der Public-Cloud-Infrastruktur erforderlich.

Jedoch ist weiterhin zu beachten (Aufzählung nicht abschließend):

- die Sicherstellung der Verfügbarkeit, auch nach Sicherheitsvorkommnissen und bei Kontrollen, und eigene dauerhafte Zugriffsmöglichkeiten,
- die durchgehende Einhaltung der Einsatz- und Betriebsbedingungen des Verschlüsselungsproduktes mit BSI-Zulassungsaussage sowie
- ggf. weitergehende Vorgaben aus dem Geheimschutzabkommen, der Project Security Instruction oder dem Security Aspects Letter.

Die jeweils erforderliche Verschlüsselung muss über die gesamte Lebensdauer der VS-NfD durchgehend sichergestellt sein und ggf. angepasst werden (z. B. KI-Anforderungen, Post-Quanten-Verschlüsselung, inhaltliche Änderung Einsatz- und Betriebsbedingungen).

Sicherheitsvorkommnisse können dann entstehen, wenn der Benutzer vor dem Entschlüsseln keine Warnmeldung erhält, dass der Ablageort der VS-NfD in einem VS-NfD-konformen Bereich zu erfolgen hat. Ein Entschlüsseln in der Public-Cloud ist ein meldepflichtiges Sicherheitsvorkommnis.

Dürfen Private-Cloud Lösungen eingesetzt werden?

Der VS-NfD-Auftragnehmer kann in seinen Räumlichkeiten bzw. seiner rechtlicher Verantwortungssphäre (z.B. Rechenzentrum, Serverraum) eine **Private-Cloud**-Infrastruktur als eigenes VS-NfD-IT-System, das seiner Selbstakkreditierung unterliegt, errichten und betreiben. Zur VS-NfD-IT-Administration wird auf obige Ausführungen verwiesen (zu Teil 3 Ziff. 3.7 des VS-NfD-Merkblattes und den dortigen Verweis auf Teil 2, Ziff. 6.3 des VS-NfD-Merkblattes).

Diese Private-Cloud ist dann in der Gesamtheit als eigene VS-NfD-IT freizugeben und Teil der Selbstakkreditierung des VS-NfD-IT-Systems. Die entsprechenden Bereiche, die VS-NfD verarbeiten, sind mit zugelassenen IT-Sicherheitsprodukten von Bereichen abzugrenzen, die nicht für die Verarbeitung von VS-NfD oder nicht als Teil des eigenen VS-NfD-IT-Systems freigegeben sind.

Im Übrigen gelten die Anforderungen u.a. gemäß Teil 3 VS-NfD-Merkblatt.

Hinweis: Die technologische Entwicklung, insbesondere im Cloud-Bereich, ist von großer Dynamik geprägt, sodass die vorstehenden Ausführungen nur eine Momentaufnahme darstellen können. Diesbezügliche Einzelfragen sind mit dem jeweiligen VS-NfD-Auftraggeber zu klären.

Abschließend wird erneut auf den Disclaimer mitsamt Unverbindlichkeitsklausel hingewiesen!