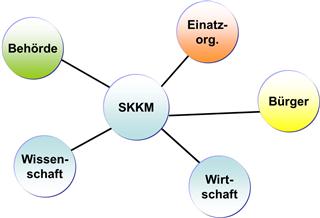
**Zivilschutz in Österreich**

**Staatliches Krisen- und Katastrophenschutzmanagement (SKKM)**

Hauptakteure im österreichischen Katastrophenmanagement © Siegfried Jachs, BMI

Die Abwehr, Beseitigung oder Linderung der Auswirkungen drohender oder eingetretener Katastrophen (Katastrophenhilfe, Einsatzvorsorgen) ist in Österreich überwiegend eine Angelegenheit der Bundesländer. Die rechtliche Basis bilden die Katastrophenhilfegesetze der Länder, die vor allem die Feststellung der Katastrophe und die behördliche Einsatzleitung in den Gemeinden, Bezirken und Ländern festlegen.

Bei Krisen und Katastrophen besteht erhöhter Koordinationsbedarf, der in Österreich durch das SKKM gewährleistet wird. Die Geschäftsstelle ist im BMI angesiedelt. Das SKKM ermöglicht eine effiziente Katastrophenhilfe im In- und Ausland, durch die Zusammenarbeit aller zuständigen Stellen des Bundes mit den Katastrophenschutzbehörden der Länder sowie den Hilfs- und Rettungsorganisationen.

Quelle: BMI Krisen- und Katastrophenmanagement

 [[](https://moodle.spengergasse.at/mod/resource/view.php?id=151079)SKKM - Führen im Katastropheneinsatz in Österreiche (verkürzt) Datei](https://moodle.spengergasse.at/mod/resource/view.php?id=151079)

** Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP)**

Das österreichische Programm zum Schutz kritischer Infrastrukturen (Austrian Program for Critical Infrastructure Protection - APCIP) beschreibt den strategischen und konzeptuellen Rahmen, die Prinzipien und strategischen Zielsetzungen und die Handlungsfelder und Maßnahmen zum Schutz kritischer Infrastruktur.

Kritische Infrastrukturen sind nach APCIP: *„Kritische Infrastrukturen im Sinne dieses Masterplans sind jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon), die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde.“*

Der Masterplan APCIP nutzt als Grundlage die Prinzipien Kooperation, Subsidiarität, Komplementarität, Vertraulichkeit und Verhältnismäßigkeit und basiert auf einem All-hazards-Ansatz. *(Unter dem All-Hazards-Ansatz wird ein Ansatz verstanden, der im Rahmender Sicherheitsvorsorge das gesamte Spektrum der potenziellen Bedrohungen umfasst.)* Der Fokus des Masterplans ist die Unterstützung von strategischen Unternehmen beim Aufbau einer umfassenden Sicherheitsarchitektur (Risikomanagement, Business Continuity Management und Sicherheitsmanagement).

Das Programm soll langfristig zur Steigerung der Resilienz und Sicherheit in Österreich beitragen. Resilienz wird in APCIP beschrieben als: *„die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, welche(s) Gefahren ausgesetzt ist,* *deren Folgen zeitgerecht und wirkungsvoll zu bewältigen, mit ihnen umzugehen, sich ihnen* *anzupassen und sich von ihnen zu erholen, auch durch Bewahrung und Wiederherstellung* *seiner bzw. ihrer wesentlichen Grundstrukturen und Funktionen.“*

** Traffic Light Protocol (TLP)**

Das Ampelprotokoll wurde geschaffen, um das Teilen sensibler Informationen zwischen Organisationen zu fördern. Der Absender muss signalisieren, inwieweit seine Informationen über den unmittelbaren Empfänger hinaus weitergegeben werden sollen, wenn überhaupt.

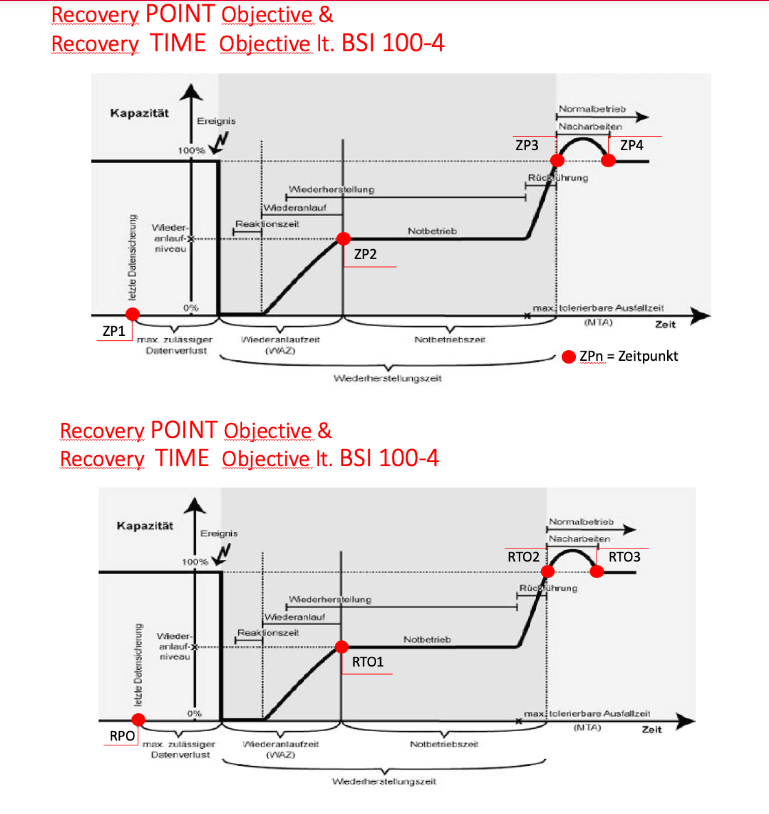
Das Ampelprotokoll basiert auf dem Konzept, dass der Absender Informationen mit einer von vier Farben kennzeichnet, um anzugeben, inwiefern die Informationen durch den Empfänger weitergegeben werden können. Der Empfänger muss den Absender konsultieren, wenn eine Weitergabe erforderlich ist.

**Die vier Farben und ihre Bedeutung sind wie folgt:**

* **ROT** – Privat und nur für die genannten Empfänger bestimmt. Im Rahmen einer Besprechung zum Beispiel sind rot gekennzeichnete Informationen auf die Anwesenden beschränkt. In den meisten Fällen werden die rot gekennzeichneten Informationen mündlich oder persönlich weitergegeben.
* **GELB** – Begrenzte Weitergabe. Der Empfänger darf gelb gekennzeichnete Informationen an andere Personen in seiner Organisation weitergeben, allerdings nur, wenn diese unbedingt in Kenntnis gesetzt werden müssen. Es wird möglicherweise vom Absender erwartet, dass er die Grenzen der Weitergabe angibt.
* **GRÜN** – Für die gesamte Gemeinschaft. Informationen in dieser Kategorie können innerhalb einer bestimmten Gemeinschaft weitergegeben werden. Die Informationen dürfen jedoch weder im Internet noch anderweitig veröffentlicht oder außerhalb der Gemeinschaft preisgegeben werden.
* **WEISS** – Unbegrenzt. Vorbehaltlich der üblichen Urheberrechtsbestimmungen dürfen weiß gekennzeichnete Informationen frei und ohne Einschränkung weitergegeben werden.

Sensible Informationen, wie auch immer sie von einem Absender bereitgestellt werden, sollten zum Zeitpunkt der Offenlegung in Übereinstimmung mit dem Ampelprotokoll gekennzeichnet sein. Alle sensiblen Informationen gelten als mit gelber Kennzeichnung versehen, sofern nichts anderes angegeben oder schriftlich mitgeteilt wird. Standardmäßig und sofern zum Zeitpunkt der Offenlegung keine anderslautenden Festlegungen bestehen, wird die Identität der Quelle der sensiblen Informationen jedoch immer rot gekennzeichnet sein.

**RPO / RTO**



RTO1 = Notbetrieb vorhanden

RTO2= Betrieb + Restore der letzten Datensicherung vorhanden

RTO3 =Betrieb + Restore + Daten nach erfasst