

Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV)

vom 4. Juli 2007

Der Schweizerische Bundesrat,

gestützt auf die Artikel 8 Absatz 1 und 43 Absatz 2 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997¹ (RVOG)
sowie auf Artikel 150 Absatz 3 des Militärgesetzes vom 3. Februar 1995² (MG),
verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

¹ Diese Verordnung regelt den Schutz von Informationen des Bundes und der Armee, soweit er im Interesse des Landes geboten ist. Sie legt insbesondere deren Klassifizierung und Bearbeitung fest.

² Vorbehalten bleiben spezialgesetzliche Bestimmungen.

Art. 2 Geltungsbereich

Diese Verordnung gilt für:

- a. die Bundesverwaltung nach Artikel 6 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998³;
- b. die Angehörigen der Armee;
- c. Organisationen und Personen des öffentlichen oder privaten Rechts, die klassifizierte Informationen bearbeiten, soweit dies im Bundesrecht vorgesehen ist oder entsprechend vereinbart wurde;
- d. eidgenössische und kantonale Gerichte, die klassifizierte Informationen bearbeiten, soweit dies im Bundesrecht vorgesehen ist.

SR 510.411

¹ **SR 172.010**

² **SR 510.10**

³ **SR 172.010.1**

Art. 3 Begriffe

In dieser Verordnung bedeuten:

- a. Informationen:
Aufzeichnungen auf Informationsträgern und mündliche Äusserungen;
- b. Informationsträger:
Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger;
- c. Bearbeiten:
jeder Umgang mit Informationen, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Erstellen, Benützen, Verarbeiten, Kopieren, Zugänglichmachen, Bekanntgeben, Übermitteln, Zur-Kennntnis-Nehmen, Aufbewahren, Archivieren und Vernichten;
- d. Verfasserin oder Verfasser:
Person, Verwaltungseinheit, Kommandostelle oder Auftragnehmer, der oder die klassifizierte Informationen erstellt;
- e. Geheimnisträgerin oder Geheimnisträger:
Person, der klassifizierte Informationen anvertraut wurden;
- f. Klassifizieren:
eine konkrete Information dem Klassifizierungskatalog (Art. 8) entsprechend beurteilen und mit dem Klassifizierungsvermerk formell kennzeichnen;
- g. Entklassifizieren:
den Klassifizierungsvermerk nach Wegfall der Schutzwürdigkeit streichen;
- h. Informatik- und Telekommunikationssysteme:
Systeme und die auf ihnen vorhandenen Anwendungen und Datensammlungen;
- i. Informatiksicherheit:
die Informatiksicherheit stellt die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit bei der elektronischen Bearbeitung von Informationen sicher;
- j. Codierung:
Anwendung von Umschreibungen und Decknamen;
- k. Verschlüsselung:
technische Umformung von Klartext, welche eine dem Stand der Technik entsprechende Qualität aufweist.

2. Abschnitt: Klassifizierungen

Art. 4 Klassifizierungsstufen

¹ Wer schutzwürdige Informationen verfasst oder herausgibt, weist sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu:

- a. GEHEIM;
- b. VERTRAULICH;
- c. INTERN.

² Werden Informationsträger physisch zu einem Sammelwerk zusammengefasst, ist zu überprüfen, ob dieses klassifiziert oder einer höheren Klassifizierungsstufe zugeordnet werden muss.

Art. 5 GEHEIME Informationen

¹ Als GEHEIM werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen schweren Schaden zufügen kann. Dabei handelt es sich namentlich um Informationen, deren Bekanntwerden:

- a. die Handlungsfähigkeit der Bundesversammlung oder des Bundesrats schwerwiegend gefährden kann;
- b. die Sicherheit der Bevölkerung schwerwiegend gefährden kann;
- c. die wirtschaftliche Landesversorgung oder die Sicherheit von landeswichtigen Führungs- und Infrastrukturanlagen schwerwiegend gefährden kann;
- d. die Aufgabenerfüllung der Bundesverwaltung, der Armee oder wesentlicher Teile davon schwerwiegend gefährden kann;
- e. die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz schwerwiegend gefährden kann;
- f. den Quellen- oder den Personenschutz oder die Geheimhaltung von operativen Mitteln und Methoden der Nachrichtendienste schwerwiegend gefährden kann.

² Träger von als GEHEIM klassifizierten Informationen sind zu nummerieren.

Art. 6 VERTRAULICHE Informationen

¹ Als VERTRAULICH werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte den Landesinteressen Schaden zufügen kann. Dabei handelt es sich namentlich um Informationen, deren Bekanntwerden:

- a. die freie Meinungs- und Willensbildung der Bundesversammlung oder des Bundesrats beeinträchtigen kann;
- b. die zielkonforme Durchführung konkreter behördlicher Massnahmen beeinträchtigen kann;
- c. die Sicherheit der Bevölkerung beeinträchtigen kann;

- d. die wirtschaftliche Landesversorgung oder die Sicherheit von wichtigen Infrastrukturanlagen beeinträchtigen kann;
- e. die Aufgabenerfüllung von Teilen der Bundesverwaltung oder von Teilen der Armee beeinträchtigen kann;
- f. die aussenpolitischen Interessen oder internationalen Beziehungen der Schweiz beeinträchtigen kann;
- g. die Beziehungen zwischen Bund und Kantonen oder zwischen Kantonen beeinträchtigen kann;
- h. wirtschafts-, geld- und währungspolitische Interessen der Schweiz beeinträchtigen kann.

² Informationsträger mit als VERTRAULICH klassifizierten Informationen können nummeriert werden.

Art. 7 INTERNE Informationen

¹ Als INTERN werden folgende Informationen klassifiziert:

- a. Informationen, die dem Amts-, Berufs-, Geschäfts- oder Fabrikationsgeheimnis unterliegen und einen erhöhten Informationsschutz benötigen, sofern sie weder GEHEIM noch VERTRAULICH klassifiziert werden müssen;
- b. Informationen der Armee, die dem Dienstgeheimnis unterliegen.

² Als «RESTRICTED» oder gleichwertig klassifizierte Informationen aus dem Ausland werden wie als INTERN klassifizierte Informationen bearbeitet.

Art. 8 Klassifizierungskatalog

Die Koordinationsstelle für den Informationsschutz im Bund (Art. 20) legt in einem Klassifizierungskatalog fest, wie gewisse häufig anfallende schutzwürdige Informationen des Bundes zu klassifizieren sind.

Art. 9 Befristete Klassifizierung

Die Klassifizierung ist zu befristen, wenn voraussehbar ist, wann die Schutzwürdigkeit dahinfallen wird.

3. Abschnitt: Geheimnisträgerinnen und Geheimnisträger

Art. 10 Anforderungen

¹ Personen, die aufgrund ihres Aufgabenbereiches Zugang zu klassifizierten Informationen erhalten sollen, sind:

- a. sorgfältig auszuwählen;
- b. zur Geheimhaltung zu verpflichten; und
- c. entsprechend aus- und weiterzubilden.

² Ob sich Geheimnisträgerinnen und Geheimnisträger, die Zugang zu als GEHEIM oder als VERTRAULICH klassifizierten Informationen erhalten sollen, einer Personensicherheitsprüfung unterziehen müssen, richtet sich nach der Verordnung vom 19. Dezember 2001⁴ über die Personensicherheitsprüfungen.

Art. 11 Aus- und Weiterbildung

Die Fachkenntnisse von Geheimnisträgerinnen und Geheimnisträgern im Bereich des Informationsschutzes und der Informatiksicherheit sind sicherzustellen und periodisch zu aktualisieren.

Art. 12 Verantwortung

¹ Wer klassifizierte Informationen bearbeitet, ist für die Einhaltung der Informationsschutzvorschriften verantwortlich.

² Die Vorgesetzten überprüfen regelmässig die Einhaltung dieser Vorschriften.

4. Abschnitt: Bearbeitung von klassifizierten Informationen

Art. 13 Grundsätze

¹ Die Erstellung, die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sind auf ein Minimum zu beschränken; dabei sind Lage, Auftrag, Zweck und Zeit zu berücksichtigen.

² Klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen.

³ Bei Gesuchen um Zugang zu amtlichen Dokumenten überprüft die zuständige Stelle, unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang nach dem Bundesgesetz vom 17. Dezember 2004⁵ über das Öffentlichkeitsprinzip der Verwaltung zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist.

⁴ Die Bearbeitung klassifizierter Informationen aus dem Ausland richtet sich nach dem entsprechenden Informationsschutzabkommen. Liegt kein solches vor, so richtet sich die Bearbeitung nach den Bearbeitungsvorschriften der mit der ausländischen Klassifizierungsstufe äquivalenten schweizerischen Klassifizierung.

⁴ SR 120.4

⁵ SR 152.3

Art. 14 Überprüfung von Schutzwürdigkeit und Verteiler

Die Verfasserin oder der Verfasser einer als VERTRAULICH klassifizierten und nummerierten oder einer als GEHEIM klassifizierten Information überprüft deren Schutzwürdigkeit und den Verteiler mindestens alle fünf Jahre und immer im Rahmen der Anbietepflicht an das Bundesarchiv.

Art. 15 Schutz bei falscher oder fehlender Klassifizierung

¹ Wer vermutet oder feststellt, dass Informationen offensichtlich falsch oder fälschlicherweise nicht klassifiziert sind, hat deren Schutz bis zur Änderung der Klassifizierung sicherzustellen.

² Sie oder er benachrichtigt unverzüglich die Verfasserin oder den Verfasser. Diese oder dieser trifft sofort die erforderlichen Massnahmen.

Art. 16 Meldung bei Verlust, Missbrauch oder Gefährdung

¹ Wer feststellt, dass klassifizierte Informationen gefährdet, abhanden gekommen oder missbraucht worden sind, trifft Schutzmassnahmen und informiert unverzüglich die vorgesetzte Person, die Verfasserin oder den Verfasser und die zuständigen Sicherheitsorgane.

² Die Verfasserin oder der Verfasser trifft in Absprache mit den zuständigen Sicherheitsorganen sofort die erforderlichen Massnahmen.

Art. 17 Archivierung

Die Archivierung klassifizierter Informationen richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

Art. 18 Bearbeitungsvorschriften

¹ Die Bearbeitung klassifizierter Informationen und der Umgang mit entsprechenden Informationsträgern sind im Anhang geregelt.

² Die Koordinationsstelle für den Informationsschutz im Bund (Art. 20) erlässt detaillierte Bearbeitungsvorschriften.

³ Sie regelt die vereinfachte Handhabung im Bereich von Informationen der Nachrichtendienste und der Polizei nach deren Bedürfnissen und unter Wahrung eines hinreichenden Informationsschutzes nach dieser Verordnung.

5. Abschnitt: Sicherheitsorgane**Art. 19** Informationsschutzbeauftragte

¹ Die Departemente und die Bundeskanzlei bezeichnen je eine Informationsschutzbeauftragte oder einen Informationsschutzbeauftragten.

² Die Informationsschutzbeauftragten nehmen insbesondere folgende Aufgaben wahr:

- a. Sie sorgen für die Umsetzung des Informationsschutzes in ihrem Zuständigkeitsbereich.
- b. Sie kontrollieren periodisch das Vorhandensein und die Vollständigkeit der als GEHEIM klassifizierten Informationsträger.

Art. 20 Koordinationsstelle für den Informationsschutz im Bund

¹ Die Informations- und Objektsicherheit im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport betreibt die Koordinationsstelle für den Informationsschutz im Bund (Koordinationsstelle).

² Die Koordinationsstelle gibt sich im Einvernehmen mit den Departementen und der Bundeskanzlei ein Geschäftsreglement, in dem die Einzelheiten ihrer Organisation und ihrer Tätigkeit geregelt sind.

³ Sie nimmt in Zusammenarbeit mit den Informationsschutzbeauftragten der Departemente und der Bundeskanzlei insbesondere folgende Aufgaben wahr:

- a. Sie erlässt die nötigen fachtechnischen Weisungen, namentlich den Klassifizierungskatalog (Art. 8) und die detaillierten Bearbeitungsvorschriften (Art. 18).
- b. Sie legt die Vorgaben für die Ausbildung der Geheimnisträgerinnen und Geheimnisträger fest und erstellt die notwendigen Ausbildungshilfsmittel.
- c. Sie kann Kontrollen und die in völkerrechtlichen Verträgen vorgesehenen Sicherheitsinspektionen durchführen.
- d. Sie ist Ansprechstelle im internationalen und nationalen Verkehr.
- e. Sie erstattet dem Sicherheitsausschuss des Bundesrats jährlich Bericht.

6. Abschnitt: Schlussbestimmungen

Art. 21 Vollzug

Die Departemente und die Bundeskanzlei vollziehen diese Verordnung.

Art. 22 Aufhebung und Änderung bisherigen Rechts

¹ Es werden aufgehoben:

- a. die Verordnung vom 10. Dezember 1990⁶ über die Klassifizierung und Behandlung von Informationen im zivilen Verwaltungsbereich;
- b. die Verordnung vom 1. Mai 1990⁷ über den Schutz militärischer Informationen (Informationsschutzverordnung).

⁶ AS 1991 44, 1999 2424

⁷ AS 1990 887, 1999 2424

² Die Bundesinformatikverordnung vom 26. September 2003⁸ wird wie folgt geändert:

Art. 16 Abs. 2 Bst. h

² Mitglieder mit beratender Stimme sind der Vertreter oder die Vertreterin:

h. der Koordinationsstelle für den Informationsschutz im Bund.

Art. 17 Abs. 3^{bis}

^{3bis} Er koordiniert seine Tätigkeit mit der Koordinationsstelle für den Informationsschutz im Bund.

Art. 23 Übergangsbestimmungen

¹ Der Klassifizierungsvermerk INTERN ist nur auf Informationsträgern anzubringen, welche nach dem Inkrafttreten dieser Verordnung erstellt werden.

² Technische Anpassungen für die Gewährleistung des Schutzes von Informationen, insbesondere für deren Klassifizierung und Bearbeitung, sind bis zum 31. Dezember 2009 vorzunehmen.

Art. 24 Inkrafttreten

Diese Verordnung tritt am 1. August 2007 in Kraft und gilt längstens bis zum 31. Dezember 2011.

4. Juli 2007

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Micheline Calmy-Rey

Die Bundeskanzlerin: Annemarie Huber-Hotz

Anhang
(Art. 18 Abs. 1)⁹

Bearbeitungsvorschriften

	GEHEIM	VERTRAULICH	INTERN	Zuständig
Erstellung				
Mittel (vorbehalten bleiben die im Rahmen des Vollzuges der V vom 29. Aug. 1990 ¹⁰ über das Geheimschutzver- fahren bei Aufträgen mit militärisch klassifiziertem Inhalt vereinbarten Regelungen)	elektronisch: nur mit von der Koordinationsstelle bewilligten Mitteln	elektronisch: nur mit von der Koordinationsstelle bewilligten Mitteln (Ausnahme: Armee)	beliebig	Verfasser
Klassifizierungsvermerk	Vermerk GEHEIM auf jeder Seite	Vermerk VERTRAULICH auf jeder Seite	Vermerk INTERN auf jeder Seite	
Nummerierung	zwingend	fakultativ	keine	
Registrierung	Formulare der Koordinationsstelle	Verteiler	fakultativ	

⁹ Vgl. auch die detaillierten Bearbeitungsvorschriften der Koordinationsstelle (Art. 18 Abs. 2).
¹⁰ SR 510.413

	GEHEIM	VERTRAULICH	INTERN	Zuständig
Speicherung bzw. Aufbewahrung				
elektronisch	Nur auf von der Koordinationsstelle bewilligten Mitteln; verschlüsselt auf Arbeitsplatzsystemen oder verschlüsselt auf entfernbaren Datenträgern Schlüssel sind getrennt von der verschlüsselten Information und unter Verschluss aufzubewahren	Verschlüsselt auf Arbeitsplatzsystemen oder auf entfernbaren Datenträgern	darf nur Berechtigten zugänglich sein	Verfasser bzw. Geheimnisträger
physisch	Tresor	Sicherheitsbehältnis	darf nur Berechtigten zugänglich sein	
Übermittlung bzw. Versand und Empfang				
Telefon, Mobiltelefon	Verschlüsselung oder geschützter Übertragungsweg oder Sicherheitskonzept	Codiert oder verschlüsselt	Codiert bzw. Bundesnetz	Verfasser bzw. Geheimnisträger
Fax	Verschlüsselung oder geschützter Übertragungsweg oder Sicherheitskonzept	Verschlüsselung oder geschützter Übertragungsweg oder Sicherheitskonzept	zulässig	
E-Mail (bzw. Anhang derselben)	Verschlüsselt und nachvollziehbar	Verschlüsselt	Zulässig, Schutz notwendig, z. B. Bundesnetz	
Datenübertragung	Verschlüsselung oder geschützter Übertragungsweg	Verschlüsselung oder geschützter Übertragungsweg	Zulässig, Schutz notwendig, z. B. Bundesnetz	
Mündliche Äusserungen	Nur gegenüber Berechtigten, in abhörsicheren Bereichen			

	GEHEIM	VERTRAULICH	INTERN	Zuständig
Übermittlung bzw. Versand und Empfang				
Persönliche Übergabe	nur gegen Quittung zulässig	zulässig, bei nummerierten Exemplaren nur gegen Quittung	zulässig	Verfasser bzw. Geheimnisträger
Post, Kurier	eingeschränkt und nur mit Spezialkurier des Bundes zulässig	eingeschränkt zulässig, bei nummerierten Exemplaren eingeschrieben	eingeschränkt zulässig	
Benützung				
Bearbeitung mit Informatikmitteln (vorbehalten bleiben die im Rahmen von Geheimschutzverfahren vereinbarten Regelungen)	Nur mit von der Koordinationsstelle bewilligten Mitteln und unter Verwendung von Sicherheitssoftware gemäss Bundesstandard	Nur mit von der Koordinationsstelle bewilligten Mitteln (Ausnahme: Armee) und unter Verwendung von Sicherheitssoftware gemäss Bundesstandard	Zulässig	Verfasser bzw. Geheimnisträger
Drucken	Eingeschränkt zulässig	Eingeschränkt zulässig	Zulässig	
Kopieren	Eingeschränkt und nur mit Bewilligung des Verfassers zulässig	Eingeschränkt zulässig	Zulässig	
Mitnahme ab dauerndem Standort	Eingeschränkt zulässig	Eingeschränkt zulässig	Zulässig	
Informationsverwaltung				
Regelmässige Überprüfung der Klassifizierung und des Verteilers	mindestens alle fünf Jahre und immer im Rahmen der Anbieterpflicht an das Bundesarchiv (Art. 14)	nur für nummerierte Exemplare: mindestens alle fünf Jahre und immer im Rahmen der Anbieterpflicht an das Bundesarchiv (Art. 14)	keine	Verfasser

	GEHEIM	VERTRAULICH	INTERN	Zuständig
Rückzug und Rückgabepflicht	zwingend	zwingend wenn nummeriert	keine	Verfasser bzw. Geheimnisträger
Archivierung	Anbietepflicht gemäss Archivierungsgesetzgebung (Art. 17).			Verfasser bzw. Geheimnisträger
Vernichtung bzw. Löschung (soweit nach Archivierungsgesetzgebung keine Ablieferungspflicht besteht)	Vernichtung nur durch Verfasser und eingeschränkt zulässig	Eingeschränkt zulässig, bei nummerierten Exemplaren nur durch den Verfasser	Eingeschränkt zulässig	