Reglement über den Zugang und die Benutzung der digitalen Plattform SIROUT (ReSi)

vom 08.07.2026 (Stand 01.07.2026)

Der Staatsrat des Kantons Wallis

eingesehen Artikel 16 bis 19 des Ausführungsgesetzes über die Bundesgesetzgebung betreffend den Strassenverkehr vom 12. Juni 2025 (AGSVG);

eingesehen das Reglement der Kantonalen Kommission für Strassensignalisation vom 16. Februar 2025 (RKKSS):
auf Antrag des für die Mobilität zuständigen Departements,

verordnet: [1)]

1 Allgemeine Bestimmungen

Art. 1 Gegenstand und Geltungsbereich

[1] Das vorliegende Reglement regelt die Zugangs- und Benutzungsmodalitäten für die digitale Plattform SIROUT im Sinne der Artikel 16 bis 19 des Ausführungsgesetzes über die Bundesgesetzgebung betreffend den Strassenverkehr (AGSVG) (nachfolgend: SIROUT). SIROUT ermöglicht der zuständigen Behörde im Sinne von Artikel 5 des Reglements der Kantonalen Kommission für Strassensignalisation (RKKSS) (nachfolgend: zuständige Behörde) die Behandlung von Dossiers, die die in Artikel 9, 12 und 13 RKKSS vorgesehenen Verfahrenshandlungen betreffen.

[2] Es gilt für alle in den Artikeln 9, 12 und 13 RKKSS vorgesehenen Verfahrenshandlungen, die über SIROUT behandelt werden.

[3] Alle SIROUT-Benutzer unterstehen dem vorliegenden Reglement.

[1)] Im vorliegenden Reglement gilt jede Bezeichnung der Person, des Status oder der Funktion in gleicher Weise für Mann oder Frau.

* Änderungstabellen am Schluss des Erlasses

Art. 2 Begriffe

[1] Im Sinne dieses Reglements versteht man unter:

a) Authentifizierung: Vorgang, der darin besteht, mittels der beim Identifizierungsvorgang gespeicherten Daten die Identität eines Benutzers zu verifizieren und nachzuweisen, bevor diesem der Zugang zu Ressourcen wie seinem Benutzerkonto oder seinen Dokumenten gewährt wird;

b) elektronische Kommunikationskanäle: Mittel zur Übertragung elektronischer Informationen zwischen einem Absender und einem Empfänger, namentlich E-Mail, Dokumentendownload, Zugang durch eine Web-Applikation usw.;

c) Benutzerkonto: zur Verfügung gestelltes Zugangsrecht zu SIROUT, das mit einem Benutzernamen, einer Rolle und einem Passwort verknüpft ist;

d) vertraulich: Eigenschaft von Daten, die vor dem unberechtigten Zugriff Dritter, sei es von Gesetzes wegen oder aufgrund einer behördlichen Verfügung, geschützt werden müssen;

e) Identifizierung: Vorgang, um die physische und die digitale Identität eines Benutzers auf deren Übereinstimmung hin sicher prüfen zu können und ihn mit seinen Daten zu verknüpfen, um ihn sodann zu authentifizieren;

f) elektronisches Identifikationsmittel (nachfolgend: e-ID): elektronisches Mittel zur Identifizierung und Authentifizierung eines Benutzers, von dem es zwei Stufen gibt:

   1. überprüft gemäss Stufe 1: erfordert einen gültigen Ausweis, der vom Anbieter der e-ID anerkannt wird, und eine gültige E-Mail-Adresse,

   2. überprüft gemäss Stufe 2: erfordert einen Pass, der vom Anbieter der e-ID anerkannt wird, und eine gültige E-Mail-Adresse;

g) SIROUT: Gesamtheit der Hardware- und Software-Komponenten des Informationssystems, das die Verwaltung oder Nutzung digitaler Dienstleistungen für die Bearbeitung von Gesuchen im Zusammenhang mit der Signalisation und Markierung auf öffentlichen Strassen ermöglichen;

h) Datensicherheit: Gesamtheit der organisatorischen Massnahmen (Informationssicherheit) und der technischen Massnahmen (operative Sicherheit) zum Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit der Informationen, Daten und Informatiksysteme der zuständigen Behörde; es können auch andere Eigenschaften, wie die Authentizität, die Zurechenbarkeit, die Nichtabstreitbarkeit, die Einhaltung von Gesetzen und Standards sowie die Zuverlässigkeit betroffen sein; diese Massnahmen schliessen die organisatorischen Massnahmen zum Schutz des Informationsbestandes ein, insbesondere die Zugriffsverwaltung;

i) Datenschutzsystem: Gesamtheit der Massnahmen und Prozesse zum Schutz der persönlichen und vertraulichen Daten;

j) Benutzer: Jede natürliche Person, die SIROUT in welcher Funktion auch immer nutzt;

k) Bestätigung: Vorgang, bei welchem der Benutzer auf SIROUT die Schaltfläche «Einreichen» betätigt.

2 Zugangs- und Benutzungsmodalitäten

Art. 3 SIROUT

[1] Für den Zugang zu SIROUT ist eine Internetverbindung erforderlich. Der Zugang erfolgt über die offizielle Website des Kantons Wallis, auf der Seite der Kantonalen Kommission für Strassensignalisation.

[2] Bei seinem ersten Login muss sich jeder Benutzer mit einer e-ID, die er zuvor bezogen hat, identifizieren, damit er sein Benutzerkonto erstellen und seine elektronische Kennung erhalten kann. Die Liste der auf SIROUT zugelassenen eID wird auf der Website des Kantons Wallis publiziert.

[3] Der Benutzer muss über Folgendes verfügen:

a) eine gemäss Stufe 1 überprüfte e-ID, um alle Aktionen innerhalb von SIROUT auszuführen, insbesondere die Einreichung und Verwaltung von Dossiers;

b) eine gemäss Stufe 2 überprüfte e-ID, um eine qualifizierte elektronische Signatur für Entscheide anzubringen.

[4] Sobald der Identifizierungsprozess abgeschlossen ist, wird die vom Benutzer erzeugte eID mit einem Benutzerkonto verknüpft, das den Zugriff auf SIROUT ermöglicht.

[5] Vom Identifizierungsprozess ausgenommen ist jede vom Kanton Wallis angestellte Person, die im Rahmen ihrer Tätigkeit für den Kanton Wallis bereits über ein von der für die Informatik zuständige kantonale Dienststelle eingerichtetes berufliches Benutzerkonto verfügt.

[6] Eine oder mehrere Rollen werden dem Benutzer von der zuständigen Behörde zugewiesen. Sie legt die Zugriffsrechte und Funktionen des Benutzers fest.

[7] Dem Benutzer können namentlich die folgenden Rollen zugewiesen werden:

a) Administrator;
b) Inspektor KKSS;
c) Mitglied KKSS;
d) Gesuchsteller Kanton;
e) Gesuchsteller Gemeinde;
f) Sekretariat;
g) kantonale Dienststelle.

[8] Ein Benutzer kann mehrere eID, private wie berufliche, erstellen. Die Angestellten des Kantons und der Gemeinden sowie die Mitglieder von kantonalen und kommunalen Behörden verwenden bei der Ausübung ihrer amtlichen Tätigkeit ihr berufliches Benutzerkonto.

Art. 4 Dossier

[1] Das Dossier umfasst alle Dokumente, die für die in Artikel 16 bis 19 AGSVG und Artikel 9, 12 und 13 RKKSS vorgesehenen Verfahrenshandlungen erforderlich sind.

[2] Das Dossier gilt als erstellt und das Verfahren als eröffnet, wenn der Gesuchsteller die entsprechende Validierung vorgenommen hat.

[3] Wird die Validierung nicht innert einem Jahr nach Anlegen des Dossiers vorgenommen, wird es dauerhaft gelöscht.

[4] Sämtliche Mitteilungen in Zusammenhang mit der Behandlung des Dossiers erfolgen über SIROUT.

[5] Jedes Dossier enthält eine eigene, von SIROUT generierte Referenznummer.

[6] Die zuständige Behörde verwaltet die Dossierzugriffe.

3 Beziehungen zwischen SIROUT und Benutzern

Art. 5 Elektronische Kommunikationskanäle

[1] Die elektronische Kommunikation erfolgt über jeden digitalen Kanal, der auf SIROUT zur Verfügung steht und der vom Benutzer bei der erstmaligen Verbindung über SIROUT akzeptiert worden ist. Die Zustimmung gilt auch für alle späteren Anfragen.

Art. 6 Eingabe und Validierung der Dokumente

[1] Alle Dokumente müssen im Format PDF auf SIROUT eingegeben werden.

[2] Es liegt in der Verantwortung des Benutzers, sich die erforderliche Infrastruktur für die Eingabe, das Öffnen und das Lesen von Dokumenten zu beschaffen, die sich auf SIROUT befinden.

[3] Alle auf SIROUT eingegebenen Dokumente müssen durch die von der zuständigen Behörde bestimmten Rollen validiert werden.

[4] Kann ein Dokument von der zuständigen Behörde nicht geöffnet oder gelesen werden, setzt diese dem Benutzer, der die Dokumente eingegeben hat, eine Frist zur Übermittlung des betreffenden Dokuments im vorgegebenen Format und über die von ihr bestimmten Kommunikationskanäle.

Art. 7 Anhörung der kantonalen Organe

[1] Das Anhörungsverfahren der kantonalen Organe erfolgt über SIROUT, sofern keine hiervon abweichende zwingende gesetzliche Regelung besteht.

4 Eröffnung der Entscheide

Art. 8 Elektronische Eröffnung

[1] Die Eröffnung von Entscheiden im Rahmen dieses Reglements erfolgt auf elektronischem Wege über SIROUT.

[2] Jeder Benutzer kann auf SIROUT Datum und Zeit der Eröffnung einsehen.

Art. 9 Format

[1] Der Entscheid wird im Format PDF eröffnet.

[2] Es liegt in der Verantwortung des Benutzers, die hierfür erforderliche Infrastruktur vorzusehen, namentlich für die Eingabe, das Öffnen und das Lesen im Format PDF.

5 Datenschutz und Archivierung

Art. 10 Datenschutz-Managementsystem

[1] Die Datenschutzbestimmungen des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA) sind anwendbar.

Art. 11 Datenübermittlung

[1] Die SIROUT-Daten dürfen an die im Rahmen des Anhörungsverfahrens konsultierten kantonalen Organe weitergegeben werden.

Art. 12 Speicherung und Archivierung

[1] Die Dossiers werden periodisch auf einem geeigneten Datenträger gespeichert. Der Zugang zum Dossier muss jederzeit sichergestellt und die Integrität der Dokumente gewährleistet sein.

[2] Die Archivierung und der Archivzugang werden mit dem Staatsarchiv Wallis koordiniert und müssen dem GIDA entsprechen.

6 Pflichten und Verantwortlichkeiten

Art. 13 Pflichten und Verantwortlichkeiten des Benutzers

[1] Mit dem Zugang zu SIROUT akzeptiert der Benutzer ausdrücklich, dass seine persönlichen Daten bearbeitet und genutzt werden, soweit dies für die Behandlung aller im AGSVG und im RKKSS vorgesehenen Verfahrenshandlungen erforderlich ist.

[2] Der Benutzer ist dafür verantwortlich, seine Daten, die er auf SIROUT angegeben hat, kontinuierlich nachzuführen.

[3] Erhält der Benutzer von der zuständigen Behörde eine Mitteilung, die nicht für ihn bestimmt ist, muss er dies dem Absender umgehend melden.

[4] Der Benutzer ist für alle Handlungen verantwortlich, die über sein eigenes Benutzerkonto erfolgen.

Art. 14 Verantwortlichkeit des Staates

[1] Die Verantwortlichkeit der zuständigen Behörde wird ausschliesslich durch das Gesetz über die Verantwortlichkeit der öffentlichen Gemeinwesen und ihrer Amtsträger geregelt.

[2] Die zuständige Behörde haftet nicht für allfällige direkte oder indirekte Beeinträchtigungen irgendwelcher Art betreffend die Vertraulichkeit oder die Qualität der Daten, die nicht zu SIROUT gehören. Die zuständige Behörde ergreift jedoch die operativen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der durch ihre Informatiksysteme bearbeiteten Daten.

[3] Die zuständige Behörde garantiert keinen ununterbrochenen Zugang zu SIROUT. Somit kann der Zugang zu SIROUT gesperrt werden, namentlich – aber nicht ausschliesslich – bei einer technischen Störung, einem böswilligen Angriff, Wartungsarbeiten oder einem anderen Fall höherer Gewalt. Die zuständige Behörde haftet nicht für die Folgen einer Unterbrechung des Zugangs zu SIROUT.

Art. 15 Missbräuchliche Benutzung von SIROUT

[1] Bei missbräuchlicher Benutzung von SIROUT wird der Zugang gesperrt.

[2] Dokumente, die keinen Bezug haben zu dem Dossier im Sinne von Artikel 4 Absatz 1, in dem sie eingereicht wurden, werden von der zuständigen Behörde entfernt.

[3] Die Sperrung wird dem Benutzer über dessen elektronischen Kommunikationskanal mitgeteilt, und es wird ihm eine Frist für die reglements- und rechtskonforme Wiederherstellung gesetzt.

[4] Strafrechtliche Schritte bleiben vorbehalten.

Änderungstabelle - Nach Beschluss

Beschluss	Inkrafttreten	Element	Änderung	Quelle Publikation
08.07.2026	01.07.2026	Erlass	Erstfassung	RO/AGS 2026-094

Änderungstabelle - Nach Artikel

Element	Beschluss	Inkrafttreten	Änderung	Quelle Publikation
Erlass	08.07.2026	01.07.2026	Erstfassung	RO/AGS 2026-094