



Merkblatt

ISDS-Anforderungen für die Nutzung der Plattform «Justitia.Swiss» durch Justizbehörden

Im Bereich der Informationssicherheit bestehen gewissen Anforderungen zur Nutzung der Plattform «Justitia.Swiss» durch die Justizbehörden. Die gesetzlichen Grundlagen werden sich im Verlauf der Einführung der Plattform «Justitia.Swiss» ändern:

- [VeÜ-ZSSV \(SR 272.1\)](#) bis Mitte 2025 (geplant)
- [Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz, BEKJ](#) (BBI 2023 680, Entwurf) ab Mitte 2025 (geplant)

Die Anforderungen / Handlungsempfehlungen in diesem Merkblatt richten sich an IT-verantwortliche Personen der Justizbehörden und kantonalen IT-Ämter.

1 Anforderungen zur Authentifikation mittels einer digitalen Identität

Die Plattform setzt beim Login eine **existierende digitale Identität** voraus. Dies kann beispielsweise das Benutzerprofil für kantonale IT-Anwendungen sein.

Für den Pilotbetrieb gemäss VeÜ-ZSSV bestehen keine Mindestanforderungen an die Qualität (das Sicherheitsniveau) der digitalen Identität. Ab Inkrafttreten des BEKJ wird die Qualität der digitalen Identität über eine Verordnung (aktuell nicht vorliegend) geregelt.

Für Justizbehörden werden die benötigten und bestehenden Identitätsdienstleistungen in die Plattform «Justitia.Swiss» integriert (AGOV, EJPD SSO-Portal, kantonale IDPs oder privatrechtliche IDPs).

2 Anforderungen zur Signatur und Signatur-Verifikation

Sowohl für den Pilotbetrieb gemäss VeÜ-ZSSV als auch für die Nutzung unter BEKJ ist jedes von einer (Justiz-)Behörde an die Plattform zu übermittelndem Dokument mit einer qualifizierten elektronischen Signatur zu versehen.

Für den Pilotbetrieb unter VeÜ-ZSSV handelt es sich um eine **qualifizierte elektronische Signatur** nach [ZertES Art. 2, Abs. e](#) und für den Betrieb unter BEKJ ein **geregeltes elektronisches Siegel** nach ZertES, Art. 2, Abs. d.

Für den Pilotbetrieb unter VeÜ-ZSSV ist es Aufgabe der Justizbehörde, die korrekte Signatur von eingehenden Sendungen zu **verifizieren**. Im Betrieb unter BEKJ übernimmt die Plattform «Justitia.Swiss» diese Aufgabe.

3 Anforderungen zur allgemeinen Informationssicherheit und Datenschutz

Aufgrund der Tatsache, dass Dokumente/Dateien auf der Plattform «Justitia.Swiss» keine Originale sind und nicht bearbeitet werden können, impliziert die Nutzung der Austauschplattform keine zusätzlichen Anforderungen hinsichtlich der Informationssicherheit und des Datenschutzes (ISDS). Die Schutzmassnahmen der Plattform «Justitia.Swiss» orientieren sich an den Informatiksicherheitsvorgaben des [NCSC für Informatikschutzobjekte mit erhöhtem Schutzbedarf](#), vergleichbares ist auch seitens der IT-Systeme der nutzenden Justizbehörden zu befolgen. Die entsprechenden Schutzmassnahmen richten sich insbesondere nach den vorliegenden Klassifikationen (gemäss [ISchV, 510.411](#) resp. [ISG, BBI 2020 2696](#), Entwurf).

4 Empfehlungen hinsichtlich des Sicherheitsbewusstseins (Security Awareness)

Mitarbeitende von Justizbehörden sind, unabhängig von der Nutzung der Plattform «Justitia.Swiss» im Sicherheitsbewusstsein (der Security Awareness) zu schulen. Für kantonale Mitarbeitende stehen verschiedene Schulungsmöglichkeiten wie das E-Learning zur [Informationssicherheit und Cybersicherheit für alle Verwaltungsangestellten der Schweiz](#) oder bundesweite Programme wie www.s-u-p-e-r.ch und www.informatiksicherheit.admin.ch zur Verfügung.

Weiterführende Informationen

Weiterführende Informationen und Informationen zu verwandten Themen erhalten Sie via: info@justitia.swiss und/oder auf der Webseite www.justitia40.ch