



Informationsaustausch mit dem Traffic Light Protocol (TLP)

Verfahrensanweisung

der Carano Software Solutions GmbH



1 Dokumenteninformation und Dokumentenstatus

1.1 Dokumenteninformation

Dokumententyp:	Verfahrensanweisung
Verantwortlich:	Bereich: Verwaltung Bearbeiter: Tugay Calhan
Bearbeitet am:	2024-01-14
Freigeber:	Gordon Groth
Freigegeben am:	23.01.2024
Version:	1.0
Dokumentname	Carano_VA_Informationsaustausch_TLP.docx
Befristet gültig bis:	Unbegrenzt
TLP-Stufe	TLP: CLEAR
TLP-Informationsersteller	Carano Software Solutions GmbH
TLP-Adressaten	Carano Software Solutions GmbH
TLP- weiter einschränken	---

1.2 Dokumentenstatus

Version	Datum	Autor	Änderung	Status
1.0	2024-01-23	Gordon Groth	Inkrafttreten	<i>in Kraft gesetzt</i>
1.0	2024-01-23	Gordon Groth	Dokument freigegeben	<i>freigegeben</i>
0.4	2024-01-14	Gordon Groth	Überarbeitung und neue Dokumentenvorlage	<i>Entwurf</i>
0.3	2023-12-06	Tugay Calhan	Einarbeitung „Klassifizierung“	<i>Entwurf</i>
0.2	2023-11-08	Tugay Calhan	Formatierung	<i>Entwurf</i>
0.1	2023-10-01	Tugay Calhan	Initialer Entwurf	<i>Entwurf</i>

Inhalt

1	Dokumenteninformation und Dokumentenstatus.....	2
1.1	Dokumenteninformation	2
1.2	Dokumentenstatus.....	2
2	Grundsatz und Begriffe.....	4
2.1	Allgemeine Informationen.....	4
2.2	Begriffe	4
2.3	Grundsatz.....	5
3	TLP-Klassifizierungen	5
3.1	Klassifizierung der Weitergabebeschränkung.....	5
3.2	Klassifizierung.....	6
3.3	Kennzeichnung von Dokumenten.....	9
3.4	Benutzen von klassifizierten Informationen	11
3.5	Benachrichtigungspflicht	12
4	Inkrafttreten	12

2 Grundsatz und Begriffe

2.1 Allgemeine Informationen

Das Traffic Light Protocol (TLP) ist eine standardisierte Vereinbarung zum Austausch schutzwürdiger Informationen. Für die eindeutige Erkennbarkeit des gewünschten Schutzes der Information werden die zu klassifizierenden Dokumente in TLP-Stufen eingeteilt.

Mit den TLP-Stufen werden die Bedingungen für die Weitergabe der Information geregelt. In diesem Dokument werden die für Carano präzisierten Regeln erläutert.

Tragen Dokumente von Carano keine Kennzeichnung nach dieser Verfahrensanweisung, ist grundsätzlich eine Weitergabe als nicht geregelt anzusehen. Eine Weitergabe ist mit dem Dokumentersteller im Einzelfall abzustimmen. Das Fehlen einer TLP-Kennzeichnung bedeutet somit nicht, dass etwa die unbegrenzte Verbreitung **TLP:CLEAR** grundsätzlich gestattet ist.

Allgemeine Informationen zur TLP-Herkunft und sonstige Verwendungen sind zu finden unter: https://de.wikipedia.org/wiki/Traffic_Light_Protocol.

2.2 Begriffe

Als **Dokument** (synonym „Information“) wird jegliche gespeicherte Ansammlung von Worten, Zahlen oder Grafiken angesehen. Die Speicherung bezieht sich in diesem Fall in erster Linie auf schriftliche Dokumente, sprich als Datei, in elektronischen Kanälen oder auf Papier. Bei der Weitergabe von Audio- und Videomaterial ist sinngemäß zu verfahren. Bei Bedarf ist ein Begleitdokument mit Klassifizierungsmerkmalen nach dieser Verfahrensanweisung zu erstellen.

Im TLP-Informationsaustausch unterscheiden sich folgende Rollen:

- **Informationsersteller:** Ersteller und Absender der Information.
- **Adressaten:** Direkt adressierte Empfänger der Informationen. Diese können Personen, Teams oder Unternehmen sein.
- **Partner:** Partner der Adressaten. Unternehmen, die Geschäftsbeziehungen zum Adressaten haben, wie beispielsweise Lieferanten oder Dienstleister.

Zusätzlich genannte Rollen:

- **Dritte:** Nicht Adressaten und ohne Geschäftsbeziehung zu Adressaten.
- **Öffentlichkeit:** Alle Personen.

2.3 Grundsatz

Bei jeglicher Weiterleitung von Informationen gilt das Prinzip:
Teilen, nur wenn notwendig!

Das TLP dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen, in dem die zulässige Weitergabe der Informationen geregelt wird.

Die Regeln der TLP sind Sicherheitsmaßnahmen, die beim Teilen und Empfangen von TLP-klassifizierten Dokumenten einzuhalten sind. Zu klassifizierten Dokumenten zählen alle schriftlich erstellten Informationen. Bei jeder Weiterleitung muss gewährleistet werden, dass die weiteren Empfänger das TLP kennen und die damit verbundenen Regeln einhalten. Daher ist im Bedarfsfall zu empfehlen, allen Dokumenten eine Kurzfassung mit dem Dokument „Carano_VA_Informationsaustausch_TLP_Infoblatt“ beizulegen.

Dieses Dokument (Langfassung), wie auch das zuvor genannte Infoblatt (Kurzfassung) werden auf folgender Website zur Verfügung gestellt: <https://www.carano.de>

Wenn dem Adressaten oder Partner die Zulässigkeit der Weitergabe der Informationen nicht klar ist, soll vor Weiterleitung eine Nachfrage beim Informationsersteller erfolgen.

3 TLP-Klassifizierungen

3.1 Klassifizierung der Weitergabebeschränkung

Der Ersteller des Dokuments ist verantwortlich dafür, dass die Weitergabe von Informationen sinnvoll beschränkt wird. Die Weitergabe von Informationen soll auf den unbedingt notwendigen Adressatenkreis beschränkt werden. Andererseits muss eine effektive Verteilung von Informationen gewährleistet sein.

Welche der nachfolgend genannten Kennzeichnungen von Ersteller des Dokuments verwendet werden sollen, lässt sich anhand der Abschätzung von Folgen bei nicht gewünschter Weitergabe bestimmen. Als Beispiele seien genannt:

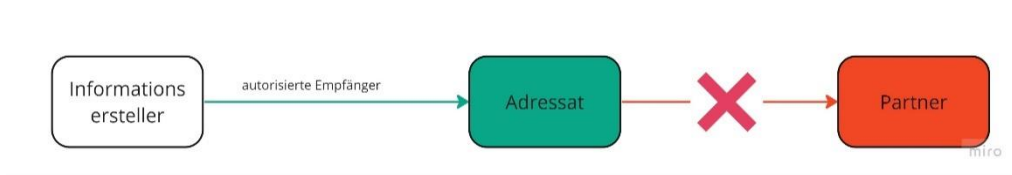
- **TLP:RED** Informationen, deren unberechtigte Weitergabe zur Verletzung der Privatsphäre von Personen, Verlust von Geschäftsgeheimnissen, existenzielle finanzielle Schäden, unberechtigter Zugang, u. ä. führen kann.
- **TLP:AMBER** vertrauliche Informationen über Geschäfte, Prozesse und Projekte mit Partnern u. ä.
- **TLP:GREEN** Informationen über mit den Partnern gemeinsam bearbeitete Projekte, Produktblätter, Beschreibungen, u. ä.
- **TLP:CLEAR** allgemein bekannte Fakten, Sachverhalte mit der gewünschten öffentlichen Verfügbarkeit, u. ä.

3.2 Klassifizierung

3.2.1 TLP:RED

TLP:RED Nur für den Adressaten

Informationen dieser Stufe sind ausschließlich für den Adressaten bestimmt. Die Weitergabe darüber hinaus ist untersagt. Beim TLP:RED muss im Dokument immer ein Adressat als Person, als Abteilung oder als Unternehmen angegeben werden.



Erläuterung zum Diagramm:

- **Persönlich:** Informationen, die mit TLP:RED eingestuft sind, sind streng vertraulich zu behandeln.
- **Ausschließlich für den Adressaten:** TLP:RED-Informationen sind ausschließlich für den Adressaten bestimmt.
- **Weitergabe an Partner oder Dritte untersagt:** Jegliche Weitergabe an Partner oder Dritte ist untersagt.

Die TLP:RED-Klassifikation wird in der Regel für sehr sensible Informationen verwendet, bei denen die höchsten Sicherheitsvorkehrungen erforderlich sind. Es soll sichergestellt werden, dass eine Information nur von den richtigen Personen gesehen wird.

Die TLP:RED-Klassifikation schließt elektronische Übermittlung nicht aus. Jedoch sind bei der Nutzung unsicherer Kommunikationssysteme (wie öffentlicher E-Mail-Versand) weitere Sicherheitsmaßnahmen (wie z.B. Verschlüsselung der Nachricht oder Postversand) einzusetzen.

Beispielangaben zum Informationsersteller, Adressaten von TLP:RED:

Informationsersteller: Person, Abteilung (o. Team), Unternehmen

Adressat:

nur 1 Person Person, Abteilung (o. Team), Unternehmen

oder 1 Gruppe Abteilung (o. Team), Unternehmen

oder 1 Firma Unternehmen

(siehe TLP:RED-Beispielbild in 3.2.1)

3.2.2 TLP:AMBER

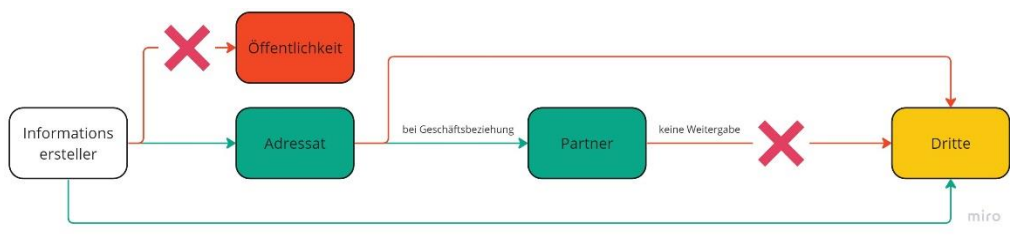
TLP:AMBER Eingeschränkte Weitergabe

Bei der Versendung muss ein Adressat angegeben werden. Falls der Informationsersteller keine zusätzlichen Einschränkungen anordnet, kann der Adressat die Informationen an einen seiner Partner (z.B. bei Geschäftsbeziehungen, ein Dienstleister oder ein Kunde) weitergeben. Nicht direkt adressierte Partner dürfen keine Weiterleitung vornehmen. Dritte dürfen die Information nicht erhalten. Eine Veröffentlichung ist untersagt.

Sollte eine Weitergabe an weitere Sub-Partner notwendig sein, ist beim Informationsersteller anzufragen. Der Informationsersteller wird dann die Information weiterleiten.

Der Informationsersteller kann zusätzliche Einschränkungen der Informationsweitergabe festlegen.

Die TLP:AMBER-Klassifikation schließt elektronische Übermittlung nicht aus. Jedoch sind bei der Nutzung unsicherer Kommunikationssysteme (wie öffentlicher E-Mail-Versand) weitere Sicherheitsmaßnahmen (wie z.B. Verschlüsselung der Nachricht oder Postversand) einzusetzen.



Erläuterung zum Diagramm:

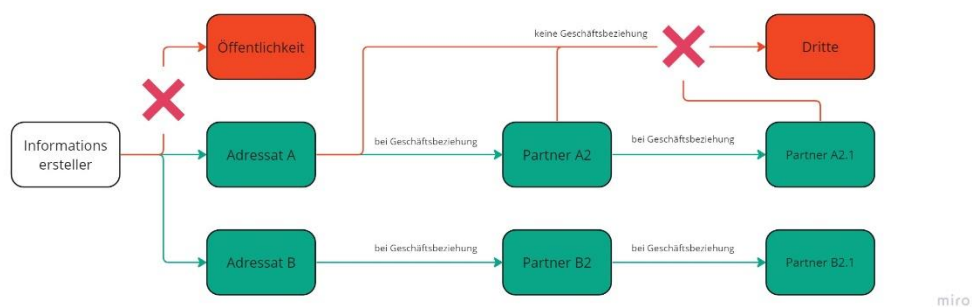
- **Weitergabe an Partner:** Adressaten können die Informationen an Partner – also bei Vorliegen von Geschäftsbeziehungen - weitergeben. Es sind ggf. zusätzliche Einschränkungen im Dokument zu beachten.
- **Keine Weitergabe durch Partner:** Allen Partnern – also Personen und Organisationen, die die Information erhalten, aber nicht Adressat sind - ist das Teilen der Information untersagt.
- **Nicht an die Öffentlichkeit:** Eine Veröffentlichung der Information ist untersagt.
- **Zusatzeinschränkungen möglich:** Der Informationsersteller kann zusätzliche Einschränkungen für die Informationsweitergabe festlegen. Üblich ist hier die Einschränkung des Kreises der Partner.

Die Einhaltung dieser TLP:AMBER-Klassifikation und Prinzipien stellt sicher, dass vertrauliche Informationen angemessen geschützt und in Situationen, in denen dies erforderlich ist, angemessen geteilt werden können.

3.2.3 TLP:GREEN

TLP:GREEN Organisationsübergreifende Weitergabe

Bei Versendung müssen ein oder können mehrere Adressaten angegeben werden. Die Adressaten sind hier in der Regel eine Organisation oder Organisationseinheit. Eine Weitergabe an Partner – also bei Vorliegen einer Geschäftsbeziehung – ist gestattet. Die Partner dürfen ihrerseits die Information an ihre Partner weitergeben. Eine Weitergabe an Dritte oder die Veröffentlichung sind nicht gestattet.



Erläuterung zum Diagramm:

- **Teilen an mehrere Adressaten möglich:** Ermöglicht es, Informationen an mehrere Adressaten zu senden.
- **Weitergabe an Partner:** Eine Weitergabe an Partner des Adressaten – also bei Vorliegen von Geschäftsbeziehungen – ist gestattet. Die Partner dürfen die Information ihrerseits an Partner weitergeben.
- **Öffentlichkeit und Dritte ist untersagt:** Eine Weitergabe Dritte oder eine Veröffentlichung sind untersagt.

Die Einhaltung dieser TLP:GREEN-Klassifikation stellt sicher, dass Informationen angemessen geschützt und breit genutzt werden.

3.2.4 TLP:CLEAR

TLP:CLEAR Unbegrenzte Weitergabe

Informationen können ohne Beschränkungen an Personen oder Organisationen weitergegeben werden. Es besteht keine Notwendigkeit für zusätzliche Sicherheitsvorkehrungen oder Schutzmaßnahmen.

Die TLP:CLEAR-Klassifikation wird für Informationen verwendet, die öffentlich zugänglich sind und daher keine besondere Vertraulichkeit erfordern.

3.3 Kennzeichnung von Dokumenten

3.3.1 Ein Dokument kennzeichnen

Ein Dokument wird nach TLP gekennzeichnet, indem vom Informationsersteller auf der ersten Seite des Dokuments und möglichst auf jeder Seite in der Kopfzeile eines der folgenden Labels angebracht wird:

* TLP: RED

TLP: AMBER

TLP: GREEN

TLP: CLEAR

Bei **TLP: RED** und **TLP: AMBER** sind zusätzlich folgende Angaben deutlich auf der ersten Seite des Dokuments, zu vermerken:

- Informationsersteller
- Adressat
- weiteren Einschränkungen der Weitergabe

Bei Dokumenten muss die TLP-Kennzeichnung eine gut lesbare Schriftgröße von mindestens 12pt haben.

Beispiel für eine TLP: RED-Kennzeichnung:

TLP: RED

carano
Software Solutions GmbH



TLP: RED Nur für Adressaten

(Beispielbild: TLP: RED Angaben)

3.3.2 Höchste TLP-Stufe gilt

Werden mehrere Informationen unterschiedlicher TLP-Stufen zusammen versendet, so sind sie entsprechend der höchsten vorliegenden TLP-Stufe zu behandeln.

3.3.3 Kennzeichnen bei elektronischen Informationen

Bei Anwendung der TLP-Kennzeichnung für **elektronischen Nachrichten** (E-Mails, ...) müssen Kennzeichnungen so erfolgen, dass sie für den Leser sofort deutlich erkennbar werden. Das TLP-Kennzeichen sollte direkt der Information vorangestellt werden.

Bei E-Mails ist zu empfehlen, dass das TLP-Kennzeichen vorangestellt im Betreff der E-Mail angegeben wird.

3.3.4 Farbcodes für TLP-Labels

TLP color-coding in RGB, CMYK und Hex:

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

3.4 Benutzen von klassifizierten Informationen

3.4.1 Elektronische Übertragung

Informationen der TLP-Stufen **TLP:RED** und **TLP:AMBER** müssen bei elektronischer Übertragung über ungeschützte Übertragungswege angemessen, z.B. durch Verschlüsselung, abgesichert werden.

3.4.2 Weitergabe an nicht genehmigten Empfängerkreis

Wird eine Weitergabe an weitere, nicht durch die Klassifikation abgedeckte, Empfänger gewünscht, so ist diese entweder durch den Informationsersteller selbst vorzunehmen oder mindestens vorab durch den Informationsersteller zu genehmigen.

3.4.3 Nutzung von öffentlichen Plattformen unterlassen

Mit **TLP:RED**, **TLP:AMBER** oder **TLP:GREEN** klassifizierte Dokumente dürfen weder manuell noch automatisiert auf Plattformen Dritter hochgeladen werden. Das betrifft beispielsweise „kostenlose“ Online-Virustools, Sprachübersetzer, nicht dienstlich genutzte Online-Speicher und weitere Werkzeuge, da die Dokumente dort Dritten zugänglich werden können.

3.4.4 Vervielfältigung vermeiden

Die Vervielfältigung von **TLP:AMBER** und **TLP:RED**-Informationen muss auf das unbedingt notwendige Maß beschränkt werden. Kopien sind genauso zu behandeln, wie die Originaldokumente einschließlich ihrer Kennzeichnung, Aufbewahrung, Weitergabe und Vernichtung.

3.4.5 Aufbewahrung

Informationen der TLP-Stufe **TLP:AMBER** und **TLP:RED** sollen auf mobilen Endgeräten auf verschlüsselten Speichern oder alternativ sonst pro Dokument verschlüsselt aufbewahrt werden.

Papierdokumente der TLP-Stufen **TLP:AMBER** oder **TLP:RED** sollen in einem verschlossenen Behältnis aufbewahrt werden.

3.4.6 Vernichtung, Löschung und Aussonderung

Datenträger, auf denen Informationen der TLP-Stufen **TLP:AMBER** oder **TLP:RED** gespeichert wurden, müssen vor Aussonderung sicher gelöscht oder die Datenträger irreversibel physisch vernichtet werden.

Papierdokumente der TLP-Stufen **TLP:AMBER** oder **TLP:RED** müssen in geeigneten Aktenvernichtern vernichtet werden.

3.5 Benachrichtigungspflicht

Wenn die Information anderen Personen, als die durch die TLP-Kennzeichnung definierten Adressaten bekannt wurde oder der begründete Verdacht des Bekanntwerdens besteht, dann ist, zum Vermeiden möglicher Schäden durch eine Verletzung der Informationssicherheit, der Informationsersteller zu informieren.

Unter www.carano.de sind die für eine Meldung relevanten Kontaktdaten zu finden.

4 Inkrafttreten

Dieses Dokument tritt in Kraft mit dem im Dokumentenstatus unter dem Status "in Kraft gesetzt" letzten angegebenen Datum und der dortigen Versionsnummer.