PROJEKT Justitia 4.0

Umfang des Piloten der Plattform Justitia.Swiss

Filename:	J40_Übersicht_MVP_Plattform
Projektphase:	Design
Erstellungs-Datum:	21. September 2023
Autor:	J. Barraud, F. Achermann

Contents

1 Einleitung 1

1.1 Rechtliche Grundlagen 2

2 Beschreibung der Software 2

2.1 Eingaben 2
2.2 Zustellung und Akteneinsicht 3
2.2.1 Akte bewirtschaften 4
2.2.2 Aktentransfer (Zustellung und Akteneinsicht) auslösen 4
2.2.3 Aktentransfer empfangen 4
2.2.4 Verwaltung der Einsichtsrechte 5
2.3 Stammdaten und Administration 5
2.3.1 Individuelles Profil 5
2.3.2 Gruppenprofil 5
2.3.3 Profile für Justizbehörden 6
2.4 Web und API Zugriff 7
2.5 Unterstützte Datentypen für MVP 7

3 Betriebsdisziplinen für den Pilotbetrieb 7

4 Auswirkungen auf bestehende Prozesse oder Arbeitsabläufe 7

1 Einleitung

Im Rahmen des Projekts Justitia 4.0 verfolgen wir das übergeordnete Ziel, die Digitalisierung in der Schweizer Justiz voranzutreiben. Das Hauptmotiv hinter diesem Vorhaben ist es, den Weg zur Rechtsprechung von papierbasierten Prozessen zu befreien und stattdessen effiziente digitale Lösungen zu etablieren.

Ziel des Piloten ist die Erprobung des rechtsgültigen Praxisbetriebs der Plattform «Justitia.Swiss» (nachfolgend: Plattform) als Beitrag zur Digitalisierung der Justiz.

Die Erkenntnisse aus dem Pilotbetrieb fliessen fortlaufend in die Weiterentwicklung der Plattform, die Planung des schweizweiten Rollouts und der digitalen Transformation ein.

Per zweitem Quartal 2024 soll das Minimal Viable Product (MVP) der Plattform realisiert sein und in einem Pilotbetrieb betrieben werden. Erläuterung:

- Software des MVP: Diese Software ist ausgetestet und erfüllt die an sie formulierten Anforderungen. In Kapitel 2 wird die Funktion der Software beschrieben.
- Pilotbetrieb: In Kapitel 3 die nötigen Betriebsdisziplinen erwähnt, mit denen das MVP betrieben und weiterentwickelt wird.

1.1 Rechtliche Grundlagen

Einen nicht unerheblichen Impact auf den Pilotbetrieb haben die rechtlichen Rahmenbedingungen, welche insbesondere die Basis die Pilotierung und ebenso die Einführung des (Pilot)Betriebs definieren.

Der Pilotbetrieb findet zunächst im engen Rahmen von Artikel 13a der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (VeÜ-ZSSV, SR 210.1) statt. Dies bedeutet, dass die in den Verfahrensgesetzen, in erster Linie der ZPO (SR 272) und der StPO (SR 312), enthaltenen gesetzlichen Bestimmungen einzuhalten sind. Insbesondere das Erfordernis einer qualifizierten elektronischen Signatur anstelle der handschriftlichen Unterschrift wird beibehalten. Es handelt sich dabei um ein Erfordernis, das sowohl für die Eingaben (Bsp. Art. 130 Abs. 2 ZPO, bzw. Art. 110 Abs. 2 StPO) an eine Justizbehörde als auch für Zustellungen (Bsp. Art. 139 ZPO, bzw. Art. 86 StPO) von einer Justizbehörde (vorerst) weiterhin gilt. Ermöglicht mit anderen Worten die Verordnung die Nutzung der Plattform anstelle der derzeit anerkannten Zustellplattformen (PrivaSphere und IncaMail), sind die formalen Anforderungen gemäss VeÜ-ZSSV – mindestens bis zum Inkrafttreten des BEKJ – für den (Pilot)Betrieb bindend.

Darüber hinaus verlangt die Verordnung, dass der Kanton formell ein Gesuch beim EJPD einreicht (Art. 13a Abs. 1 VeÜ-ZSSV) und dass der Anwendungsbereich der Plattform klar definiert ist (Art. 13a Abs. 3 VeÜ-ZSSV). Die technische Dokumentation, die zur Genehmigung eingereicht werden muss, wird vom Projekt bereitgestellt.

2 Beschreibung der Software

Die Software bzw. Plattform «Justitia.Swiss» ermöglicht drei grundlegende Transaktionen: Eingabe, Zustellung und Akteneinsicht. Technische erfolgen diese Transaktionen durch die Übermittlung von Sendungen, welche aus einzelnen Dokumenten, resp. Dateien bestehen. Es werden die Dateien verschlüsselt, um ihre Sicherheit zu gewährleisten; die Sendungen werden mit einem elektronischen Siegel versehen, um ihre Integrität zu schützen.

Für jede Übermittlung einer Sendung werden Quittungen: die Eingangsquittung, die Abrufquittung und die Nichtabholquittung. Diese 3 Quittungen dienen dem rechtsgültigen Nachweis der Sendung.

2.1 Eingaben

Eine Eingabe besteht aus 2 Teilprozessen: Die sendende Partei erstellt die Eingabe (Create Submission) und diese Eingabe wird durch die Justizbehörde empfangen und verarbeitet (Receive Submission):

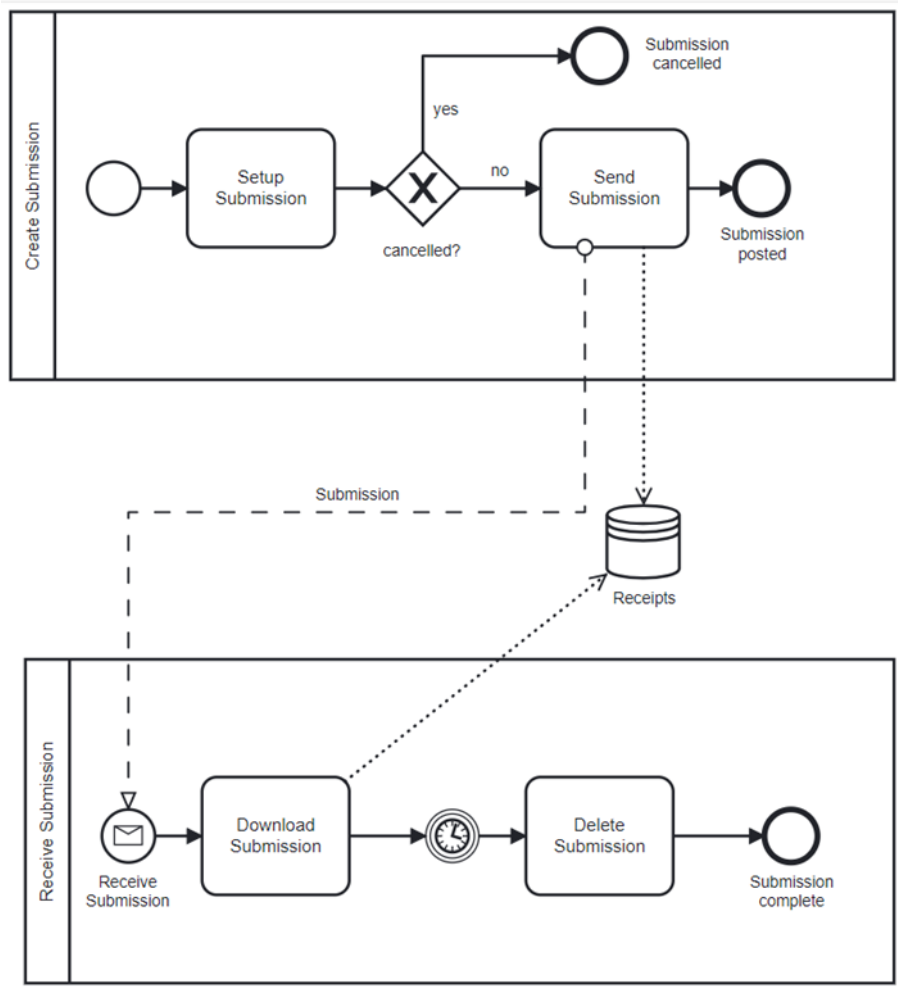

Abbildung 1 Eingabe

Eingabe erstellen («Setup Submission»)**:** Mit Erstellen ist das Hochladen von Dateien zum Aufsetzen einer Eingabe im Status «Entwurf» gemeint. Dabei können Dateien resp. Dokumente beliebig hinzugefügt oder entfernt – jedoch nicht bearbeitet – werden. Eine Eingabe im Status 'Entwurf' kann jederzeit wieder gelöscht werden.

Mit der **Übermittlung der Eingabe** an den Empfänger – die zuständige Justizbehörde - («Send Submission») wird die Eingabe abgeschlossen. Ab diesem Zeitpunkt kann die Eingabe nicht mehr verändert werden. Die Eingabe wird an die Justizbehörde übermittelt und es wird gleichzeitig eine Eingangsquittung erstellt.

Eingabe Empfangen: Mit dem Abruf der übermittelten Eingabe kann die Justizbehörde die eingegebenen Dokumente herunterladen («Download Submission») und verarbeiten. Mit dem erstmaligen Abruf wird automatisch eine Abrufquittung erstellt.

Frühestens 90 Tage nach dem erstmaligen Abruf werden die Eingabe und die zugehörigen Quittungen automatisch gelöscht («Delete Submission»).

2.2 Zustellung und Akteneinsicht

Folgender Prozess zeigt das Zusammenspiel des Bereitstellens von Akten und den Transfer dieser Akten im Rahmen der Zustellung oder Akteneinsicht:

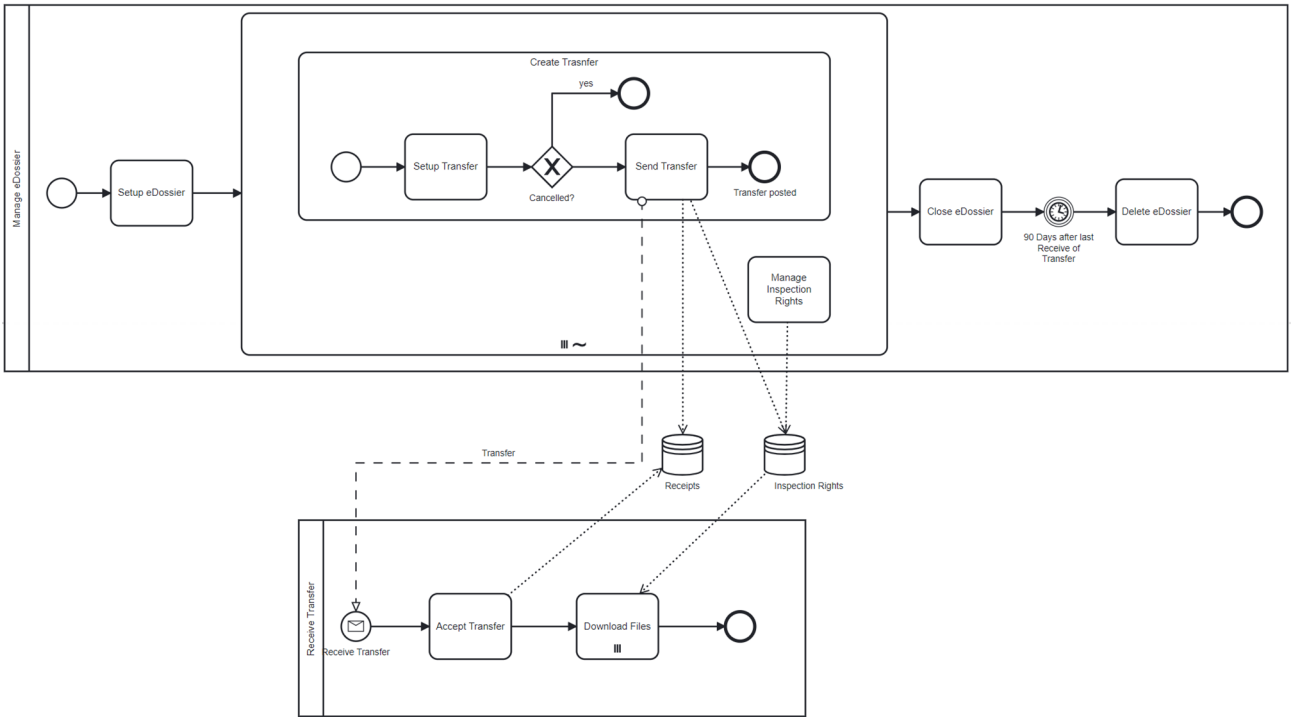

Abbildung 2 Aktentransfer

2.2.1 Akte bewirtschaften

Mit dem Prozess «Manage eDossier» stellen Justizbehörden während eines Verfahrens eine einsehbare Kopie der Akte auf der Plattform zur Verfügung. Dazu werden initial die wichtigsten Stammdaten (Aktennummer, Gegenstand etc.) bekanntgegeben («Setup eDossier»). Bei Änderungen dieser Daten können diese nachträglich aktualisiert werden.

Während der Verfahren können auf der Plattform diese Tätigkeiten mehrfach ausgeführt werden:

- Aktentransfer auslösen («Make Transfer») und
- Einsichtsrechte verwaltet («Manage Inspection Rights»)

Mit Abschluss oder Sistierung des Verfahrens werden die auf der Plattform bereitgestellten einsehbaren Kopien der Akten wieder zur Löschung vorgemerkt («Close eDossier») und spätestens nach 90 Tagen nach dem letzten Aktentransfer automatisch gelöscht («Delete eDossier»).

2.2.2 Aktentransfer (Zustellung und Akteneinsicht) auslösen

Zum Aufsetzen eines Aktentransfers können Dokumente (resp. Dateien) zu Verfahren auf die Plattform replizieren werden («Setup Transfer»). Dies geschieht via Web-Oberfläche aus dem FileShare oder direkt aus der bestehenden IT-Umgebung via API.

Der Aktentransfer besteht technisch aus dem Erteilen von Einsichtsrechten auf Dokumente (resp. Dateien) der Akte an das Profil einer verfahrensbeteiligten Person. Ein Transfer kann für die Zustellung oder das Erteilen einer Akteneinsicht genutzt werden.

Nach Prüfung des vorbereiteten Aktentransfers wird dieser übermittelt («Send Transfer») und automatisch eine Eingangsquittung erstellt.

2.2.3 Aktentransfer empfangen

Bevor die Dokumente (resp. Dateien) durch das empfangende Profil gelesen werden können, muss der Empfang des Aktentransfers explizit akzeptiert werden («Accept Transfer»). Damit wird die Abrufquittung erstellt und das

empfangende Profil kann die Dokumente, resp. Dateien herunterladen, für welche es berechtigt wurde («Download Files»).

Wird innerhalb von 7 Tagen kein Abruf getätigt, wird durch die Plattform automatisch eine Nichtabholquittung erstellt (Zustellfiktion).

2.2.4 Verwaltung der Einsichtsrechte

Mitarbeitende einer Justizbehörde können die erteilten Einsichtsrechte auf die Aktenstücke jederzeit überprüfen («Manage Inspection Rights»). Die Einsichtsrechte können entzogen, zeitlich eingeschränkt (z.B. für den Anwaltswechsel) oder verlängert werden.

Normalerweise erfolgt mit der Änderung von Einsichtsrechten auch eine zeitnahe Information (z.B. Schreiben betr. Verlängerung) an die Beteiligten. Die Plattform gibt dazu jedoch keinen Ablauf vor, die Übermittlung dieser Information erfolgt durch einen eigenen Aktentransfer.

2.3 Stammdaten und Administration

Die Plattform bietet verschiedene Profile für unterschiedliche Benutzergruppen an, darunter Organisationen, Justizbehörden und Einzelpersonen. Die Authentifizierung der Benutzerinnen und Benutzer erfolgt durch externe IDP-Provider (Bspw. TrustID und SwissID), diese tragen zur Sicherheit und Zuverlässigkeit der Zugriff bei.

2.3.1 Individuelles Profil

Ein individuelles Profil erlaubt einer einzelnen, physischen Person am Rechtsverkehr und der Akteneinsicht teilzunehmen:

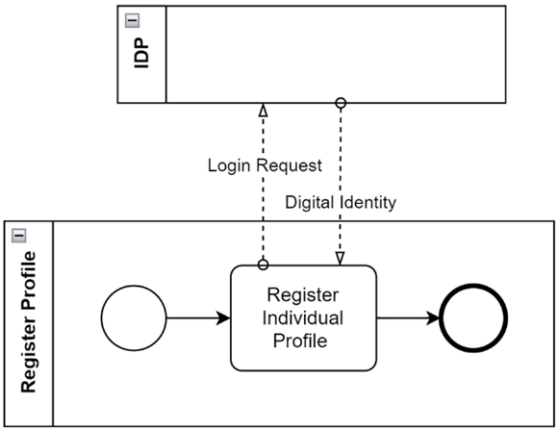

Abbildung 3 Individuelles Profil

Bevor das Profil erstellt werden kann, muss bei einem integrierten externen IDP eine digitale Identität registriert werden.

Individuelles Profil registrieren: Eine Privatperson kann ein Profil auf ihren Namen (der beim externen IDP Provider hinterlegt ist) erfassen.

2.3.2 Gruppenprofil

Mit einem Gruppenprofil kann eine Person weiteren Mitgliedern Zugang zu ihrem Profil geben. Die Vorbedingungen sind entsprechend dem Individualprofil:

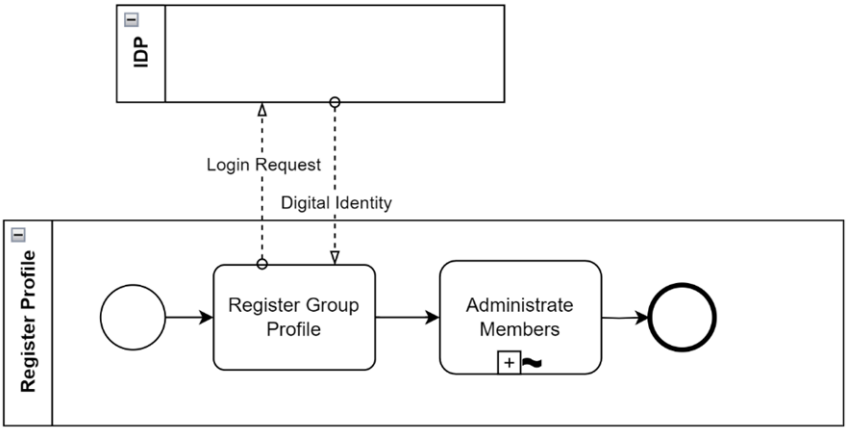

Abbildung 4 Gruppenprofil

Es können weitere Mitglieder eingeladen werden («Administrate Members»). Für diese Mitglieder kann festgelegt werden, ob sie nur am Rechtsverkehr und der Akteneinsicht teilnehmen, oder ob sie selber auch das Profil bewirtschaften können.

2.3.3 Profile für Justizbehörden

Profile für Justizbehörden werden aus Gruppenprofilen durch einen administrierten Schritt erstellt:

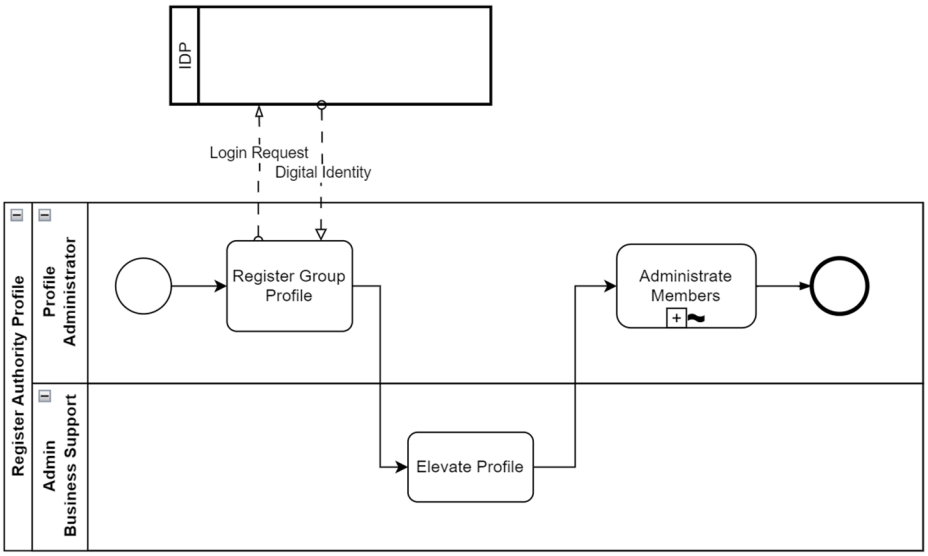

Abbildung 5 Profile für Justizbehörden

Die Registrierung und Bewirtschaftung eines administrierten Profils erfolgt – wie das Gruppenprofil – durch den Profil-Administrator.

In einem unterstützenden Schritt werden die Bedingungen für die Umwandlung des Profils geprüft und die Umwandlung wird durch den Business Admin Support vorgenommen («Elevate Profile»). An das Profil einer Justizbehörde können Eingaben erstellt werden, die Zustelladresse der Behörde ist für alle sichtbar.

Der Profiladministrator kann weiteren Mitarbeitenden der Justizbehörden (z.B. Mitarbeiter oder Mitarbeiterin Kanzlei) Zugriff auf das Profil erteilen.

2.4 Web und API Zugriff

Der Zugriff auf die Plattform kann wahlweise über das Web-Portal erfolgen, oder via eine integrierte Fachapplikation, welche direkt über eine Rest-API mit der Plattform kommuniziert.

Die Dokumentation des Rest-APIs wird durch das Projekt allen interessierten Software-Herstellern zur Verfügung gestellt.

Ein wichtiger Aspekt ist die Barrierefreiheit des Web-Portals gemäss den Richtlinien WCAG 2.1, um eine barrierefreie Nutzung der Plattform zu gewährleisten.

2.5 Unterstützte Datentypen für MVP

Alle durch die Plattform übermittelten Dateien haben einen Zweck. Je nach Zweck wird der Datentyp geprüft:

- Dateien vom Typ 'Dokument' sind im PDF-Format.
- Dateien vom Typ 'Beilage' können in verschiedenen Formaten vorliegen.

Die maximale Grösse einer Datei ist auf 100MB beschränkt. Es ist zu beachten, dass aufgrund sehr langsamer Internet Verbindungen der Up- resp. Download von sehr grossen Dateien unterbrochen werden kann.

3 Betriebsdisziplinen für den Pilotbetrieb

Ziel des Pilotbetriebs ist es namentlich, die Betriebsprozesse und Informationssicherheit umzusetzen und von Anfang an einzuhalten. Dies betrifft folgende Disziplinen:

- Anwendungsbetrieb (Monitoring, Verwalten von Profilen): Stellt den fachlichen, operativen Betrieb der Services zur Verfügung.
- Support Prozesse (Incident- & Problem Management): Bearbeiten von Service Incidents oder Service Requests.
- SLA Management: Regelmäßiges Messen der erreichten Service-Qualität und Identifizieren von Bereichen, in denen die Service-Qualität verbessert werden muss.
- Change & Releasemanagement: Der Prozess gewährleistet, dass Änderungen bezüglich der Serviceangebote des Service-Providers sowie der zugrunde liegenden Komponenten erst nach sorgfältigem Abwägen der Risiken und möglichen Nebeneffekte erfolgen.
- Security: Security wird über organisatorische und technische Massnahmen gemäss ISDS-Konzept sichergestellt:
  - Organisatorische Massnahmen bereits im MVP: Das Security Operations Center (SOC) erkennt Anomalien und stellt sicher, dass diese angemessen adressiert werden. Die kontinuierliche Messung und Weiterentwicklung der Qualität der Security Services anhand eines Information Security Management Services (ISMS) wird sichergestellt.
  - Technische Massnahmen bereits im MVP umgesetzt:
    - Verschlüsselung sämtlicher Dokumente
    - Virenprüfung
- Business Continuity Management: Die Verfügbarkeit und Leistung der Plattform wird auch im Katastrophenfall auf einem ausreichenden Niveau gehalten.

4 Auswirkungen auf bestehende Prozesse oder Arbeitsabläufe

Die Softwareeinführung kann Änderungen in den Arbeitsabläufen mit sich bringen, erfordert möglicherweise Schulungen und das Erlernen neuer Fähigkeiten der Beteiligten. Die Plattform digitalisiert Aufgaben, Arbeitsschritte und verändert die Rollen der Mitarbeitenden. Sie kann ebenfalls die Zusammenarbeit und Kommunikation verändern. Insgesamt wird die Einführung der Plattform «Justitia.Swiss» bestehende Prozesse und Arbeitsabläufe der beteiligten

Organisationen beeinflussen. Das von Justitia 4.0 gewählte Vorgehen eröffnet dabei den Kantonen die Möglichkeit ihre internen Prozesse einem Review zu unterziehen, zu testen und weiterzuentwickeln.