Anhang 10 Grobanforderung Plattform Justitia.Swiss

Inhaltsverzeichnis

Redaktionelle Hinweise

Dieses Dokument enthält die Grobanforderungen der Plattform Justitia.Swiss als Beilage der Ausschreibung.

Die Grobanforderungen sind im weitesten Sinn funktional gegliedert und befinden sich auf Stufe 2 mit FUN-xx-yy. Für einen initialen Überblick sind einleitend die Fachkonzepte, das Systemdiagramm mit Interfaces und des Operating Modells als Big Picture dargestellt.

Die einzelnen Grobanforderungen habe unterschiedliche Prioritäten. Dabei bedeuten:

- Muss: Die Anforderung muss für einen produktiven Betrieb im Sinne eines Minimal-Viable Products umgesetzt sein.
- Prio 1: Wichtige Anforderung, die in erster Priorität umgesetzt werden soll.
- Prio 2: Weniger wichtige Anforderung, in zweiter Priorität umgesetzt werden soll.
- Option: Die Anforderung ist optional. Je nach Bedürfnis wird die Dringlichkeit angepasst, oder die Anforderung nicht umgesetzt.

FUN-01 Master Data Management

Stammdatenprozesse für die Verwaltung von Informationsobjekten zu Personen, Profilen und Delegationen.

FUN-01-01 Profil verwalten Muss

Das Profil ist das zentrale Stammdatenobjekt für die Nutzung der Plattform. Jede Person (natürliche oder eine Organisation) hat ein Profil. Auf dem Profil werden folgende Eigenschaften festgehalten:

- Die Person nimmt durch Setzen einer Zustelladresse am Rechtsverkehr und der Akteneinsicht teil.
- Eine Benachrichtigungsadresse kann definiert werden. Einstellungen zur Art und Häufigkeit der Benachrichtigung können definiert werden.
- Weitere Attribute wie z.B. eine Zusatzbezeichnung, unter der die Person im Adressverzeichnis beschreiben sein soll.

Ein Teilnehmer ist eine Person (Natürliche Person mit einem Profil einer Privatperson oder eine Organisation mit einem selbst administrierten Profil oder einem Profil einer administrierten Organisation), die auf der Plattform eine Zustelladresse besitzt.

Hinweis: die Verwaltung des Profils erfolgt über das API Justitia.Swiss.02.

FUN-01-02 Natürliche Personen verwalten Muss

Attribute der natürlichen Personen werden vom externen Identitätsprovider übernommen. Damit hat die Datenqualität der Personen eine definierte Qualität gemäss Art. 19 VE-BEKJ: Amtliche Attribute der natürlichen Personen werden amtlich geprüft.

Hinweis: Duplikate von Person in unterschiedlichen Rollen von unterschiedlichen Identitätsprovider (z.B. Privatperson und Mitarbeiter einer Behörde) werden nicht verhindert.

FUN-01-03 Organisationen selbst verwalten Muss

Organisationen sind Gruppen von natürlichen Personen gemäss Art. 24 VE-BEKJ. Eine natürliche Person kann selbstbedient eine Organisation eröffnen und bewirtschaften. Die eröffnende Person ist initial Administrator dieser selbstadministrierten Organisation.

Der Administrator kann weitere Personen über ein Einladungsverfahren als Mitglieder der Organisation hinzufügen und diesen Mitgliedern Rechte an der Organisation (und dem zugehörigen Profil) erteilen.

Hinweis: damit können Anwälte oder andere professionelle Vertreter selbstadministrierte Organisationen mit zugehörigem (Anwalts)Profil eröffnen.

Hinweis: die eigenständige Verwaltung einer selbstadministrierten Organisation erfolgt über das API Justitia.Swiss.02.

FUN-01-04 Organisationen administrieren Muss

Justizbehörden und Organisationen (wie zum Beispiel Versicherungen) können auch über einen administrativen Prozess eine Organisation auf der Plattform erhalten. Organisationen sind Gruppen von natürlichen Personen gemäss Art. 24 VE-BEKJ. Die Datenqualität der Profile von administrierten Organisationen hat eine höhere Vertrauenswürdigkeit als selbst-administrierte Organisationen.

Administrierte Organisationen können einen eigenen Identitätsdienst einbinden (= IDP-verwaltete Organisationen), mit dem sie den Benutzern dynamisch Rechte an der Organisation und dem zugehörigen Profil geben (durch den IDP der Organisation verwaltete Benutzer). Sie können ihre Systeme mittels API und technischen Schlüsseln mit der Plattform integrieren.

Profile von selbst-administrierten Organisationen können in Profile von administrierten Organisationen gewandelt werden.

Hinweis: Mitarbeiter der Justizbehörden und Organisationen können mit ihrem Mitarbeiterlogin auf der Plattform arbeiten.

Hinweis: für die technische Anbindung, die Übermittlung von Schlüsseln und das Mapping der Rollen sind entsprechende Vorkehrung zu treffen, siehe FUN-08-03.

FUN-01-05 Verfahrensspezifische Delegation verwalten Prio 1

Der Inhaber und Berechtigte eines Profils kann bestimmte Handlungen an andere Personen delegieren. Diese Delegation kann spezifisch für ein Verfahren im engeren Sinn pro Behörde festgelegt werden.

Das Errichten einer Delegation muss die Wahrung der Privatsphäre von Benutzern gewährleisten: das heisst, es wird ein Einladungsverfahren verwendet, welches die Sichtbarkeit der Personen erst nach gegenseitigem Einverständnis ermöglicht.

Hinweis: Delegierte handeln in Vertretung einer anderen Person.

Hinweis: die Verwaltung der Delegation erfolgt über das API Justitia.Swiss.02.

FUN-01-06 Adressverzeichnis lesen Muss

Die Plattform führt ein Adressverzeichnis der Profile, die eine Zustelladresse auf der Plattform besitzen. Die Sichtbarkeit des Adressverzeichnisses ist eingeschränkt:

- Mitarbeiter der Justizbehörden (Personen, die ein Mitarbeiterprofil bei einem Profil einer Justizbehörde haben) können definierte Attribute aller Profile die eine gültige Zustelladresse haben lesen.
- Alle anderen Benutzer der Plattform können die definierten Attribute der Profile der Justizbehörden lesen.

Jedes im Adressverzeichnis geführte Benutzerattribut hat eine definierte Qualitätsstufe.

Hinweis: Das Adressverzeichnis ist über das API Justitia.Swiss.01 einsehbar.

FUN-02 Meldungsvermittlung

Die Kerntransaktionen der Plattform für den elektronischen Rechtsverkehr beinhalten die Vermittlung von Eingaben von verfahrensbeteiligten Personen an Justizbehörden und die Zustellung von Links auf Aktenstücke einer Akte als Aufforderung zur Akteneinsicht.

FUN-02-01 Eingabe Muss

Eine Eingabe besteht aus einer oder mehreren Dateien und den zugehörigen Metadaten, die von einer verfahrensbeteiligten Person an eine Justizbehörde übermittelt werden.

Die Plattform erlaubt eine flexible und erweiterbare Anreicherung der Eingabe (resp. der beigefügten Dateien) mit zusätzlichen Metadaten für eine Kategorisierung. Diese Anreicherung kann auch abhängig vom Profil des Absenders oder des Empfängers sein.

Die Metadaten werden für verschiedene Zwecke verwendet:

- Zur Verbesserung der Sicherheit z.B. bei Verdacht auf Viren.
- Erlaubt (beim Empfänger) die automatische Verarbeitung oder das Routing von strukturierten Dateien (z.B. für die Kommunikation zwischen Polizei und Behörden).
- Stammen die einzugebenden Dateien selber aus einer Akte, enthalten die Metadaten Rubriken und Aktennummern, um das Referenzieren sicherstellen zu können oder um Verweise (Links) auf zur Verfügung gestellte Aktenstücke oder Asservate mitzugeben.
- Metadaten enthalten kryptographische Schlüssel, um die Integrität der Dokumente nachzuweisen.
- Technische, optionale Metadaten der Dokumente, welche Teil der Dateien sind (z.B. exif Daten bei Bildern oder Hinweise auf Softwareversionen), werden bei Bedarf dem Eingebenden angezeigt und können aus Datenschutzgründen entfernt werden.
- Eine Eingabe kann sich über eine AkteId auf ein laufendes Verfahren einer Behörde beziehen.
- Es kann geprüft werden, ob die eingegebene Rechtsschrift mit einer gültigen qualifizierten elektronischen Signatur versehen ist. Dies kann im Pilotbetrieb nötig sein, da erst mit Inkrafttreten des BEKJ die Unterschriftserfordernis angepasst wird.

Die Dateien werden durch die Plattform mit dem Siegel der Körperschaft Justitia.Swiss gesiegelt. Auf Wunsch (optionales Argument des Serviceaufrufs oder in den Einstellungen auf dem Profil) wird automatisch beim Abschluss der Aufgabe eine Quittung erstellt, welche ebenfalls gesiegelt wird.

Die gesiegelte Eingabe wird von den Justizbehörden ab ihrem Postfach abgeholt. Abgeholte Eingaben werden nach einer definierten Zeit auf der Plattform gelöscht.

Falls auf dem Profil der (empfangenden) Justizbehörde eine Benachrichtigung für Eingaben konfiguriert ist, erhält diese eine entsprechende Benachrichtigung.

Die Plattform bietet Erweiterungsmöglichkeiten, um standardisierte Eingaben (z.B. Fristverlängerungen) strukturiert erfassen zu können.

Hinweis: Eingaben werden über das API Justitia.Swiss.03 erfasst und heruntergeladen.

FUN-02-02 Zustellung Muss

Eine Zustellung ist die Übermittlung des Einsichtsrecht in ein oder mehrere Aktenstücke der Justizbehörde an eine verfahrensbeteiligte Person. Es gibt verschiedene Ausprägungen:

- Eine Zustellung mit Frist, innerhalb der der Empfänger der Zustellung das Aktenstück konsultieren muss. Die Plattform quittiert das Versenden der Zustellung und das erstmalige Lesen der so berechtigen Aktenstücke.
- Das reine Gewähren einer Akteneinsicht erfolgt ohne Verbindung einer Frist. Die Plattform quittiert das Gewähren der Akteneinsicht.

Auf Wunsch (optionales Argument des Serviceaufrufs oder in den Einstellungen auf dem Profil) wird automatisch nach dem vollständigen Übermitteln und Bestätigen der Akteneinsichtsrechte eine Quittung erstellt, welche gesiegelt wird.

Falls auf dem Profil der (empfangenden) Person eine Benachrichtigung für Zustellungen konfiguriert ist, erhält diese eine entsprechende Benachrichtigung.

Hinweis: Zustellungen werden über das API Justitia.Swiss.04 administriert.

FUN-02-03 Zustellung mit Einladungsverfahren Prio 2

Justizbehörden können eine Zustellung an einen noch-nicht Teilnehmer vornehmen. Dazu eröffnen sie ein temporäres Profil mit einer Zustelladresse und laden (beispielsweise über den Briefkanal) die Person ein, sich zu registrieren und mit diesem Profil zu verbinden.

Hinweis: Der Prozess des Einladungsverfahrens, insbesondere das Lifecycle Management dieses 'temporären Profils' bei nicht beantworteten Einladungen, die Möglichkeit eines Benutzers bei parallelen Einladungen diese zusammenzuführen, etc. wird im Design geklärt.

FUN-02-04 Antwort auf Eingaben ohne Verfahren Prio 1

Justizbehörden können über die Plattform auf Eingaben antworten, ohne ein Verfahren zu eröffnen.

Aus Sicht der Justizbehörden erfolgt dies mit den Mechanismen und Schnittstellen der Zustellung, das heisst es wird ein Dokument ohne AkteId zugestellt.

Der Empfänger erhält Einsicht in ein Dokument (die Antwort), ohne dass dieses in eine Aktenstruktur eingebettet ist. Eine Delegation oder eine Replik auf eine solche Antwort sind nicht möglich.

Die Plattform löscht das Dokument nach einer definierten Zeit, nachdem es durch den Empfänger gelesen wurde.

FUN-03 Dossier Store - Aktenbrowser

Der Dossier Store gibt jedem berechtigten Benutzer eine Sicht auf die Akten der Verfahren, für die er Berechtigungen hat.

FUN-03-01 Aktendeckel replizieren Muss

Die Verfahren werden in den IT-Systemen der angeschlossenen Justizbehörden administriert und die für die Darstellung der Aktenstücke eines einsehbaren Aktendossiers minimale Information wird auf die Plattform repliziert. Das heisst für das Lifecycle Management der Akten auf der Plattform:

- mit der erstmaligen Zustellung wird eine eindeutige Identifikation des Aktendossiers festgelegt,
- während der Laufzeit des Verfahrens wird die Information zur Akte im Aktendeckel aktualisiert,
- mit Abschluss des Verfahrens werden Daten auf der Plattform zu diesem Verfahren gelöscht, respektive zur Löschung vorgemerkt. Der Zeitpunkt der effektiven Löschung wird im Bearbeitungsreglement je Datenobjekt festgelegt.

Hinweis: der genaue Datenumfang der je Akte nötigen Daten wird im Rahmen des Designs unter Berücksichtigung der Datensparsamkeit festgelegt.

Hinweis: Der Lifecycle einer Akte wird über das API Justitia.Swiss.06 administriert.

FUN-03-02 Aktenstruktur darstellen Muss

Mit Erteilung eines Zugriffsrechts auf ein Aktenstück wird eine Akte für den Verfahrensbeteiligten sichtbar: die so berechtigten Benutzer sehen die Information des Aktendeckels und die für sie berechtigten Aktenstücke in der Aktenhierarchie.

Eine Rubrik der Aktenhierarchie ist für einen Benutzer sichtbar, wenn mindestens ein Aktenstück dieser Rubrik sichtbar ist. (D.h. leere Rubriken sind nicht sichtbar).

Benutzer können über sämtliche für sie einsehbaren Akten nach diversen Kriterien der Akten (siehe Daten der Akte gemäss FUN-03-01) und Metadaten der Aktenstücke suchen.

Hinweis: Akten werden über das API Justitia.Swiss.07 eingesehen.

FUN-03-03 Aktenstücke berechtigen Muss

Die Berechtigungsprüfung (Policy Decision Point und Policy Enforcement Point) wird auf der Plattform vor jedem Zugriff auf ein Aktenstück sichergestellt, insbesondere:

- Hat die verfahrensleitenden Justizbehörde eine Zustellung erteilt? (Policy Administration Point)?
- Ist die Zustellung gültig (Zeitraum)?
- Hat die lesende Person eine Berechtigung auf dem Profil, für welches eine Zustellung definiert wurde oder wurde das Einsichtsrecht an sie delegiert?

Die Berechtigung hat 2 mögliche Ausprägungen:

- Nur Existenz bekannt, wenn die verfahrensbeteiligte Person nur die Metadaten lesen darf. (z.B. die Existenz eines Preisplans der gegnerischen Partei)
- Inhalt sichtbar

Hinweis: Die Berechtigung «nur auf die Metadaten» wird zum Beispiel im Wettbewerbsrecht verwendet, wenn eine Gegenseite sehen soll, dass die andere Partei entsprechende Produktbeschreibungen oder Preispläne dem Gericht vorgelegt hat, diese Partei aber nicht das konkrete Design des Produkts sehen soll.

FUN-03-04 Berechtigung entziehen Muss

Zustellungen haben eine Gültigkeitsdauer, während der ein Empfänger die Aktenstücke einsehen kann. Die Gültigkeitsdauer kann auch offen sein, d.h. die Einsicht gilt unbeschränkt (bis das Verfahren gelöscht wird).

In besonderen Fällen können die Justizbehörden erteilte Berechtigungen vorzeitig entziehen.

Hinweis: Der Entzug eines Einsichtsrecht erfolgt über das API Justitia.Swiss.04.

FUN-03-05 Aktenstücke zentral vorhalten Muss

Aktenstücke können auf der Plattform vorgehalten werden. Der Zugriff auf Aktenstücke wird via FUN-03-03 berechtigt. Behörden laden ihre Aktenstücke via *Justitia.Swiss.06* auf die Plattform hoch.

Mit dem Löschen der Akte werden sämtliche zugehörige Aktenstücke entfernt.

FUN-03-06 Auf dezentrale Aktenstücke zugreifen Option

Optional können Aktenstücke anstelle zentral auf der Plattform auf IT-Systemen in Verantwortung der Justizbehörden vorgehalten werden. Die Justizbehörden implementieren dazu das API *Justitia.Swiss.05.*

Hinweis: Auch beim dezentralen Vorhalten der Aktenstücke prüft die Plattform die Berechtigung bei jeder Akteneinsicht (Siehe FUN-03-03).

FUN-03-07 Medientypen der Aktenstücke Muss

Die Plattform erlaubt Dateiformate flexibel zu kategorisieren. Dabei sind insbesondere vorzusehen:

- Durch die Justizbehörden gesiegelte PDF Dateien.

- Von den Justizbehörden bereitgestellte Medientypen (Bild, Ton). Je nach Typ des Mediums wird ein entsprechender Viewer für dieses Format zur Verfügung gestellt oder ein Benutzer kann die Dateien 'nur' herunterladen. Spezielle Viewer müssen für spezifische Formate wie Pläne oder 3-dimensionale Szenen definiert werden können.
- Spezielle Formate der Daten erlauben nur ein Siegel in eigenständigen Dateien (z.B. PKCS#7). In diesem Fall muss die Darstellung resp. der Download der Datei mit oder ohne Siegel möglich sein.

Weitere Medientypen (Bild, Ton) müssen bei Bedarf hinzugefügt werden können.

Hinweis: die Kategorisierung der Aktenstücke folgt denselben Prinzipien, wie diese auch für die Eingabe (FUN-02-01) skizziert sind.

FUN-03-08 Akten vermerken und markieren — Option

Verfahrensbeteiligte können auf der Plattform nur für sie sichtbare (oder delegierbare) Vermerke und Tags auf Akten und Aktenstücke anbringen.

Mit dem Entfernen der Akte (durch die Justizbehörden) werden die zugehörigen Tags und Vermerke ebenfalls gelöscht.

Hinweis: das Anbringen von Vermerken und Tags auf Akten soll in keiner Weise den Eindruck erwecken, dass Verfahrensbeteiligte auf der Plattform Dokumente editieren oder anderweitig bearbeiten können. Vermerke oder Tags sind viel mehr im Sinne von 'Wichtig', 'Dringend' oder ähnlich zu verstehen.

Hinweis: Tags und Vermerke auf Akten werden via API Justitia.Swiss.07 vergeben.

FUN-03-09 Video streamen — Option

Videos können als Medientyp gemäss FUN-03-07 definiert werden. Dies beinhaltet insbesondere die Möglichkeit, so zur Einsicht berechtigte Videos streamen zu können.

FUN-04 Siegelservice

Mit dem Siegelservice können Siegel an Dokumente angebracht werden und versiegelte Dokumente validiert werden.

FUN-04-01 Siegel für Justizbehörden anbringen — Option

Beim Hochladen von Dateien zur Einsicht oder Zustellung durch Justizbehörden prüft die Plattform, ob diese Dateien durch die Justizbehörden gesiegelt sind. Optional kann die Plattform die Siegelung für diese Justizbehörden direkt anbringen.

Hinweis: Dokumente werden mit dem API Justitia.Swiss.10 gesiegelt.

FUN-04-02 Siegel validieren — Muss

Die Plattform erlaubt es allen Benutzern (nicht nur den registrierten Teilnehmern) das Siegel eines verfügbaren PDF oder XML Dokuments zu validieren. Dazu wird:

- die Gültigkeit des Behördensiegels validiert.

Hinweis: Für die eigentliche Prüfung wird der Validatorservice des BIT verwendet, welcher über die Plattform eingebunden wird. Wir gehen davon aus, dass dieser Validator in Zukunft auch für weitere Dateitypen (z.B. PKCS#7) erweitert wird.

Hinweis: Dokumente werden mit dem API Justitia.Swiss.09 validiert.

FUN-05 Audit Trail

Die Audit Trail zeichnet Ereignisse (Transaktionen und Stammdatenänderungen) verbindlich und nicht-abstreitbar auf.

FUN-05-01 Ereignisse aufzeichnen Muss

Die Plattform wird rechtsverbindliche Ereignis nicht-veränderbar, authentisch und nicht-abstreitbar aufzeichnen. Diese Ereignisse sind mindestens:

- Der Abschluss einer Eingabe
- Das Übermitteln einer Zustellung mit Frist
- Das erstmalige Einsehen eines zugestellten Aktenstückes

Weitere relevante Ereignisse sind einfach konfigurierbar inklusive des Festlegens, welche Daten genau im Audit Trail aufgezeichnet werden sollen.

Für Ereignisse des Rechtsverkehrs gibt es zwei interessierte Personen als «Besitzer der zugehörigen Daten»: den Absender und den Empfänger der Übermittlung. Entsprechend werden zwei unterschiedliche Sichten auf die Ereignisse geboten. Zum Beispiel darf die Justizbehörde auf Eingaben nicht die eingeloggte Person sehen, sondern nur die handelnde Person auf dem Profil, aber bei Delegationen soll der Delegierende durchaus sehen, welche Person nun in seinem Namen eine Aktion vorgenommen hat.

FUN-05-02 Ereignisse einsehen Muss

Ereignisse können einer Person als Urheber zugeordnet werden. Im Sinne des Datenschutzes 'gehören' die Daten des Ereignisses dem Urheber, das heisst, nur er darf die Daten sehen und Zugriff auf diese gewähren.

Hinweis: die Sicht auf den Audit Trail wird mittels Justitia.Swiss.08 gegeben

FUN-05-03 Quittungen erzeugen Muss

Damit Empfänger oder Absender im ERV rechtsverbindlich und nicht-abstreitbar nachweisen können, dass ein Ereignis im ERV stattgefunden hat, stellt die Plattform basierend auf den Daten der Ereignisse Quittungen aus.

Die Quittungen werden mit kryptographischen Mitteln so abgesichert, dass Integrität und Authentizität nachgewiesen werden kann.

FUN-05-04 Audit Trail auswerten Muss

Daten des Audit Trails können durch die Körperschaft (anonymisiert) zu statistischen Zwecken ausgewertet werden. Damit können Aussagen für den Betrieb und die Weiterentwicklung der Plattform gemacht werden.

Hinweis: Aus Datenschutzgründen werden keine personalisierten Auswertungen ermöglicht, resp. diese erfordern explizit die Einwilligung des Besitzers der Daten.

FUN-06 Web Portal / API

Über das Web Portal und API können Nutzer Funktionen der Plattform nutzen.

FUN-06-01 Öffentlichkeit informieren Muss

Die Plattform enthält einen Bereich für öffentlich zugängliche Informationen und die Möglichkeit, Kontakt aufzunehmen. In diesem Bereich können mehrsprachig Text, Bilder und Videos zur Verfügung gestellt werden. Es existiert eine Preview-Möglichkeit für Änderungen (Content-Management-System).

Der Service API *Justitia.Swiss.09* zum Validieren von Siegeln (FUN-04-02) wird öffentlich angeboten.

Der öffentlich (ungesicherte) Zugang ist technisch und soweit sinnvoll physisch von der zu sichernden Funktionalität getrennt.

FUN-06-02 Sicheren Zugang über API oder Web Portal gewähren Muss

Zugang zu der gesicherten Funktionalität erfolgt ausschliesslich nach einer Authentifizierung durch einen akzeptierten IDP mit dem Sicherheitsniveau substanziell oder höher.

Dies betrifft alle APIs ausser *Justitia.Swiss.09.*

FUN-06-03 Funktionalität via API Muss

Die Funktionalität der Plattform soll via Services basierend auf einem offenen Protokoll verfügbar sein.

Das Justitia.Swiss Web Frontend wird durch eine Single Server Page bereitgestellt, die auf die APIs zugreift.

Hinweis: Damit ist die gleiche Funktionalität für das Webportal nutzbar, wie sie auch aus einem Backend genutzt wird. Gemäss FUN-07-03 wird jeder Serviceaufruf kontrolliert.

FUN-06-04 Versionierte Schnittstellen Muss

Die Plattform bietet, bis zu einem sinnvollen Grad, rückwärtskompatible und versionierte Schnittstellen an.

FUN-06-05 UX Design und Barrierefreiheit Muss

Die Darstellung des Portals muss mit adaptivem oder responsive Design auf unterschiedlichen Endgeräten lesbar sein.

Die Weboberfläche genügt den Anforderungen an Barrierefreiheit.

Die Weboberfläche ist mehrsprachig.

Das User Interface ist intuitiv nutzbar.

FUN-07 Sicherheit und Datenschutz

Die Plattform wird sehr sensitive Daten halten. Deshalb ist dem Aspekt der Sicherheit und des Datenschutzes grosses Gewicht zuzumessen. Dies bedingt organisatorische Massnahmen, ein System für die laufende Sicherheitsüberwachung und technische Massnahmen zur Sicherstellung der Vertraulichkeit und Verfügbarkeit. Die applikatorischen Anforderungen zur Sicherstellung der Integrität der Daten werden im Siegelservice und die Nachvollziehbarkeit der Ereignisse im Audit Trail beschrieben.

FUN-07-01 Organisatorische Massnahmen Muss

Detailkonzepte für Informations- und Datenschutzthemen müssen erarbeitet werden. Dies beinhaltet unter anderem:

- Datenschutzfolgeeinschätzung (Anforderung aus dem revidierten Datenschutzgesetz);

- Bearbeitungsreglement (Anforderung aus der veränderten HERMES Vorlage für ISDS-Konzepte);
- Detailkonzept für die Benutzer-, Gruppen- und Berechtigungsverwaltung;
- Detailkonzept für die Implementierung von Siegel-Service und Validator;
- Detailkonzept für die Implementierung von Audit Trail und Protokollierungs-Service;
- Vorgaben für kryptographische Algorithmen, Schlüssellängen und Schlüsselverwaltung;
- Vorgaben für die Anbindung von Identity Providern;
- Vorgaben für den Anschluss von Systemen der Justizbehörden und Anwaltskanzleien;

Der Entwicklungs- und Betriebspartner leistet für diese Konzepte wesentliche Beiträge.

Die öffentlich-rechtliche Körperschaft (örK) etabliert für die Plattform «Justitia.Swiss» ein Information Security Management System (ISMS) und lässt dieses nach ISO/IEC 27001 zertifizieren.

Etablierung eines Awareness Programms für sämtliche Nutzer und Mitarbeiter der örK, des Entwicklungspartners und des Betreibers für Sicherheitsmassnahmen.

Die örK hat ein jederzeitiges, vollumfängliches und ungehindertes Einsichts- und Prüfrecht in Bezug auf den Betrieb der Plattform «Justitia.Swiss».

Die örK beauftragt spezialisierte und unabhängige Dritte damit, die Sicherheit der Plattform «Justitia.Swiss» zu überprüfen.

Der Betriebspartner sichert den Betrieb und insbesondere die administrativen Zugänge.

FUN-07-02 Security Information and Event Management (SIEM) Muss

Die örK etabliert ein Security Information and Event Management (SIEM) und lässt dieses nach ISO/IEC 27001 zertifizieren.

Das SIEM umfasst alle nötigen Prozesse und Vorgaben für die Überwachung, Erfassung, Bewertung, Kommunikation und Eskalation von Sicherheitsvorfällen.

Das SIEM nutzt die Expertise eines Security Operation Centers (SOC) um die Sicherheitslage einer Organisation zu steuern und zu verbessern. Dabei werden Ereignisse, die einen Sicherheitsvorfall darstellen könnten, klassifiziert, priorisiert und einer Ursachenanalyse unterzogen. Dies bedingt insbesondere das Erkennen von Anomalien zwischen fachlichen und technischen Aspekten (z.B. ein versuchter Zugriff aus dem Ausland).

Die Logs aller Infrastrukturkomponenten der Plattform «Justitia.Swiss» sowie des Audit Trails werden vom Betreiber in einem zentralen Protokollierungsdienst gesammelt und für die Detektion von Sicherheitsvorfällen genutzt.

Zur koordinierten Lösung von konkreten IT-Sicherheitsvorfällen trägt ein «Computer Emergency Response Team (CERT)» bei.

FUN-07-03 Vertraulichkeit und Zugriffskontrolle sicherstellen Muss

Folgende fachliche Aspekte stellen die Authentizität der Benutzer und deren Autorisierung sicher:

- Das Design der Profile und Personen als deren Inhaber gewährleistet, dass alle im Adressverzeichnis geführten natürlichen Personen über eine bestätigte digitale Identität mit dem Sicherheitsniveau substanziell oder höher verfügen. Nur Benutzer mit entsprechender Autorisierung (Mitglieder einer Organisation oder via Delegation) können Funktionen der Plattform nutzen. Siehe alle Grobanforderung der FUN-01. Der Zugriff über APIs erfolgt bei Bedarf über technische Schlüssel.

- Die Nutzung der Plattform «Justitia.Swiss» erfordert eine starke Benutzer-Authentifizierung mit dem Sicherheitsniveau substanziell oder höher. Siehe FUN-06-02.
- Der Zugriff auf Aktenstücke wird nur gewährt, wenn von der verfahrensleitenden Justizbehörde ausreichende Einsichtsrechte hinterlegt wurden. Siehe FUN-03-03.
- Die Webapplikation der Plattform «Justitia.Swiss» bietet den Verfahrensbeteiligten einen zugriffsgeschützten persönlichen Arbeitsbereich an, in dem sie beispielsweise Eingaben vorbereiten können. Siehe FUN-02-01.

Technische Massnahmen:

- Alle über das Internet geführten Kommunikationsverbindungen sind verschlüsselt.
- Die Plattform «Justitia.Swiss» prüft alle transferierten Dateien mit Virenscan und blockiert Dateien, die nicht geprüft werden können (z.B. verschlüsselte Dateien).
- Die Plattform «Justitia.Swiss» akzeptiert verschiedene Datenformate. Die akzeptierten Datenformate sind flexibel erweiterbar und (insbesondere für die Gewährung der Sicherheit) auch einschränkbar.
- Alle Kommunikationsverbindungen aus dem Internet werden auf einer vorgelagerten Web Application Firewall (WAF) terminiert und auf schädliche Inhalte kontrolliert.
- Auf dem Applikationsserver der Plattform «Justitia.Swiss» gibt es keinen anonym (d.h. öffentlich) zugänglichen Bereich, siehe FUN-06-01.
- Daten at rest, insb. die Dateien des DossierStores mit den Kopien der einsehbaren elektronischen Aktenstücke und die angehängten Dateien von Eingaben sind verschlüsselt abgelegt. Der Zugriff auf Daten für Administrationszwecke erfolgt protokolliert.
- Kryptographische Schlüssel (u.a. für das Entschlüsseln von Dateien des DossierStores oder für verschlüsselte Kommunikation) befinden sich in einer sicheren Hardware (Hardware Security Module).

FUN-07-04 Verfügbarkeit der Business Services sicherstellen Muss

Die Verfügbarkeiten der Business Services und Datenbestände (z.B. Adressverzeichnis, Audit Trail) der der Plattform «Justitia.Swiss» werden durch entsprechende Service Level Agreements (SLA) mit dem Plattformbetreiber sichergestellt.

Die Business Services für Akteneinsicht und Rechtsverkehr sind 99.9% verfügbar.

Damit die Daten auch nach Katastrophen schnell wieder verfügbar sind, werden diese synchron in einem Backup-Rechenzentrum gespeichert.

Damit keinesfalls Daten verloren gehen, werden diese zusätzlich zur Georedundanz auch separat als Backup gesichert.

FUN-07-05 Dedizierte Hardware für Justitia.Swiss Muss

Sämtliche Softwarekomponenten des gesicherten Bereichs der Justitia.Swiss-Plattform, die nicht mit anderen Kunden geteilt werden müssen, laufen auf dedizierter Hardware.

Hinweis: Der gesicherte Bereich der Justitia.Swiss-Plattform umfasst alle Komponenten, auf denen Aktenstücke bearbeitet oder gespeichert werden. Nicht zum gesicherten Bereich der Justitia.Swiss-Plattform gehören beispielsweise anonym zugängliche, öffentliche Webseiten sowie Infrastrukturen des Anbieters, die für den Plattformbetrieb benötigt werden (z.B. Firewall-Systeme, Loghost, Überwachungssysteme u.dgl.).

FUN-08 Operation

Der Betriebspartner betreibt ein Service Desk für Nutzer als erster Ansprechpartner bei Anliegen und stellt die technische Plattform für die Daten, Rechenkapazität und Zugänge bereit.

FUN-08-01 Service Desk Muss

Der Service Desk dient als Anlaufstelle für alle Arten von Service Aufträgen der Benutzer und überwacht und steuert die Lösung von Incidents und Problemen.

Für Nutzer (insb. Privatpersonen oder Anwälte) ist der Service Desk der first-level support. Mitarbeiter von Behörden haben meistens ihre eigene Service Organisation.

Der Service-Desk leitet Probleme an die spezialisierten Einheiten weiter (namentlich Infrastruktur, Sicherheit, Entwicklung oder fachliche Abklärungen an die Körperschaft).

Der Service Desk kann im Fehlerfall von 7 Uhr bis 24 Uhr telefonisch kontaktiert werden.

Hinweis: Die Servicezeiten am Abend bis Mitternacht sind primär für Nutzer vorgesehen, damit diese die Nicht-Verfügbarkeit oder Nicht-Erreichbarkeit der Plattform einfach nachweisen können, um eine Erstreckung einer Frist zu begründen.

FUN-08-02 Entkoppelung von Infrastruktur, Daten und Applikationen Muss

Der Betriebspartner stellt in einem Plattform-as-a-Service (PaaS) Modell containerbasierte Umgebungen für den Entwicklungspartner zur Verfügung. Er stellt den laufenden Betrieb der Infrastruktur und der installierten Anwendungen gemäss Service Anforderungen (SLA) sicher.

FUN-08-03 Identitätsprovider administrieren Muss

Für die Einbindung von verschiedenen Identitätsprovidern müssen Stammdaten und/oder Konfigurationsmöglichkeiten bereitgestellt werden. Entsprechende administrative Prozesse (On- und Offboarding des Identitätsproviders, Massnahmen für Schutz der durch den Provider verwalteten Identitäten) werden unterstützt.

Ist der Identitätsprovider Administrator einer Organisation (verwaltet Behördenmitarbeiter), müssen Mappings von Funktionen und Rollen des Identitätsproviders auf Funktionen der Plattform definiert werden können

FUN-08-04 Service Management Tool Muss

Der Betriebspartner stellt sein Service Management Tool zur Verfügung mit dem Benutzer selbstständig Service Requests erfassen und die Bearbeitung ihre Requests verfolgen können.

Das Service Management Tool kann auf (z.B. für Tickets) auf die entsprechenden Daten der Personen der Plattform zugreifen.

FUN-08-05 Testumgebungen Muss

Für Testzwecke auf Seiten der Kantone und für Hersteller von Anwaltssoftwaren gibt es dezidierte Testumgebungen.