Betriebskonzept

<Name des IT-Verfahrens>

|  |  |
| --- | --- |
| Version | 0.2 |
| Datum der Version | XX.XX.XXXX |
| Erstellt von (Funktion/Pers) | <OE>-<Rolle>/Bearbeiter **Beispiel**: IAB-IT-Gruppe/Meier |
| Genehmigt durch/am | OE-Leitung/YY.YY.YYYY **Beispiel**: IAB-Leitung 05.08.2022 |
| Vertraulichkeitsstufe | ( ) öffentlich  (X) Intern (hochschulöffentlich)  ( ) vertraulich (OE)  ( ) streng vertraulich (-/-) |
| Verteiler | OE, CIO-Board, GB1, CISO, DSB, PR |
| Review (geplant) | jährlich |
| Dokument | Betriebskonzept-Name-des-IT-Verfahrens-OE |

Inhaltsverzeichnis

[Inhaltsverzeichnis 2](#_Toc1)

[1 Einleitung, Zweck des IT-Verfahrens 6](#_Toc2)

[2 Anwendungsbereich und Anwendende 6](#_Toc3)

[3 Beschreibung des IT-Verfahrens 6](#_Toc4)

[3.1 Ausgangssituation, Anforderungen 6](#_Toc5)

[3.2 Zielbeschreibung, gewählter Lösungsweg 7](#_Toc6)

[3.3 Mit dem IT-Verfahren abgebildete Prozesse 7](#_Toc7)

[3.4 Rollen und Rechte 7](#_Toc8)

[4 Technische Maßnahmen zur Betriebs- und Datensicherheit 8](#_Toc9)

[4.1 Beschreibung und Übersicht der Systemlandschaft 8](#_Toc10)

[4.2 Beschreibung zu System 1 9](#_Toc11)

[4.3 Systembetrieb und Einrichtung 9](#_Toc12)

[4.4 Absicherung der Systeme 9](#_Toc13)

[4.4.1 Technische Absicherung 9](#_Toc14)

[4.4.2 Physische Absicherung (Zugangskontrolle) 10](#_Toc15)

[4.5 Verschlüsselung 10](#_Toc16)

[4.6 Patchmanagement 10](#_Toc17)

[4.7 Datensicherung und Wiederherstellung 11](#_Toc18)

[4.8 Redundanzen 11](#_Toc19)

[4.9 Überwachung und Protokollierung der IT-Systeme 11](#_Toc20)

[5 Organisatorische Maßnahmen 12](#_Toc21)

[5.1 Dokumentation und Schulungen 12](#_Toc22)

[5.2 Datenfeldkatalog und Löschkonzept 13](#_Toc23)

[5.3 Regelmäßige Revision des Betriebskonzeptes 13](#_Toc24)

[6 Gültigkeit und Dokumentenmanagement 13](#_Toc25)

[Referenzen 14](#_Toc26)

[Anlagen 14](#_Toc27)

[Traffic Light Protocol 15](#_Toc28)

**Anlage 2: Muster-Betriebskonzept zur IT-Rahmen-DV**

Dieses Dokument ist die Anlage 2 der „IT-Rahmendienstvereinbarung über die Einführung, Anwendung und wesentliche Änderung von IT-Verfahren (IT-Rahmen-DV)“ gemäß §2 (5) und stellt ein Muster für eine standardisierte Gliederung für ein Betriebskonzept eines IT-Verfahrens dar. Es enthält Ausfüllhinweise und beispielhafte Formulierungen. Die beispielhaften Formulierungen sind grundsätzlich auf ihre Passgenauigkeit hin zu überprüfen und entsprechend anzupassen. Die am Erstellungsprozess beteiligten Personen gehen davon aus, dass der Umfang einer final ausgefüllten Vorlage für einfache IT-Verfahren im Bereich von 10 bis 15 Seiten liegen dürfte, für große und komplexe IT-Verfahren, die die Verarbeitung von personenbezogenen Daten für eine besonders große Anzahl an betroffenen Personen enthalten, darüber liegen wird.

Für einen Start empfiehlt es sich, zunächst den Projektsteckbrief des PMO, in den Abschnitten „Konzeptphase“ und „Dauerbetrieb“ auszufüllen. So einiges an Informationen kann hier Verwendung finden. Gleichzeitig zahlt dieses Dokument auf die verpflichtend zu erstellende Verfahrenstätigkeitsbeschreibung gemäß DSGVO ein, so dass die spezifisch zu generierenden Informationen geringgehalten werden.

Diese Textbox soll in der finalen Version entfernt werden.

Dieses Dokument wird regelmäßig überarbeitet. Die aktuelle Version wird über das Informationsportal bereitgestellt.

**Hinweise zu verwendeten Formatierungen:**

***(Beschreibung, was in diesem Abschnitt erwartet wird (Klammern, kursiv, blau), kann nach Bearbeitung entfernt werden zwecks besserer Lesbarkeit.***

**Beispielhafte aber zu prüfende Formulierungen für den einfacheren Start.**

# Einleitung, Zweck des IT-Verfahrens

Der Zweck des IT-Verfahrens … ist, …  
*(Eine Übersicht des Systems, incl. einer Kurzbeschreibung liefern. Beginnen Sie beispielsweise mit dem Projektnamen (ggf. Akronym) aus dem von Ihnen bereits entworfenen Projektsteckbrief.)*

# Anwendungsbereich und Anwendende

Der Anwendungsbereich erstreckt sich auf alle Mitglieder und Angehörige der TU [ | sofern sie organisatorisch zu der das IT-Verfahren betreibenden OE zugeordnet sind | der Fakultäten A und B | in der Rolle [DV-Koordinierende | wissenschaftliche Mitarbeitende | …] | …].

Das Informationsangebot ist auf die breite Öffentlichkeit ausgerichtet und zielt auf die Gewinnung von Teilnehmenden der Konferenz mit rund 1000 Teilnehmenden. In verschiedenen internen Prozessen arbeiten die rund 50 Mitarbeitenden der OE mit dem IT-Verfahren.

*(Die Beschreibung soll den organisatorischen Einsatz, Gruppen und Rollen von Mitarbeitenden/Mitgliedern und Angehörigen/Externen und damit die grobe Anzahl der Betroffenen darstellen. Dies ist auf verschiedenen Ebenen wichtig, beispielsweise im Sinne einer Risikobetrachtung und damit u.a. Hinweisen zur Ableitung von Maßnahmen zu Ausfallsicherheit und Redundanz ermöglichen. Gleichen Sie hier mit den Angaben aus dem Projektsteckbrief „Welche OEn sind von dem Projekt betroffen“ ab, gehen Sie jedoch eine oder mehrere Ebenen tiefer für eine ausreichende Differenzierung.)*

# Beschreibung des IT-Verfahrens

*(Bedienen Sie sich in diesen Abschnitten Ihres Projektsteckbriefes und den Feldern „Zielsetzung“, „Nicht-Ziele“, ggf. „Strategische Relevanz“. Gehen Sie auf die Anforderungen ein, denn es hilft später im Rahmen der regelmäßigen Revision, der Weiterentwicklung oder Ablösung eines Systems, hier noch einmal prüfend ansetzen zu können, ob und wie sich die Anforderungen verändert haben.)*

## Ausgangssituation, Anforderungen

Die Mitarbeitenden sind über verschiedene Institute und Arbeitsgruppen verteilt … Hieraus ergibt sich eine Schwierigkeit in der Bearbeitung, die in die Formulierung folgender Anforderungen mündete: …

## Zielbeschreibung, gewählter Lösungsweg

Wie einleitend beschrieben … Es wird mit dem im IT-Verfahren eingesetzten Software-Werkzeug … und den damit verbundenen Prozessen … erreicht, dass …

## Mit dem IT-Verfahren abgebildete Prozesse

In diesem Abschnitt werden die innerhalb des IT-Verfahrens stattfindenden Prozesse beschrieben, die sowohl auf Seite der Nutzenden als auch auf Seite der Betreibenden durchgeführt werden.

*(Die Beschreibung kann mit dem Erfassen von Prozesseingang und –Ausgang kurz ausfallen, wenn die Beschreibung der Prozessabläufe in einem Werkzeug zur Prozessdokumentation erfasst sind. Konzentrieren Sie sich zunächst auf Prozesse, bei denen personenbezogene Daten verarbeitet werden.*

*Auf Seite der Nutzenden sind es die Prozesse, die sich aus den Beschreibungen in den beiden vorstehenden Abschnitten ergebenden.*

*Auf Seite der Betreibenden sind es die direkt mit dem Betrieb des IT-Verfahrens verbundenen Prozesse, beispielsweise im Zusammenhang mit dem für das IT-Verfahren spezifischen Zuweisen von Rollen und Rechten.*

*Immer dann, wenn mit den beschriebenen Prozessen personenbezogene Daten verarbeitet werden, ist auch eine Verfahrenstätigkeitsbeschreibung in dem von der TU Braunschweig betriebenen System zu deren Dokumentation (ergibt sich aus der DS-GVO) zu erstellen. Das, was sie hier im Betriebskonzept erstellen, zahlt auch auf die Dokumentationspflichten zu den Verfahrenstätigkeitsbeschreibungen mit ein.*

*Die Prozesse. die zur Umsetzung von technischen und organisatorischen Maßnahmen zur Betriebs- und Datensicherheit benötigt werden, gehören in der Regel in die entsprechenden folgenden Abschnitte, sofern diese spezifisch für das IT-Verfahren sind. Allgemein anzuwendende Prozesse, die Maßnahmen zur Betriebs- und Datensicherheit betreffend, sollten in gesonderte Dokumente ausgelagert werden (Richtlinien, Betriebskonzepte, Arbeitsanweisungen für Infrastrukturen).)*

## Rollen und Rechte

*(Das Ziel eines Rollen- und Rechtekonzepts ist es, den Zugriff auf Daten oder Informationen auf die berechtigten Personen zu beschränken. Es ist zu klären, ob die im IT-Verfahren eingesetzte Software geeignet ist, damit Gruppen eingerichtet werden können, um Berechtigungen von Mitarbeitenden für deren verschiedenen Rollen zu bündeln. Beispielsweise das Trennen der Rolle von Administrierenden und Nutzenden.)*

# Technische Maßnahmen zur Betriebs- und Datensicherheit

*(Dieser Abschnitt zahlt eindeutig auf die zu erstellenden und im System zur Dokumentation der Verfahrenstätigkeitsbeschreibungen benötigten technischen (und organisatorischen) Maßnahmen ein. Technisch-organisatorische Maßnahmen (TOM) dienen der Umsetzung einer sicheren Verarbeitung von personenbezogenen Daten. TOM müssen schriftlich dokumentiert werden, dies fordert die DS-GVO. Die TU Braunschweig betreibt ein eigenes System zur Verwaltung von Verfahrenstätigkeitsbeschreibungen sowie zugehörigen technischen und organisatorischen Maßnahmen, so dass alles was Sie hier dokumentieren auf die dort auszuführenden Dokumentationsaufgaben einzahlt.*

*Tipp: Elemente, die bei der Dokumentation von technischen Maßnahmen vom Dokumentationssystem der TU abgefragt werden und die Sie nicht dieser Dokumentation – auch nicht als Referenz auf andere Maßnahmen und Systeme – entnehmen können, fehlen hier. Nutzen Sie dieses Wechselspiel, um Ihre IT-Verfahren und deren Dokumentation besser hinsichtlich Konformität und möglicher Kontrollen zu gestalten (nicht abschließend und insbes. Datenschutz, Informationssicherheit, Fernmelde- und Telekommunikationsrecht, Arbeitsrecht & Leistungskontrollverbot, Software und UrhG, IT-Strafrecht))*

## Beschreibung und Übersicht der Systemlandschaft

*(In diesem Abschnitt sollen eine Beschreibung und ein Schaubild der beteiligten Systeme erstellt werden, aus denen mindestens hervorgeht:*

*Anzahl und Umfang der Systeme*

*Physische Zusammenhänge (Netzwerkplan)*

*Prozessuale Zusammenhänge (Datenaustausch)*

*Absicherung der Systeme untereinander*

*Ggf. sind im Folgenden weitere Abschnitte zu den weiteren für die Umsetzung des IT-Verfahrens von der Einrichtung betriebenen Systeme hier anzufügen. Grundlage des Umfangs ist, dass die hier beschriebene Systemlandschaft vollständig aufgegriffen wird.*

*Existieren für einige der in der Systemlandschaft angegebenen Systeme eigene Betriebskonzepte, so ist es ausreichend, die Funktion im Zusammenhang mit dem IT-Verfahren kurz in wenigen Sätzen zu beschreiben und auf das zu referenzierende Betriebskonzept dieses Systems hinzuweisen.)*

## Beschreibung zu System 1

*(Die Darstellung sollte gegliedert enthalten:*

*Systembeschreibung*

*Referenzen zu anderen Dokumenten, falls zutreffend*

*Ggf. Datentransportkatalog (Tabelle)*

*Ein Datentransportkatalog wird Ihnen bei der Anpassung von Prozessen und dem Berücksichtigen von Abhängigkeiten helfen. Frage: Welche Daten werden ausgetauscht? Diese Daten benötigen Sie auch im Datenfeldkatalog, der unter anderem von DSB, DSMGMT, CISO, Personalrat be(gut)achtet wird. In der Praxis erscheint es jedoch einfacher, zunächst für ein konkretes System die Daten zu erfassen.*

*Beispiel: LDAP zur Authentifizierung mit Abfrage userid, password sowie Antwort userid, Vorname, Nachname, OU, Ergebnis der Authentifizierung.*

*Beispiel: regelmäßiges skriptbasiertes Löschen von Nutzerkonten (userid, Verzeichnispfad) durch Skript „user\_delete“ per cron um 22:20 Uhr UTC.)*

## Systembetrieb und Einrichtung

Alle für das IT-Verfahren betriebenen Server sind auf der gleichen Betriebssystemplattform aufgebaut und zwar … in der „Long Term Support“-Version (LTS). Durch die Reduzierung auf nur ein Betriebssystem wird das Risiko für Fehlkonfigurationen verringert. Damit die betriebssysteminterne Sicherheitsstruktur genutzt werden kann, werden die verwendeten Softwarepakete stets über die systeminternen Installationsmechanismen bereitgestellt. Für die anbieterspezifischen Softwarepakete wurden die direkt vom Hersteller bereitgestellten spezifischen Quellen mit eingebunden.

## Absicherung der Systeme

### Technische Absicherung

Auf allen Systemen soll die interne Firewall immer aktiv sein und nur die benötigten Ports freigegeben werden. Weiterhin wird der Zugriff von allen Systemen des IT-Verfahrens auf das Internet standardmäßig protokolliert. Damit soll bei einem Angriff und einer eventuellen Übernahme der Systeme durch Dritte eine Rückkopplung zu den angreifenden Systemen (Nachladen von Schadcode) oder der Verbindungsaufbau zu Bot-Netzwerken bemerkt werden.

### Physische Absicherung (Zugangskontrolle)

*(Insbesondere Beschreibung der Maßnahmen zur Umsetzung der Zutrittskontrolle wie Alarmanlagen, Schließsysteme, Protokollierung der Zutritte, Beschreibung des für den Zutritt berechtigten Personenkreises, auch Externer. Umgang mit Besuchenden.)*

## Verschlüsselung

*(Den nachfolgenden Text müssen Sie auf Ihre Situation anpassen. Achten Sie darauf, dass ältere Geräte die mit höchsten Ratings verbundenen technischen Voraussetzungen nicht liefern können und sie – natürlich abhängig vom Zweck Ihres IT-Verfahrens – beispielsweise internationale Studierende aus Entwicklungs- und Schwellenländern ausschließen könnten. Fallbezogen ist eine Abwägung sinnvoll.)*

Das IT-Verfahren setzt auf eine Webanwendung, zu der festgelegt ist, dass diese transportverschlüsselt angeboten wird und nur noch TSL 1.2 und TSL 1.3 in Kombination mit aktuell sicheren Chiffren genutzt werden. Eine Validierung der Sicherheit erfolgt immer über einen mehrstufigen Sicherheitstest anerkannter Webseiten. Konkret wird jeweils zu Beginn eines Quartals https://globalsign.ssllabs.com/ verwendet. Maßnahmen zur Verbesserung des Ratings werden angewendet. Das Rating Ziel ist eine Bewertung mit „A“. Das Rating soll nicht schlechter als mit „B“ bewertet sein.

## Patchmanagement

*(Hier beschreiben Sie die Verfahrensweise für das Patchmanagement, also dem Umgang mit Patches, Updates und Upgrades in der gesamten das IT-Verfahren betreffenden Umgebung. Klären Sie die Frage, mit welchen Werkzeugen und in welchen Zyklen Sie das Einspielen von Patches, Updates und Upgrades sicherstellen. Je nach Verfügbarkeitsanforderungen beschreiben Sie einen Prozess, wann Sie (ggf. wie getestet und freigegeben) das Einspielen vornehmen, beispielsweise innerhalb eines feststehenden und kommunizierten Wartungsfensters.)*

## Datensicherung und Wiederherstellung

*(In diesem Abschnitt dokumentieren Sie die Art und Weise, wie Sie die Datensicherung und Wiederherstellung für das IT-Verfahren betreiben. Dies umfasst u.a. die Darstellung von Anforderungen, verbindlicher Prozesse und die Beschreibung des Backupsystems. Denken Sie auch an eine räumlich getrennte Aufbewahrung. Moderne Systeme bieten auch zusätzliche Mechanismen wie snapshots an. Denken Sie auch an einen Ausfall des Backups. Sie können hier auch auf ein Backup am GITZ verweisen.)*

## Redundanzen

*(In diesem Abschnitt wird die Absicherung der bestehenden Hard- und Software-Infrastruktur hinsichtlich der Minimierung des Ausfallrisikos beschrieben. Dieser Beschreibung sollte das Ergebnis einer Abwägung zur benötigten Ausfallsicherheit vorangestellt werden. Üblicher Weise werden technisch der Einsatz von Loadbalancern, redundante Netzanbindungen usw. beschrieben. Sofern das IT-Verfahren nicht im Rechenzentrum des GITZ betrieben wird, müssen Sie auch die physische Absicherung zur Umsetzung von Verfügbarkeit (Beispiele: Feuer- und Rauchmelder, Feuerlöschung, Klimatisierung, Stromversorgung) hier beschreiben oder auf ein eigenes Dokument verweisen.)*

## Überwachung und Protokollierung der IT-Systeme

*(Ziele der Protokollierung können sein:*

*Sicherheitsvorfälle nachvollziehen können*

*Auftreten von Funktionsstörungen und Sicherheitsvorfällen zu identifizieren*

*Patchlevel von Betriebssystemen und Anwendungen zu überwachen*

*Regelmäßige Auswertung der Firewall-Logs durchzuführen (BSI-Anforderung), um beispielsweise Anomalien oder Angriffe zu erkennen.*

*Gescheiterte Anmeldeversuche zu protokollieren als Hinweis auf Eindringversuche*

*Auslastung und die Entwicklung der Auslastung von Diensten zwecks Planung von Systemanpassungen*

*Verfügbarkeiten bzw. Ausfallzeiten zu messen*

*Im Folgenden könnten die verwendeten Systeme beschrieben werden, idealer Weise existiert zu diesen ebenfalls ein Betriebshandbuch oder Sie beschreiben eine im IT-Verfahren angelegte Überwachung und Protokollierung so, dass sie den formulierten Zielen entspricht. Sie dienen nicht zur Leistungs- und Verhaltenskontrolle der die IT-Systeme nutzenden Mitarbeitenden.)*

Protokoll- und Logdateien werden nur solange vorgehalten, wie sie für ihren vorgesehenen Zweck gebraucht werden. Anschließend werden sie gelöscht. Die administrierenden Personen wissen, dass Protokolldaten auf keinen Fall zur Verhaltens- und Leistungskontrolle der Nutzenden ausgewertet werden dürfen und sie sich hierzu nicht anweisen lassen dürfen. Es gelten die Regelungen der IT-Rahmen-DV.

Die folgenden Ziele sollen erreicht werden: … Mit folgenden Systemen und Verfahren soll dies sichergestellt werden: …

Die Haltedauer der Protokollierungen beträgt aufgrund der Anbindung an eine Angriffserkennung … Tage und überdeckt somit die Zeiträume üblicher Schließungen der TU Braunschweig ausreichend.

# Organisatorische Maßnahmen

*(Dieser Abschnitt zahlt eindeutig auf die zu erstellenden und im System zur Dokumentation der Verfahrenstätigkeitsbeschreibungen benötigten (technischen und) organisatorischen Maßnahmen ein. Technisch-organisatorische Maßnahmen (TOM) dienen der Umsetzung einer sicheren Verarbeitung von personenbezogenen Daten. TOM müssen schriftlich dokumentiert werden, dies fordert die DS-GVO*

*Tipp: Elemente, die bei der Dokumentation von organisatorischen Maßnahmen vom Dokumentationssystem der TU abgefragt werden und die Sie nicht dieser Dokumentation – auch nicht als Referenz auf andere Maßnahmen und Systeme – entnehmen können, fehlen hier. Nutzen Sie dieses Wechselspiel, um Ihre IT-Verfahren und deren Dokumentation besser hinsichtlich Konformität und möglicher Kontrollen zu gestalten (nicht abschließend und insbes. Datenschutz, Informationssicherheit, Fernmelde- und Telekommunikationsrecht, Arbeitsrecht & Leistungskontrollverbot, Software und UrhG, IT-Strafrecht))*

## Dokumentation und Schulungen

*(Wo ist die Dokumentation abgelegt? Wie und ggf. in welchen Abständen wird diese überarbeitet? Welche Schulungen werden für (neue) Mitarbeitende angeboten und werden/müssen diese regelmäßig wiederholt? Dies ist zu klären sowohl für Anwendende/Mitarbeitende in Prozessen, die die Systeme administrierenden Personen. Siehe Abschnitt „Qualifizierungen und Schulungen“ der IT-Rahmen-DV.)*

## Datenfeldkatalog und Löschkonzept

*(Welche personenbezogenen und personenbeziehbaren Daten werden verwendet, welchen Datenkategorien sind diese zuzuordnen und mit welchen Fristen werden die Datenkategorien aus den Systemen wie (manuell, automatisiert) entfernt? In einer praktischen Umsetzung kann eine Excel-Tabelle mit den relevanten Datenfeldern, deren Kategorisierung mit Zuordnung zu Löschfristen eingebunden werden. Artikel 30 der DSGVO sieht vor, dass das Verzeichnis der Verarbeitungstätigkeiten die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien enthalten soll. Der Artikel 17 DSGVO formuliert ein Recht auf Löschung personenbezogener Daten. Deshalb ist immer dann, wenn mit personenbezogenen Daten gearbeitet wird ein Löschkonzept vorzusehen. Legen Sie daher fest, welche Daten wann zu löschen sind. Bedenken Sie, dass Betroffene ein Auskunftsrecht haben. Bestimmen Sie zunächst Datenkategorien und legen Sie Löschfristen fest. Gibt es Trigger oder Regeln für ein Löschen? Legen Sie klare Umsetzungen fest, wie genau gelöscht wird. Sie können sich auch an der DIN 66398 orientieren.)*

## Regelmäßige Revision des Betriebskonzeptes

*([Herkunft: mittellateinisch revisio = prüfende Wiederdurchsicht, zu lateinisch revisum]*[[1]](#footnote-1)*)*

Dieses Dokument soll in jährlichen Revisionsterminen oder anlassbezogen bei relevanten Veränderungen überprüft und fortlaufend weiterentwickelt werden.

# Gültigkeit und Dokumentenmanagement

Dieses Dokument tritt mit Freigabe durch die das IT-Verfahren betreibende OE-Leitung ohne Unterschrift in Kraft. Als für das IT-Verfahren verantwortliche OE-Leitung legt sie den Verteilerkreis fest und sorgt für die Verteilung der freigegebenen Version. Alle vorangehenden Versionen verlieren hiermit ihre Gültigkeit.

Dieses Dokument ist grundsätzlich nur für den internen Gebrauch bestimmt. Eine Weitergabe an Dritte bedarf der Legitimation durch die das IT-Verfahren betreibende OE-Leitung.

# Referenzen

*(Liste der referenzierten Richtlinien und Betriebskonzepte)*

# Anlagen

*(Hier können z.B. (ADV-)Dokumente oder Serviceverträge mit IT-Dienstleistern aufgenommen werden. Fügen Sie bei, was immer nötig ist, insbesondere wenn es Ihren Abläufen dienlich ist.)*

# Traffic Light Protocol

Zur Klassifikation wird das innerhalb des Landes Niedersachsen eingesetzte Traffic Light Protocol verwendet. Siehe auch <https://de.wikipedia.org/wiki/Traffic_Light_Protocol>

* **TLP:RED**: Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/ Audiokonferenz bzw. auf die direkten Empfangenden bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
* **TLP:AMBER**: Informationen dieser Stufe dürfen die Empfangenden innerhalb ihrer Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Die Empfangenden dürfen die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz der Empfangenden oder zur Schadensreduktion bei den Empfangenden benötigen. Hierfür muss sichergestellt sein, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln Traffic Light Protocol (TLP) einhalten. Die informationserstellende Person kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.
* **TLP:GREEN**: Informationen dieser Stufe dürfen innerhalb der Organisationen und anderen beteiligten Personen frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
* **TLP:WHITE**: Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

1. <https://www.duden.de/rechtschreibung/Revision> [↑](#footnote-ref-1)