

Richtlinie zur Informationssicherheit

Traffic Light Protocol im Bundesverwaltungsamt

| | |
|--------------|---|
| Stand Datum: | 26. Juni 2025 |
| Version: | 2.7.1 |
| Status: | <input type="checkbox"/> in Bearbeitung <input type="checkbox"/> vorgelegt <input checked="" type="checkbox"/> abgenommen |

Inhaltsverzeichnis

| | | |
|-----------|---|-----------|
| 1. | Geltungsbereich und Vertraulichkeit..... | 3 |
| 1.1. | Zielgruppe | 3 |
| 1.2. | Geltungsbereich | 3 |
| 1.3. | Einstufung | 3 |
| 1.4. | Zuständigkeit und Revision | 3 |
| 2. | Einsatz von TLP..... | 4 |
| 3. | Vorgehensweise..... | 6 |
| 3.1. | Rollen | 6 |
| 3.2. | TLP-Verpflichtung | 7 |
| 3.3. | Verstoß gegen die Vorgaben | 8 |
| 3.4. | Weitergabe von TLP-Informationen | 8 |
| 3.5. | Ausnahmen von Weitergabebeschränkungen | 9 |
| 3.6. | Verschlüsselung | 9 |
| 4. | Anhang..... | 14 |
| 4.1. | Anlagen/Referenzen..... | 14 |

1. Geltungsbereich und Vertraulichkeit

1.1. Zielgruppe

Diese Richtlinie findet immer dann Anwendung, wenn in der Kommunikation zwischen BVA-Beschäftigten und Dienstleistenden oder anderen externen Beschäftigten Informationen – zum Beispiel in Form von Dokumenten – ausgetauscht werden müssen, deren Inhalte aus Sicht der erstellenden Person eine gewisse Sensibilität/Vertraulichkeit aufweisen können, aber keine Einstufung aus Sicht der VSA erfordern. Diese Richtlinie richtet sich in erster Linie an alle Beschäftigten in Bereichen der Softwareentwicklung und/oder IT-Projekten des Bundesverwaltungsamts, in denen Software entwickelt oder eingekaufte Software angepasst wird, sowie für Personen, die zur Einhaltung des Traffic Light Protocol (TLP) im Rahmen dieser Richtlinie zum Kommunikationsaustausch mit dem BVA aufgefordert wurden.

Diese Richtlinie ist als Anhang in die jeweiligen Verträge mit externen (Rahmen-)Vertragspartnerinnen und -partnern mit aufzunehmen, die beispielweise Beratungs- oder Softwareentwicklungsdienstleistungen für das BVA erbringen.

1.2. Geltungsbereich

Dieses Dokument ist ausschließlich für den internen Gebrauch, sowohl im BVA als auch bei externen Partnerunternehmen (Softwareentwicklungsdienstleistende, IT-Dienstleistende) des BVA, bestimmt. Eine Vervielfältigung, Speicherung, Umformatierung, Übertragung und/oder Weitergabe bzw. Verteilung in elektronischer und/oder physikalischer Form, auch von Auszügen, außerhalb des BVA bedarf der vorherigen Genehmigung der/des Informationssicherheitsbeauftragten (ISB) des BVA.

1.3. Einstufung

Für das vorliegende Dokument wird **keine Einstufung** nach der VS-Anweisung des Bundes (VSA) vorgenommen. Dieses Dokument ist nicht nach dem Traffic Light Protocol (TLP) markiert.

1.4. Zuständigkeit und Revision

Die Zuständigkeit für diese Richtlinie obliegt der/dem ISB BVA. Das Dokument ist entsprechend der jeweiligen IT-Sicherheitslage und Entwicklung fortzuschreiben. Die Richtlinie ist spätestens nach zwei Jahren einer Revision zu unterziehen.

Die Freigabe der Richtlinie erfolgt durch die Behördenleitung des BVA.

2. Einsatz von TLP

WICHTIG: Diese Richtlinie regelt den Einsatz des Traffic Light Protocol (TLP) im Bundesverwaltungsamt. **Das Merkblatt des BSI (im Folgenden auch „BSI-Merkblatt“), welches dieser Richtlinie als Anlage [Anl 01] beigelegt ist, ist zu befolgen und einzuhalten. Zusätzlich sind die BVA-spezifischen Auflagen zum TLP Einsatz im BVA verbindlich.**

Die im BVA angewendete Version des TLP entstammt der im Merkblatt des BSI festgelegten Version¹, welche auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Teams“ (FIRST)² basiert. Dabei soll diese Richtlinie über das Merkblatt hinaus BVA-spezifische Vorgaben festlegen, Zuständigkeiten benennen, einen Überblick über die Einsatzmöglichkeiten des TLP im BVA geben und als Handreichung für den Umgang mit sensiblen Informationen, die nach dem TLP behandelt werden sollen, dienen.

Die Schlüsselworte „MUSS“, „MUSS NICHT“, „VORAUSGESETZT“, „SOLL“, „SOLL NICHT“, „SOLLTE“, „SOLLTE NICHT“, „EMPFOHLEN“, „KANN“ und „OPTIONAL“ werden (analog zum Vorgehen des BSI) gemäß der Spezifikation RFC-2119³ verwendet.

Die Softwareentwicklung im BVA arbeitet mit externen Dienstleistenden zusammen. In den Projekten können bedingt durch die Fachlichkeit sensible Informationen anfallen, deren Vertraulichkeit und Integrität ausreichend geschützt werden müssen.

Um diesen Anforderungen gerecht zu werden, wird das Traffic Light Protocol (TLP) für Dokumente aus der Softwareentwicklung des BVA, die für eine Kenntnisaufnahme durch externe Firmen vorgesehen sind und bei deren Verarbeitung der Einsatz von VS-konformen IT-Arbeitsplätzen nicht gewährleistet werden kann, eingesetzt. Das TLP-Verfahren definiert durch die Farben „clear“ (ehemals „Weiß“), „Grün“, „Bernstein“ und „Rot“ auf verständliche Art und Weise, in welchem Adressatenkreis die so markierten Dokumente weitergegeben werden dürfen.

Das TLP dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. **Es ist damit eine standardisierte Vereinbarung zum Austausch schutzwürdiger Informationen, gilt aber nicht für Informationen, die nach der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) eingestuft sind. Für Informationen, die gemäß VSA eingestuft sind, gelten ausschließlich die**

¹ Merkblatt zum TLP 2.0 des BSI, Anlage [Anl 01]

² Zu finden unter <https://www.first.org/tlp/> (Stand März 2023)

³ <https://www.rfc-editor.org/rfc/rfc2119>

Auflagen aus der Verschlusssachenanweisung). Sobald eine Information, gleich welcher Art, nach VSA eingestuft wird, findet das TLP keine Anwendung mehr.

Das TLP regelt nicht den Schutz personenbezogener Informationen. Bitte beachten Sie hierzu die Vorgaben der Dienstanweisung IT-Arbeitsplatz (Kap. 4.3).

3. Vorgehensweise

Nach BSI-Merkblatt fällt die Aufgabe der TLP-Markierung der erstellenden Person (im Merkblatt als „Informationsersteller“ bezeichnet) zu. Dabei MUSS die erstellende Person die betreffende Information deutlich kennzeichnen:

- In E-Mails
 - als erste Worte in der **Betreffzeile**,
 - dem eigentlichen **Mail-Text** (im sog. Body) vorangestellt sowie
 - im **Dateinamen** (falls vorhanden).
- In Dokumenten
 - auf der **ersten Seite** als Teil des Titels oder dem Titel vorangestellt sowie
 - auf jeder folgenden Seite **in der Kopf- und Fußzeile** und
 - im **Dateinamen**
- Die Bezeichnungen **TLP:CLEAR**, **TLP:GREEN**, **TLP:AMBER**, **TLP:AMBER+STRICT** und **TLP:RED** werden jeweils ohne Leerschritt zwischen den Worten sowie in Versalschrift (Großbuchstaben) verwendet. Wenn möglich, SOLLTE die Kennzeichnung farbig gemäß BSI-Merkblatt erfolgen (vgl. [Anl 01] und [Anl 02]). Wenn die genaue Darstellung der Kennzeichnung aufgrund Farbe oder Doppelpunkt, beispielsweise in Dateinamen, aus technischen Gründen nicht eingehalten werden kann, darf davon abgewichen werden. Vorlagen für ein TLP-eingestuftes Konzept sowie für eine TLP-eingestufte Präsentation befindet sich in den Anlagen zu dieser Richtlinie ([Anl 03] und [Anl 04]).
- In nach TLP markierten Dokumenten MUSS auf das TLP-Merkblatt verwiesen werden. Das TLP-Merkblatt MUSS jedem dieser Dokumente beigelegt werden.

3.1. Rollen

Im BSI-Merkblatt werden die Rollen der beteiligten Personen definiert, die (in abgewandelter Form) auch in dieser Richtlinie verwendet werden:

- „Informationsersteller“ (in dieser Richtlinie „informationserstellende Person“)
- Verteilerlisten (z. B. BSI, CERT, SPOC, Verbände)
- „Empfänger“ (z. B. Behörden, Betreibende, Unternehmen, in dieser Richtlinie als „empfangende Person/Einrichtung“)
- ggf. verpartnerte Organisationen der empfangenden Einrichtung (i. d. R. vertraglich verbundene Organisationen, entweder als Dienstleistende oder als Kundenorganisation)

3.2. TLP-Verpflichtung

Weitergabe/Kenntnisnahme von TLP-markierten Informationen, mit Ausnahme von Informationen, die als **TLP:CLEAR** gekennzeichnet sind, ist nur gestattet, sofern Folgendes eingehalten wird:

Gemäß dem BSI-Merkblatt „erklären natürliche und juristische Personen [durch die Unterschrift auf der TLP-Verpflichtung] ihre Verpflichtung, die Regeln des TLP einzuhalten“ [Anl 01]. Je nach Personengruppe gilt im BVA:

- **Interne Beschäftigte des BVA** MÜSSEN sich an die vorliegende ISR zu TLP im BVA halten, so dass von einer zusätzlichen Verpflichtung durch eine Verpflichtungserklärung abgesehen werden kann.
 - **Externe Vertragspartnerinnen und -partner aus Rahmenverträgen des BVA** MÜSSEN im Rahmen ihrer Verträge zur Einhaltung der TLP-Richtlinie des BVA und des TLP-Merkblatts des BSI verpflichtet werden. Dies beinhaltet auch die Durchführung firmeninterner Sensibilisierungsmaßnahmen zu den Auflagen des TLP. Eine zusätzliche Verpflichtungserklärung vor Informationsaustausch mit dieser Personengruppe ist dann nicht erforderlich. Das entsprechende Unternehmen MUSS darüber hinaus zusichern, dass sie vor einer zulässigen Weitergabe der Informationen zu Subunternehmen, die jeweilige Firmenleitung über die TLP-Vorgaben informieren, damit diese geeignete Sensibilisierungsmaßnahmen veranlassen kann.
 - **Externe Beraterinnen und Berater, die nicht aus Rahmenverträgen des BVA beschäftigt werden,** MÜSSEN eine Verpflichtungserklärung [Anl 05] unterzeichnen, sofern sie mit dem TLP in Berührung kommen. Dadurch verpflichten sie sich, die Regeln des TLP einzuhalten. Die Verpflichtung MUSS durch die auftraggebende Organisationseinheit im BVA mit den eingesetzten Beraterinnen und Beratern durchgeführt werden. Die auftraggebende Organisationseinheit MUSS die unterzeichnete Verpflichtungserklärung bis zwei Jahre nach Tätigkeitsende der externen Kraft aufbewahren.
- **Bedienstete von deutschen und Behörden anderer Nationen, die mit dem BVA im Austausch stehen** und durch das BVA Kenntnis von TLP-markierten Informationen erhalten sollen, MÜSSEN die Vorgaben zur Handhabung von TLP ausgehändigt bekommen. Daher ist seitens des BVA sicherzustellen, dass innerhalb der Dokumente die Vorgaben des TLP-Merkblatts niedergeschrieben sind. Sofern es sich bei dem Adressaten um eine ausländische Behörde handelt, ist die englische Version der TLP-Vorgaben zu nutzen. Diese Vorgaben sind auf den ersten Seiten des Dokuments deutlich aufzuführen, so dass eine Einhaltung auf Seiten der Adressaten auch umsetzbar ist. Bei anderen Austauschformaten wie E-Mail ist das BSI-Merkblatt (ggf. Übersetzung in Englisch) mit dem eigentlichen Versand der TLP-Informationen, als (unverschlüsselter) Anhang im Rahmen einer Erstkontaktaufnahme zu übergeben.

- **SONDERFALL: Im Rahmen der Fachanwendung „Entwicklerportal“** MÜSSEN die Nutzenden über die Vorgaben des Umgangs mit TLP im BVA belehrt werden (beispielsweise durch Aushändigen des BSI-Merkblatts). Anschließend MÜSSEN sie eine Verpflichtungserklärung [Anl 06] unterschreiben und an die, für die fachliche Administration der Systeme zuständige Organisationseinheit des BVA zurücksenden. Dort MUSS die Verpflichtungserklärung aufbewahrt werden und darf erst nach zwei Jahren ab Beendigung der Zugriffsmöglichkeit der Person auf die Systeme, bzw. nachdem ein Account für die Person im System dauerhaft deaktiviert oder gelöscht wurde, vernichtet werden.

Wird das Dokument der TLP-Verpflichtung oder das TLP-Merkblatt seitens BSI oder diese Richtlinie durch die OE ISB in einer neuen Version herausgegeben, behalten die jeweils unterzeichneten Verpflichtungen ihre Gültigkeit, SOLLTEN jedoch, insbesondere bei Inhaltsänderungen, erneuert werden.

3.3. Verstoß gegen die Vorgaben

Bei einem Verdacht auf den Verstoß gegen die TLP-Vorgaben ist zusätzlich zu der erstellenden Person die/der Informationssicherheitsbeauftragte BVA zu informieren.

Die Kontaktinformationen der/des ISB BVA sind im Wiki-Bereich der OE ISB (<https://confluence.zssi.bva.in.bund.de/x/U4InAw>) zu finden.

3.4. Weitergabe von TLP-Informationen

| TLP-Markierung | Weitergabe an ext. Dienstleistende |
|------------------|---|
| TLP:CLEAR | Uneingeschränkte Weitergabe und Veröffentlichung. |
| TLP:GREEN | <p>Informationen dieser Stufe dürfen innerhalb des BVA, an Kunden- und Partnerbehörden sowie an beauftragte externe Dienstleistende weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.</p> <p>Eine Weitergabe von den beauftragten externen Dienstleistenden an weitere Unterauftragnehmende ist zulässig, sofern die weiteren Unterauftragnehmenden vertraglich benannt sind und somit ebenfalls für das BVA als Auftraggeber tätig sind.</p> |
| TLP:AMBER | <p>Informationen dieser Stufe dürfen innerhalb des BVA, an Kunden- und Partnerbehörden sowie an beauftragte externe Dienstleistende weitergegeben werden.</p> <p>Beauftragte externe Dienstleistende dürfen diese an Unterauftragnehmende weitergeben, sofern diese vertraglich benannt sind. Bei der Weitergabe gilt grundsätzlich das Prinzip „Kenntnis nur, wenn nötig“. Eine Weitergabe an Dritte⁴ ist nicht erlaubt.</p> |

⁴ Das BVA hat mit diesen natürlichen oder juristischen Personen keine vertraglichen Beziehungen.

| | |
|-------------------------|--|
| | Die informationserstellende Person/Stelle kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden. |
| TLP:AMBER+STRICT | Die Weitergabe ist ausschließlich auf die Organisation/Personenkreis der empfangenden Stelle/Stellen (Behörde, Institution) beschränkt. Es gilt das Prinzip „Kenntnis nur, wenn nötig“. Die informationserstellende Person/Stelle kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden. |
| TLP:RED | Informationen dieser Stufe sind ausschließlich auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten empfangenden Personen bei schriftlicher, elektronischer und E-Mail Korrespondenz beschränkt. Eine Weitergabe außerhalb dieses Kreises ist untersagt. |

Es ist NICHT erlaubt, dass TLP-markierte Informationen – mit Ausnahme von **TLP:CLEAR** auf Plattformen Dritter (bspw. KI-Tools (Übersetzer, Zusammenfasser, u. W.), Viruserkennung (Virustotal u. W.)) hochgeladen werden.

3.5. Ausnahmen von Weitergabebeschränkungen

Sollte im Ausnahmefall eine Weitergabe von Informationen an Personen oder -kreise (bspw. an Betroffene zur Krisenabwendung) notwendig sein, die der TLP-Markierung widerspricht, so KANN dies durch die erstellende Person nachvollziehbar genehmigt werden. Die empfangenden Personen MÜSSEN darauf hingewiesen werden, dass sie die Informationen nur für den genehmigten Einsatzzweck verwenden dürfen und sich an die Vorgaben des TLP-Merkblatts des BSI, welches Ihnen zu übermitteln ist, zu halten haben. Bei Verstößen werden sie zukünftig keine TLP-markierten Dokumente – mit Ausnahme von **TLP:CLEAR** – mehr erhalten.

3.6. Verschlüsselung

Die Voraussetzung zur Verschlüsselung richtet sich nach der jeweiligen Aufbewahrungsart, der TLP-Markierung und dem Kreis der Personen, die auf die Information zugreifen können. Von dieser Aufzählung explizit ausgenommen ist die Stufe **TLP:CLEAR** – Daten dieser Stufe können frei und gemäß den geltenden Vorschriften verteilt werden. Zur „geeigneten Verschlüsselung“ bieten sich folgende Vorgehensweisen an:

- 1) **GnuPG VS-Desktop** – Eine VS konforme Verschlüsselung ist zu bevorzugen, sofern alle Kommunikationspartner über die Software „VS-Desktop“ verfügen. Andernfalls wird empfohlen, eine PGP-Software in Abstimmung mit dem Adressatenkreis und mit angemessen gewählter Verschlüsselung zu verwenden. Für PGP-verschlüsselte Daten kann

die im BVA installierte Software „GnuPG VS-Desktop“ zur Ver- und Entschlüsselung verwendet werden. Für eine genauere Erklärung verweisen wir auf das Wiki der OE ISB⁵.

- 2) **Passwortgeschützte 7z/ZIP-Archive** – Hier ist die AES-256 Verschlüsselung zu wählen – dies ist ebenfalls auf der Wikiseite zu finden.
- 3) **Veracrypt-Container** – Die Software Veracrypt kann über den IT-Antrag beantragt werden.

Es können folgende Szenarien unterschieden werden:

1) **Ablage auf Netzlaufwerken des BVA**

- a. bis einschließlich **TLP:AMBER+STRICT**: Dateien dürfen auf Netzlaufwerken des BVA unverschlüsselt abgelegt werden, da nur BVA-Beschäftigte⁶ und externe Beschäftigte mit einer SINA-VW des BVA darauf zugreifen können.
- b. **TLP:RED** MUSS auf Gruppen- bzw. Projektnetzlaufwerken verschlüsselt abgelegt werden.

2) **Dateien in Ablage-, Versionierungs- und Kollaborationssystemen⁷ (NICHT Netzlaufwerke)**

Voraussetzung für die Nutzung von Ablage-, Versionierungs- und Kollaborationssystemen im Zusammenhang mit der Speicherung von TLP-Informationen ist, dass die Systeme über geeignete Authentifizierungsmechanismen und über ein stringentes Rechte-Rollenmanagement verfügen.

- a. **Innerhalb des Hausnetzes BVA** dürfen TLP-markierte Informationen unverschlüsselt abgelegt werden, da ausschließlich BVA-Beschäftigte und externe Beschäftigte mit einer SINA-VW des BVA auf diese Dateiablage zugreifen können. **TLP:RED** markierte Dateien MÜSSEN verschlüsselt werden.
- b. **Innerhalb der Netze des Bundes (NdB)** dürfen TLP-markierte Informationen nur bis einschließlich **TLP:AMBER** unverschlüsselt abgelegt werden. Informationen, die als **TLP:AMBER+STRICT** oder als **TLP:RED** klassifiziert sind, MÜSSEN verschlüsselt werden.
- c. In Dateiablagen, die **aus dem Internet** erreichbar sind, MÜSSEN Daten bereits ab einschließlich **TLP:GREEN** verschlüsselt werden.
- d. **SONDERFALL ZSSI**: Bei Nutzung eines Ablage-, Versionierungs- und Kollaborationssystems, das über die **Fremdfirmeneinwahl BVA** erreichbar ist,

⁵ <https://confluence.zssi.bva.in.bund.de/x/1oDHaw>

⁶ BVA-Beschäftigte sind in diesem Kontext nur interne Mitarbeitende. Die ITZBund-Administration der Fileserver wird hier nicht betrachtet.

⁷ Solche Systeme sind beispielsweise Alfresco, BSCW, SVN, CVS und GIT.

MÜSSEN Informationen, die als **TLP:AMBER+STRICT** oder als **TLP:RED** eingestuft sind, anhand von Ordnerstrukturen, die mit entsprechenden restriktiven Rechten belegt sind, geschützt werden. Der Grundsatz „Kenntnis, nur wenn nötig“ MUSS durch das Rechte-Rollenmanagement vollumfassend gewährleistet werden. Als **TLP:RED** markierte Dateien MÜSSEN zusätzlich verschlüsselt werden.

3) TLP eingestufte Dateien auf mobilen Endgeräten (Laptops, dienstlichen Smartphones usw.) oder Datenträgern (z. B. USB-Sticks)

- a. Dateien MÜSSEN ab **TLP:GREEN** geeignet verschlüsselt werden. Falls das Endgerät / der Datenträger selbst schon einen geeignet verschlüsselten und gesicherten Bereich für diese Dateien verwendet, gilt Fall 3b.
- b. Bei geeigneter Verschlüsselung der genutzten Datenträger oder Endgeräte, wie sie beispielsweise bei der Verwendung eines BVA-SINA-Laptops oder der SecurePIM-Umgebung gegeben ist, MÜSSEN Dateien erst bei einer Markierung mit **TLP:RED** verschlüsselt werden.

4) E-Mails mit TLP-markierten Daten⁸ oder Inhalten im Text

- a. E-Mails an bva.bund.de-Adressen und an NdB-angeschlossene Empfangsadressen dürfen unverschlüsselt versendet werden. **TLP:RED** markierte Inhalte MÜSSEN generell verschlüsselt werden.
- b. Bei Mailempfangsadressen im Internet MÜSSEN alle Inhalte ab **TLP:GREEN** geeignet verschlüsselt versendet werden.

SONDERFALL:

- c. Ist das BVA **Ersteller** einer **TLP:AMBER+STRICT** markierten Information, so gelten die Vorgaben aus 4a und 4b.
- d. Ist das BVA **nicht Ersteller**, sondern **nur** Empfänger einer **TLP:AMBER+STRICT** markierten Information, so DARF diese NICHT an Dritte außerhalb der Domäne bva.bund.de weitergeleitet werden. Ausgenommen ist die Kommunikation mit der Person, die die markierte Information erstellt hat.

5) Papierdokumente

⁸ Die Daten in E-Mails können sowohl im Mail-Text als auch im Anhang stehen. Falls die technischen Rahmenbedingungen zur Verschlüsselung kompletter E-Mails nicht erfüllt werden können, bietet sich folgendes Vorgehen an: Im Falle der Notwendigkeit einer Verschlüsselung SOLLTEN die zu schützenden Informationen nur im Dateianhang der Mail stehen, nicht im Mail-Text.

- a. Papierdokumente ab der Stufe **TLP:GREEN** MÜSSEN so aufbewahrt werden, dass sie von unbefugten Dritten nicht einsehbar sind. Papierdokumente der Stufen **TLP:AMBER**, **TLP:AMBER+STRICT** und **TLP:RED** MÜSSEN in verschlossenen Containern (z. B. abschließbare Büromöbel) aufbewahrt werden.
- b. Auf dem postalischen Weg MÜSSEN Papierdokumente der Stufe **TLP:GREEN** in einem verschlossenen Umschlag verschickt werden auf dem die TLP-Markierung zu erkennen ist. Papierdokumente der Stufen **TLP:AMBER** und **TLP:AMBER+STRICT** MÜSSEN in einem verschlossenen Umschlag mit der Bezeichnung der TLP-Stufe in einem weiteren Umschlag versendet werden, auf dem nur Absende- und Empfangsadresse, nicht jedoch die TLP-Stufe verzeichnet ist. Bei **TLP:AMBER+STRICT**-markierten Dokumenten vom BVA ist der Versand per Einschreiben durchzuführen.
- c. Ist das BVA Empfänger von **TLP:AMBER+STRICT**-markierten Dokumenten, DÜRFEN diese in Papierform ausschließlich über die Hauspost in versiegelten Umlaufmappen oder durch persönliche Übergabe an andere BVA-Liegenschaften weitergegeben werden.
- d. Papierdokumente der Stufe **TLP:RED** MÜSSEN der empfangenden Person persönlich ausgehändigt werden oder per Einschreiben mit persönlicher Übergabe versandt werden. Bei Letzterem MÜSSEN die Papierdokumente in einem verschlossenen Umschlag mit der Bezeichnung der TLP-Stufe in einem weiteren Umschlag versendet werden, auf dem nur Absende- und Empfangsadresse, nicht jedoch die TLP-Stufe verzeichnet ist.

| TLP-Stufe | Regelungen für den postalischen Versand |
|-------------------------|--|
| TLP:CLEAR | Normaler Versand - ohne Einschreiben |
| TLP:GREEN | Normaler Versand - ohne Einschreiben |
| TLP:AMBER | Normaler Versand - ohne Einschreiben |
| TLP:AMBER+STRICT | BVA ist Ersteller: Versand mit Einschreiben BVA ist nicht Ersteller: Weitergabe ausschließlich auf BVA intern beschränkt |
| TLP:RED | Einschreiben mit persönlicher Übergabe |

| Regelungen zur Verschlüsselung von TLP-markierten Informationen | | | | | |
|---|-------------------------|---|------------------------------------|---|---|
| Netz-Zugriff | TLP-Stufe | Versand per E-Mail | Projekt- und Gruppen-Netzlaufwerke | Ablage-, Versionierungs- und Kollaborationssysteme | Mobile Datenträger und Endgeräte |
| BVA-Netz | TLP:CLEAR | unverschlüsselt | unverschlüsselt | unverschlüsselt | Keine Verschlüsselung bei TLP:CLEAR . Verschlüsselung, wenn KEIN gesicherter/verschlüsselter Bereich auf dem Datenträger/Endgerät vorhanden ist. Bei der Verwendung eines BVA-SINA-Laptops ist eine geeignete Verschlüsselung bereits sichergestellt. TLP:RED markierte Dateien MÜSSEN verschlüsselt werden. |
| | TLP:GREEN | unverschlüsselt | unverschlüsselt | unverschlüsselt | |
| | TLP:AMBER | unverschlüsselt | unverschlüsselt | unverschlüsselt | |
| | TLP:AMBER+STRICT | unverschlüsselt | unverschlüsselt | unverschlüsselt | |
| | TLP:RED | verschlüsselt | verschlüsselt | verschlüsselt | |
| NdB-Netz | TLP:CLEAR | unverschlüsselt | - entfällt - | unverschlüsselt | |
| | TLP:GREEN | unverschlüsselt | | unverschlüsselt | |
| | TLP:AMBER | unverschlüsselt | | unverschlüsselt | |
| | TLP:AMBER+STRICT | unverschlüsselt (Fall 4c) keine Weitergabe erlaubt (Fall 4d) | | verschlüsselt unverschlüsselt: Sonderfall ZSSI 2)d | |
| | TLP:RED | verschlüsselt | | verschlüsselt | |
| Internet | TLP:CLEAR | unverschlüsselt | - entfällt - | unverschlüsselt | |
| | TLP:GREEN | verschlüsselt | | verschlüsselt | |
| | TLP:AMBER | verschlüsselt | | verschlüsselt | |
| | TLP:AMBER+STRICT | verschlüsselt (Fall 4c) keine Weitergabe erlaubt (Fall 4d) | | verschlüsselt | |
| | TLP:RED | verschlüsselt | | verschlüsselt | |

4. Anhang

4.1. Anlagen/Referenzen

| Referenz | Dokument / Link / Quelle |
|----------|---|
| [Anl 01] | „Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0“ (BSI Merkblatt TLP V2.0.pdf) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/TLP/merkblatt-tlp.html (Stand 06/2023) |
| [Anl 02] | TLP-Kennzeichnungsvorlage |
| [Anl 03] | Vorlage für ein TLP-eingestuftes Konzept |
| [Anl 04] | Vorlage für eine TLP-eingestufte Präsentation |
| [Anl 05] | Verpflichtungserklärung auf das TLP für externe Personen |
| [Anl 06] | Verpflichtungserklärung auf das TLP „Entwicklerportal“ |