



ALTERNATIVE LINKE BERN
Postfach 504 - 3018 Bern - www.al-be.ch - Info@al-be.ch

Per Mail an
rechtsinformatik@bj.admin.ch

Bern, 15. Februar 2021

Vernehmlassungsantwort

Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ)

Sehr geehrte Damen, sehr geehrte Herren,

Die AL Bern nimmt mit dem folgenden Schreiben vom Recht Gebrauch, an der Vernehmlassung zum Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz teilzunehmen.

Die AL ist nicht grundsätzlich gegen die Einführung elektronischer Hilfsmittel und die Zurverfügungstellung digitaler Abläufe. Der vorliegende Entwurf hat aber noch schwerwiegende Mängel und bedarf dringend einer umfassender Überarbeitung.

Für Rückfragen stehen wir zur Verfügung.

Raffael Joggi

Klingsor Reimann

Christa Ammann

Alwin Egger



Stellungnahme Vernehmlassung BEKJ

Alternative Linke Bern

www.al-be.ch / info@al-be.ch

Bern, 10. Februar 2021

Inhaltsverzeichnis

1 Einleitung	3
2 Generelle Mängel des vorliegenden Gesetzesentwurfs	3
2.1. Projektorganisation und Zeitplan.....	3
2.2. Zulassung jeglicher e-Beweismittel muss möglich sein.....	3
2.3. Obligatorium für die Langzeitarchivierung von e-Urteilen fehlt.....	4
2.4. Open Government Data.....	4
3 Kommentare zu den einzelnen Artikeln	5
3.1. Zu Artikel 1.....	5
3.2. Zu Art. 3 Abs. 1.....	5
3.3. Zu Artikel 4.....	5
3.4. Zu Artikel 5.....	6
3.5. Zu Artikel 14 Abs. 3 und 4.....	6
3.6. Zu Artikel 17.....	7
3.7. Zu Artikel 18.....	8
3.8. Zu Artikel 19.....	8
3.9. Zu Artikel 21.....	9
3.10. Zu Artikel 23.....	10
3.11. Zu Artikel 25.....	10
3.12. Zu Artikel 26.....	11
3.13. Zu Artikel 27.....	12
3.14. Zu Artikel 28.....	12
3.15. Zu Artikel 29.....	13

1 Einleitung

Diese Stellungnahme zur Vernehmlassung zum BEKJ wurde durch die *Arbeitsgruppe Digitales* der Partei Alternative Linke (AL) Bern formuliert. Die Arbeitsgruppe Digitales setzt sich mit der Digitalisierung in Verwaltung, Wirtschaft und Gesellschaft auseinander und interveniert wo notwendig, so auch bei kantonalen und eidgenössischen Vernehmlassungen.

2 Generelle Mängel des vorliegenden Gesetzesentwurfs

Im Zusammenhang mit Justitia 4.0. ist anzumerken, dass das Projekt den Fokus auf die Zugangsfrage („wer hat Zugang zu Recht“) in den Mittelpunkt rücken soll. Die Digitalisierung soll dazu beitragen, dass der Zugang erleichtert oder erweitert wird und in keinem Fall, dass der Zugang erschwert wird.

Die hier vorliegende Gesetzesentwurf enthält viele Aspekte eines Anforderungskatalogs für eine Softwarelösung. Der gesetzliche Rahmen wird hier gesprengt. Im Gesetz sollten allgemeingültige und längere Zeit aufrechtzuerhaltende Grundsätze festgeschrieben werden und keine technischen Details. Da aber der vorgegebene Zeitplan offenbar keine dem legislativen Prozess nachfolgende Anforderungsanalyse zulässt, wird hier versucht alles auf einmal zu machen.

2.1. Projektorganisation und Zeitplan

Der Webseite des Projekts Justitia 4.0 ist zu entnehmen¹, dass parallel zum Gesetzgebungsprozess bereits die Ausschreibung des Umsetzungsprojekts stattfinden soll. Dies ist aus folgenden Gründen hochgradig problematisch:

- Der hier vorliegende Gesetzesvorschlag beinhaltet viele Aspekte einer Spezifikation, welche die Grundlage für die Ausschreibung darstellt. Eine massgebliche Veränderung dieser während des Gesetzgebungsprozess ist sehr wahrscheinlich. Die Voraussetzungen für die Umsetzung werden also verändert und das Projekt wird sicher finanziell unter Umständen aber auch fachlich in Schieflage geraten.
- Der Zeitplan ist gar nicht einzuhalten. Die Fristen zwischen letztmöglichen Veränderungen der zukünftigen Gesetzgebung und der Einführung sind zu kurz gehalten.

2.2. Zulassung jeglicher e-Beweismittel muss möglich sein

Mit zunehmender Digitalisierung der Rechtswelt, werden immer mehr Beweismittel nur noch in spezifischen elektronischen Formen vorliegen (digital born).²

Elektronische Beweismittel können in zahlreichen Dateiformaten und Formen (bspw. Dateien mit dazugehöriger standalone-Applikation) vorliegen. Elektronische Beweismittel müssen grundsätzlich in jeder Form von den Behörden entgegengenommen werden können.

Im BEKJ muss zwingend festgehalten werden, dass die Behörden/Gerichte keine Form von e-Beweismittel aus technischen Gründen ablehnen dürfen. Die Plattform muss alle Datei-Formate entgegennehmen. Die richterliche Beweiswürdigung ist dadurch nicht beeinträchtigt.

Die digital eingereichten Dokumente dürfen dabei in keiner Form verändert werden. Die Daten/Dateien müssen in der eingereichten Form erhalten bleiben. Natürlich muss mittels Hash-Verfahren und Datei-externer Signatur eine Quittung für die eingereichten Daten ausgestellt werden.

Die Folgen eines Ausschluss gewisser Typen von e-Beweismittel wäre für die Anwaltschaft und Rechtssuchenden fatal: Sie wäre gegebenenfalls gezwungen, elektronische Beweismittel zu verändern (konvertieren) oder müsste aufwändige Massnahmen (Gutachten, etc.) an die Hand nehmen.

Mit der Einführung von Justitia 4.0 wird nicht nur auf Anwaltsseite, sondern auch auf Behördenseite ein Mindestmass an Kenntnis der digitale Forensik zur Voraussetzung, damit gängige elektronische

1 <https://www.justitia40.ch/de/vorgehensweise/>

2 Zum Beispiel mit qualifiziertem Zeitstempel versehene Logfiles eines Webshops oder signierte E-Mails.

Beweismittel wie signierte E-Mails (eml-Format, msg-Format), signierte Word- oder LibreOffice-Dateien, signierte PDF-Dateien etc. ohne den Zuzug von Experten beurteilt werden können.

2.3. Obligatorium für die Langzeitarchivierung von e-Urteilen fehlt

Künftig werden Entscheide/Urteile in elektronischer Form ausgestellt. Es gibt Entscheide, die auch nach Jahrzehnten noch in der ursprünglichen Form konsultierbar sein müssen.³

Damit stellt sich die Frage, wie alle diese elektronisch signierten Urteile/Entscheide in eine geeignete elektronische Langzeitarchivierung überführt werden, die eine Validierung (von wem wurde das Urteil gezeichnet? Wurde das Urteil nach der Unterzeichnung verändert? etc.) auch nach Jahrzehnten ermöglicht, und zwar unabhängig von der IT-Infrastruktur der Gerichte.

Derzeit werden Urteile/Entscheide von Behörden nicht systematisch dauerhaft aufbewahrt, vielfach findet vorgängig eine historisch-wissenschaftliche Bewertung statt (bspw. Aufbewahrung nur eines Samples oder einer Selektion von Urteilen/Entscheidungen).

Heute ist es den Parteien möglich, ein Urteil in Papierform dauerhaft aufzubewahren. Ein elektronisches File hingegen ist dauerhaft nur lesbar, wenn es in eine elektronische Langzeitarchivierung überführt wird.

Das BEKJ muss die Behörden/Gerichte dazu verpflichten, sämtliche Urteile inkl. Urteilsbegründung (nicht aber zwingend das ganze Verfahrensdossier) in eine Langzeitarchivierung gemäss OAIS inkl. Signaturerhalt bzw. äquivalente Massnahmen zu überführen. Die Anforderungen an ein solches Langzeitarchiv entsprechen die Anforderungen an ein Langzeitarchiv für originär elektronische Urschriften bzw. Urkunden.

2.4. Open Government Data

Das Prinzip der offenen Verwaltungsdaten (Open Government Data) ist ein wichtiger Grundsatz für zeitgemässe E-Government Lösungen. Es besagt, dass Verwaltungsdokumente und Daten, wenn immer möglich, im Interesse der Allgemeinheit ohne jede Einschränkung zugänglich gemacht werden müssen.

In seiner Strategie für offene Verwaltungsdaten in der Schweiz 2019–2023 (Open-Government-Data-Strategie, OGD-Strategie)⁴ hat der Bundesrat die Grundsätze für einen offenen Zugang zu Verwaltungsdaten formuliert. Das BEKJ scheint diesen Richtlinien nicht Rechnung zu tragen, da darin nicht geregelt wird, wie die anfallenden Daten gemäss der Open-Government-Data-Strategie des Bundes umgesetzt werden sollen.

Die Form der Umsetzung der OGD-Strategie müsste im Gesetz zwingend erläutert werden.

3 Bspw. Gerichtliche Verbote, Ehescheidungsurteile, Adoptionsentscheide, etc.

4 <https://www.admin.ch/opc/de/federal-gazette/2019/879.pdf>

3 Kommentare zu den einzelnen Artikeln

3.1. Zu Artikel 1

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 1 Zweck und Gegenstand</i></p> <p><i>1 Dieses Gesetz bezweckt die Gewährleistung einer sicheren und einfachen elektronischen Kommunikation in der Justiz zwischen Privaten und Behörden sowie unter Behörden.</i></p> <p><i>2 Es regelt:</i></p> <ul style="list-style-type: none"><i>a. den Aufbau und Betrieb einer zentralen Plattform für die Übermittlung von elektronischen Dokumenten in der Justiz (E-Justiz-Plattform);</i><i>b. die Schaffung einer öffentlich-rechtlichen Körperschaft als Trägerschaft der Plattform;</i><i>c. allgemeine verfahrensrechtliche Aspekte der elektronischen Kommunikation und Akteneinsicht.</i>	<p><i>Art. 1 Zweck und Gegenstand</i></p> <p><i>1 Dieses Gesetz bezweckt die Gewährleistung einer sicheren und einfachen elektronischen Kommunikation in der Justiz zwischen Privaten und Behörden sowie unter Behörden.</i></p> <p><i>2 Es regelt:</i></p> <ul style="list-style-type: none"><i>a. den Aufbau und Betrieb einer zentralen Plattform für die Übermittlung von elektronischen Dokumenten in der Justiz (E-Justiz-Plattform);</i><i>b. die Schaffung einer öffentlich-rechtlichen Körperschaft als Trägerschaft der Plattform;</i><i>c. allgemeine verfahrensrechtliche Aspekte der elektronischen Kommunikation und Akteneinsicht.</i>

Zu Absatz 1

Der Aspekt der Sicherheit sollte in jedem Fall dem Wunsch nach „Einfachheit“ vorgehen.

Vorschlag: „Einfach“ streichen. Es ist zu prüfen, ob der Begriff der „Einfachheit“ mit „einheitlich geregelt“ zu ersetzen ist. Wenn „einfach“, dann in Richtung von Nutzer*innenfreundlich.

3.2. Zu Art. 3 Abs. 1

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 3 Gründung</i></p> <p><i>1 Der Bund und die Kantone gründen zum Aufbau und zum Betrieb der Plattform eine Körperschaft mit eigener Rechtspersönlichkeit. Dazu schliessen sie eine Vereinbarung ab.</i></p> <p><i>2 Der Bundesrat ist dafür zuständig, die Vereinbarung für den Bund zu genehmigen.</i></p> <p><i>3 Die Vereinbarung tritt erst in Kraft, nachdem der Bund und mindestens 18 Kantone sie genehmigt haben.</i></p>	<p><i>Art. 3 Gründung</i></p> <p><i>1 Der Bund und die Kantone gründen zum Aufbau und zum Betrieb der Plattform eine öffentlich-rechtlichen Anstalt. Dazu schliessen sie eine Vereinbarung ab.</i></p> <p><i>2 Der Bundesrat ist dafür zuständig, die Vereinbarung für den Bund zu genehmigen.</i></p> <p><i>3 Die Vereinbarung tritt erst in Kraft, nachdem der Bund und mindestens 18 Kantone sie genehmigt haben.</i></p>

Diese Plattform muss von einer öffentlich-rechtlichen Körperschaft mit eigener Rechtspersönlichkeit betrieben werden. Die derzeitige Formulierung würde auch eine privatrechtliche Körperschaft zulassen. Der Betrieb einer derart zentralen neuen Institution des schweizerischen Justizwesens durch ein Privatrechtssubjekt ist staatspolitisch und staatsrechtlich mehr als nur problematisch. Zudem regeln die Artikel 3-16 des BEKJ derart viele Einzelheiten der Trägerschaft, dass eine privatrechtliche Form der Trägerschaft nicht mehr wirklich Sinn machen würde. Die Plattform erfüllt auch ausgelagerte hoheitliche Aufgaben für die Gerichte des Bundes; der Corporate Governance Bericht des Bundesrates sieht für solche ausgelagerte hoheitliche Aufgaben des Bundes nur die Organisationsform einer öffentlich-rechtlichen Anstalt vor.

3.3. Zu Artikel 4

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 4 Subsidiäre Zuständigkeitsregelung</i></p> <p><i>Besteht keine Vereinbarung nach Artikel 3 zwischen allen 26 Kantonen und dem Bund, so sind die Artikel 6–13, 15 und 16</i></p>	<p><i>streichen</i></p>

<p><i>nicht anwendbar und der Bundesrat setzt die folgenden Stellen ein: a. eine Verwaltungseinheit der zentralen Bundesverwaltung als Trägerschaft der E-Justiz-Plattform; die Verwaltungseinheit übernimmt unter Ausnahme von Artikel 5 die Aufgaben der Körperschaft; b. einen Beirat mit Vertretungen der Kantone und des Bundes, der den Aufbau und Betrieb der Plattform fachlich begleitet.</i></p>	
--	--

Es wäre höchst problematisch, wenn die Plattform von einer Verwaltungseinheit der zentralen Bundesverwaltung betrieben würde, weil in diesem Fall der Bund Aufgaben übernehmen würde, die grundsätzlich in die kantonale Hoheit und Zuständigkeit fallen. Bei der Anlagerung der Plattform in einer Verwaltungseinheit des Bundesamt für Justiz, würde der Grundsatz der Gewaltentrennung missachtet. Zudem sollte diese Regelung in den Übergangsbestimmungen geregelt werden, weil sie keine dauerhafte Lösung darstellen darf. Beim Nichtzustandekommen der öffentlich-rechtlichen Körperschaft müsste eine grundsätzlich neue Lösung angestrebt und neu im Gesetz geregelt werden. Daher Art. 4 streichen.

3.4. Zu Artikel 5

<p><i>Entwurf</i></p> <p><i>Art. 5 Weitere Dienstleistungen Die Körperschaft kann neben der E-Justiz-Plattform weitere Dienstleistungen anbieten für die elektronische Kommunikation in Justizverfahren, insbesondere zur Durchführung von Video- und Telefonkonferenzen gemäss dem anwendbaren Verfahrensrecht.</i></p>	<p><i>Änderungsvorschlag</i></p> <p><i>streichen</i></p>
--	--

Zur „elektronischen Kommunikation in Justizverfahren“ gehört nach heutigem Verständnis auch die Publikation von Urteilen. Die Körperschaft soll deshalb auch ein Publikationsmodul für Entscheide zur Verfügung stellen können. Dieses Modul soll von der Öffentlichkeit unentgeltlich genutzt werden können (ohne Login; nach den Grundsätzen von Open Governement Data). Der Bundesrat soll die zu verwendenden Formate und Metadaten regeln können.

Was das Anbieten von Anwendungen zur Durchführung von Telefon- und Videokonferenzen betrifft, stellt sich die Frage, ob die öffentlich-rechtliche Körperschaft von ihrer Grundaufgabe her eine geeignete Trägerschaft darstellt, beruhen doch solche Anwendungen auf völlig anderen Technologien als der elektronische Rechtsverkehr. Es wäre zwar zu begrüssen, wenn schweizweit ein einheitliches und taugliches Tool für Telefon- und Videokonferenzen der Justiz und für weitere Kommunikation mit den Verwaltung bei Bund und Kantonen zur Verfügung stünde, jedoch sollte dieses wohl besser separat aufgebaut und in einem separaten Gesetz geregelt werden. Keine unnötige Komplexität.

3.5. Zu Artikel 14 Abs. 3 und 4

<p><i>Entwurf</i></p> <p><i>Art. 14 Anwendbares Recht</i></p> <p><i>1 Auf die mit der Erfüllung der Aufgaben der Körperschaft verbundenen Rechtsfragen ist Bundesrecht anwendbar, insbesondere betreffend: a. Öffentlichkeit der Verwaltung und Informationsschutz; b. öffentliche Beschaffungen; c. Archivierung; d. Rechtsweg.</i></p> <p><i>2 Die Körperschaft kann in eigenem Namen öffentliche Beschaffungen ausschreiben.</i></p> <p><i>3 Für Arbeitsverhältnisse und die damit verbundenen Fragen wie die berufliche Vorsorge gilt das Obligationenrecht.</i></p>	<p><i>Änderungsvorschlag</i></p> <p><i>streichen</i></p>
--	--

<p><i>4 Wird Personal von einem Gemeinwesen gestellt, so bleibt auf diese Arbeitsverhältnisse und die damit verbundenen Fragen dessen Recht anwendbar.</i></p> <p><i>5 Sieht das Bundesrecht einen Entscheid durch Verfügung vor, so wird diese von der Geschäftsleitung erlassen.</i></p>	
--	--

Es ist nicht stufengerecht, Arbeitsverhältnisse in diesem Gesetz zu regeln.

Viel relevanter erscheint die Regelung von Unvereinbarkeiten: Angestellte der Körperschaft können nicht gleichzeitig für die Justiz oder die Justizverwaltung arbeiten / oder: für einen anderen Bereich der Justiz oder der Justizverwaltung arbeiten

3.6. Zu Artikel 17

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 17 Adressverzeichnis</i></p> <p><i>1 Die E-Justiz-Plattform enthält ein Verzeichnis mit den Adressen, die für die Kommunikation über die Plattform verwendet werden, von: a. Behörden b. in den kantonalen Anwaltsregistern eingetragenen Rechtsanwältinnen und Rechtsanwälten; c. weiteren Personen, die zur berufsmässigen Vertretung befugt sind; d. weiteren Personen, die freiwillig mit Behörden über die Plattform kommunizieren.</i></p> <p><i>2 Die verfahrensleitenden Behörden haben Zugriff auf sämtliche Einträge im Verzeichnis.</i></p> <p><i>3 Die übrigen Benutzerinnen und Benutzer haben Zugriff auf die im Adressverzeichnis eingetragenen Adressen nach Absatz 1 Buchstabe a.</i></p>	<p><i>Art. 17 Adressverzeichnis</i></p> <p><i>1 Die E-Justiz-Plattform enthält ein Verzeichnis mit den Adressen, die für die Kommunikation über die Plattform verwendet werden, von: a. Behörden b. in den kantonalen Anwaltsregistern eingetragenen Rechtsanwältinnen und Rechtsanwälten; c. weiteren Personen, die zur berufsmässigen Vertretung befugt sind; d. weiteren Personen, die freiwillig mit Behörden über die Plattform kommunizieren und ihren Eintrag freischalten.</i></p> <p><i>2 Die verfahrensleitenden Behörden haben Zugriff auf sämtliche Einträge im Verzeichnis.</i></p> <p><i>3 Die übrigen Benutzerinnen und Benutzer haben Zugriff auf die im Adressverzeichnis eingetragenen Adressen nach Absatz 1 Buchstabe a und b.</i></p> <p><i>4. Der hier geregelte Zugriff betrifft nur das Adressverzeichnis und keinesfalls die Verfahrensdaten.</i></p>

Zu Absatz 1

Personen, die freiwillig mit Behörden über die Plattform kommunizieren (Bst. d), müssen die Möglichkeit haben, auf einen Eintrag im Adressverzeichnis zu verzichten, um sicherzustellen, dass sie weiterhin steuern können, in welchen Verfahren sie mit welchen Behörden elektronisch kommunizieren wollen (Opt-In Adressverzeichnis für Private). Dies muss auch für Anwalt*innen gelten, sofern sie an Verfahren in ihrer Eigenschaft als nicht dem BGFA unterstellte Personen teilnehmen (siehe oben Leitsatz #F3).

Zu Absatz 2

Es ist sicherzustellen, dass die betreffende Behörde im Rahmen der Einsichtnahme bezogen auf eine bestimmte Person nach Absatz 1 Bst. b-d nur Kenntnis von Verfahren erhält, in denen sie die Verfahrensleitung innehat. Diese Regelung darf nicht dazu führen, dass die Behörden über die bisherigen gesetzlichen Regelungen hinaus (bspw. Strafregister, etc.) via Plattform Informationen über Verfahrensparteien oder ihre Anwälte beschaffen können. Die Amts- und Rechtshilfeverfahren dürfen nicht durch Art. 17 Abs. 2 unterlaufen werden.

Zu Absatz 3

Benutzer*innen nach Art. 17 Abs. 1 Bst. b, c und d sollten ebenfalls Einsicht in die Adressen der Benutzer*innen nach Art. 17 Abs. 1 Bst. b haben, da die kantonalen Anwaltsregister ja auch heute öffentlich sind.

3.7. Zu Artikel 18

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 18 Benutzeroberfläche und Schnittstelle zu Fachapplikationen</i></p> <p><i>1 Die E-Justiz-Plattform stellt eine Benutzeroberfläche zur Verfügung, die über gängige Technologien erreicht und benutzt werden kann.</i></p> <p><i>2 Sie stellt eine Schnittstelle für die Anbindung von Fachapplikationen an die Plattform zur Verfügung.</i></p> <p><i>3 Das EJPD regelt die technischen Anforderungen an die Schnittstelle.</i></p>	<p><i>Art. 18 Benutzeroberfläche und Schnittstelle zu Fachapplikationen</i></p> <p><i>1 Die E-Justiz-Plattform stellt eine Benutzeroberfläche zur Verfügung, die ohne die Installation zusätzlicher Software erreicht und benutzt werden kann.</i></p> <p><i>2 Sie stellt eine offen zugängliche, dokumentierte Schnittstelle für die Anbindung von Fachapplikationen an die Plattform zur Verfügung.</i></p> <p><i>3 Das EJPD regelt die technischen Anforderungen an die Schnittstelle.</i></p>

Zu Absatz 1

Diese Regelung garantiert nicht die Nutzbarkeit der Plattform durch die mehrheitlich verwendeten Technologien. Der Begriff „gängig“ ist zu unbestimmt und weit, es darf nicht der Fall eintreten, dass die zuständige Stelle eine einzige „gängige“ Technologie für die Nutzung der Plattform als anwendbar erklärt. Die Nutzbarkeit muss betriebssystemunabhängig garantiert sein und integrierbar in verschiedene Fachanwendungen sein.

Zu Absatz 2

Diese Schnittstelle muss lückenlos dokumentiert und kostenlos zugänglich sein.

3.8. Zu Artikel 19

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 19 Authentifizierung der Benutzerinnen und Benutzer</i></p> <p><i>1 Die Benutzerinnen und Benutzer müssen sich gegenüber der E-Justiz-Plattform authentifizieren.</i></p> <p><i>2 Sie benötigen dazu eine elektronische Einheit, die zur Identifizierung natürlicher Personen verwendet wird (E-ID), auf dem Sicherheitsniveau «substanziell» oder Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz nach Artikel 4 Absatz 1 Buchstaben b und c des E-ID-Gesetzes vom 27. September 2019.</i></p> <p><i>3 Für Personen, denen keine E-ID ausgestellt werden kann, lässt der Bundesrat weitere Mittel zur Authentifizierung zu, sofern diese eine vergleichbare Sicherheit bieten.</i></p>	<p><i>Art. 19 Authentifizierung der Benutzerinnen und Benutzer</i></p> <p><i>1 Die Benutzerinnen und Benutzer müssen sich gegenüber der E-Justiz-Plattform authentifizieren.</i></p> <p><i>2 Sie benötigen dazu eine elektronische Einheit, die zur Identifizierung natürlicher Personen verwendet wird (E-ID), auf dem Sicherheitsniveau «substanziell» oder Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz nach Artikel 4 Absatz 1 Buchstaben b und c des E-ID-Gesetzes vom 27. September 2019.</i></p> <p><i>3 Für Personen, die über keine E-ID verfügen, lässt der Bundesrat weitere Mittel zur Authentifizierung zu, sofern diese eine vergleichbare Sicherheit bieten.</i></p>

Zu Absatz 2

Um den Datenschutz bzw. besondere Geheimhaltungsvorschriften respektieren zu können, ist es zwingend notwendig, dass eine natürliche Person entsprechend ihren unterschiedlichen Rollen im Verfahren mehrere E-ID's haben und zur Authentifizierung verwenden kann, ohne dass diese von der Plattform auf Doubletten geprüft und zusammengeführt werden können.

Zu Absatz 3

Eine E-ID zu besitzen und zu nutzen darf nicht verpflichtend sein. Personengruppen mit eingeschränktem oder nicht gewährtem Zugang zu einer E-ID, den notwendigen technischen Hilfsmitteln oder notwendigen Kenntnissen dürfen in keiner Weise diskriminiert werden. Der Zugang zu Gerichten muss stets für alle Rechtssuchenden hindernisfrei möglich sein.

3.9. Zu Artikel 21

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 21 Ablauf der Übermittlung</i></p> <p><i>1 Die E-Justiz-Plattform nimmt die Dokumente der Benutzerinnen und Benutzer entgegen.</i></p> <p><i>2 Werden Dokumente von einer Behörde übermittelt, so prüft die Plattform, ob die Dokumente mit einem geregelten elektronischen Siegel nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES) versehen sind. Ist dies nicht der Fall, so weist die Plattform die Dokumente zurück.</i></p> <p><i>3 Werden Dokumente von anderen Benutzerinnen und Benutzern übermittelt, so bringt die Plattform selbst ein geregeltes elektronisches Siegel nach dem ZertES an.</i></p> <p><i>4 Die Plattform stellt eine Quittung mit dem Zeitpunkt der Entgegennahme der Dokumente (Eingangsquittung) aus.</i></p> <p><i>5 Sie stellt den Adressatinnen und Adressaten die Dokumente zum Abruf zur Verfügung.</i></p> <p><i>6 Sie stellt beim erstmaligen Abruf der Dokumente eine Quittung (Abrufquittung) aus. Für jede Adressatin oder jeden Adressaten wird eine separate Abrufquittung ausgestellt.</i></p> <p><i>7 Werden zuzustellende Dokumente von einer Adressatin oder einem Adressaten bis zum Ablauf des siebten Tags nach der Übermittlung nicht abgerufen, so stellt die Plattform darüber eine Quittung aus.</i></p> <p><i>8 Die Quittungen stehen der Absenderin oder dem Absender sowie der Adressatin oder dem Adressaten zum Abruf zur Verfügung.</i></p> <p><i>9 Der Bundesrat regelt Form, Zustellung und Inhalt der Quittungen und Benachrichtigungen.</i></p>	<p><i>Art. 21 Ablauf der Übermittlung</i></p> <p><i>1 Die E-Justiz-Plattform nimmt die Dokumente der Benutzerinnen und Benutzer entgegen.</i></p> <p><i>1x Eine unabhängig von der Plattform betriebene Schnittstelle zur fristwährenden Übermittlung sowie der Postweg sind weitere Übermittlungswege.</i></p> <p><i>2 Werden Dokumente von einer Behörde übermittelt, so prüft die Plattform, ob die Dokumente mit einem geregelten elektronischen Siegel nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur (ZertES) versehen sind. Ist dies nicht der Fall, so weist die Plattform die Dokumente zurück.</i></p> <p><i>3 Werden Dokumente von anderen Benutzerinnen und Benutzern übermittelt, so erstellt die Plattform selbst ein geregeltes elektronisches Siegel neben der Originaldatei nach dem ZertES an.</i></p> <p><i>4 Die Plattform und die Übermittlungsschnittstellen stellen eine Abgabequittung mit dem Zeitpunkt der Entgegennahme der Dokumente (Eingangsquittung) aus.</i></p> <p><i>5 Sie stellt den Adressatinnen und Adressaten die Dokumente zum Abruf zur Verfügung.</i></p> <p><i>6 Sie stellt beim erstmaligen Abruf der Dokumente eine Quittung (Abrufquittung) aus. Für jede Adressatin oder jeden Adressaten wird eine separate Abrufquittung ausgestellt.</i></p> <p><i>7 Werden zuzustellende Dokumente von einer Adressatin oder einem Adressaten bis zum Ablauf des siebten Tags nach der Übermittlung nicht abgerufen, so stellt die Plattform darüber eine Quittung aus.</i></p> <p><i>8 Die Quittungen stehen der Absenderin oder dem Absender sowie der Adressatin oder dem Adressaten zum Abruf zur Verfügung.</i></p> <p><i>9 Der Bundesrat regelt Form, Zustellung und Inhalt der Quittungen und Benachrichtigungen.</i></p>

Absatz 1

Die zentrale Plattform muss zwingend alternative elektronische Übermittlungswege vorsehen, die von den Benutzenden eingesetzt werden können, wenn die Plattform nicht zur Verfügung steht. Diese alternative Übermittlung muss auf Gesetzebene geregelt werden. Denkbar wäre bspw. eine Schnittstelle, die es erlaubt, fristwährend (mit Abgabequittung) elektronische Eingaben zu übermitteln, und die Eingabe auf dem Postweg, da es theoretisch auch grössere Netzstörungen geben kann, die für die eingebende Person nicht umgehbar sind.

Absatz 3

Es kann nicht sein, dass auf die Plattform geladene Dokumente systematisch mit einem elektronischen Siegel versehen und damit verändert werden. Dieser Absatz lässt vermuten, dass der Gesetzgeber implizit annimmt, lediglich PDF-Files dürften auf die Plattform geladen werden. Ein Signaturdienst muss alle möglichen Dateiformate signieren können. Mit einer solchen Signatur ohne Speicherung der hochgeladenen unveränderten Datei kann der Beweiswert dieser Datei nachhaltig vernichtet oder vermindert werden. Die ursprünglich hochgeladenen Dokumente müssen also zwingend im Original behalten werden.

Absatz 4

Die Anwaltschaft benötigt zwingend eine **Abgabequittung** des Portals (vergleichbar mit der heutigen Postaufgabequittung bei LSI-Sendungen und vergleichbar mit der Abgabequittung im heutigen elektronischen Rechtsverkehr). Eine Empfangsquittung ist in Bezug auf die Fristwahrung irrelevant.

3.10. Zu Artikel 23

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<i>Art. 23 Validator Die Körperschaft stellt einen Validator zur Verfügung, mit welchem Personen und Behörden überprüfen können, ob die Signaturen und Zeitstempel der über die E-Justiz-Plattform ausgetauschten Dokumente und Quittungen gültig sind</i>	<i>Art. 23 Validator Die Körperschaft stellt einen Validator zur Verfügung, mit welchem Personen und Behörden überprüfen können, ob die Signaturen und Zeitstempel der über die E-Justiz-Plattform ausgetauschten Dokumente und Quittungen gültig sind. Der Validator kann auf dem eigenen Rechner ohne Datenkommunikation betrieben werden.</i>

Es ist störend, dass die heutige Validator-Lösung (www.validator.ch) keine diskrete Validierung vorsieht, obwohl dies technisch ohne Weiteres möglich ist. Die künftige Validator-Lösung muss zwingend diskret ausgestaltet sein, d.h. nur Übermittlung des Hashwertes und der Signatur, und nicht Übermittlung des ganzen Dokumentes.⁵ Die diskrete Validierung ist gesetzlich zu verankern.

3.11. Zu Artikel 25

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<i>Art. 25 1 Ist die E-Justiz-Plattform am Tag, an dem eine Frist abläuft, nicht erreichbar, so verlängert sich die Frist bis zu dem Tag, der auf den Tag folgt, an dem die Plattform erstmals wieder erreichbar ist. 2 Fällt der Folgetag auf einen Samstag, einen Sonntag oder einen vom Bundesrecht oder vom kantonalen Recht anerkannten Feiertag, so endet die Frist am nächstfolgenden Werktag. Massgebend ist das Recht des Kantons, in dem die verfahrensleitende Behörde ihren Sitz hat. 3 Die Nichterreichbarkeit der Plattform ist von der Benutzerin oder dem Benutzer glaubhaft zu machen.</i>	<i>Komplett überarbeiten</i>

Zu Absatz 1

Diese Bestimmung ist weder zielführend noch sinnvoll.

Die Gesetzgebung in der Schweiz kennt verschiedene Arten von Fristen: gesetzliche Fristen, richterliche Fristen, Verjährungsfristen und materiellrechtliche Verwirkungsfristen. Die vorliegende Bestimmung würde sich dem Wortlaut nach auf alle Arten diese Frist-Arten beziehen. Allerdings sind nicht alle dieser Fristen erstreckbar. Art. 25 wäre demnach nur dann ein Behelf, falls eine erstreckbare Frist nicht eingehalten werden kann. In den anderen Fällen hätte diese Regelung zur Folge, dass die Anwaltschaft und die Rechtssuchenden bei einem Ausfall der Plattform die entsprechende Frist auf dem elektronischen Weg nicht wahren kann, es sei denn, es werde in Art. 25 BEKJ ausdrücklich

⁵ Vgl. auch: https://www.openegov.admin.ch/egov/de/home/produkte/validieren/diskreter_validator.html: „Im Gegensatz zum Validator Service werden beim diskreten Validator die zu überprüfenden Dokumente nicht dem Webservice übergeben, sondern lediglich der berechnete Hashwert sowie die Unterschriften. Damit ist sichergestellt, dass vertrauliche Dokumente bei der Validierung den Verantwortungsbereich des Anwenders/der Anwenderin nicht verlassen.“

festgehalten, dass diese Regelung allen gesetzlichen Fristen (bundesrechtlich und kantonrechtlich) vorgeht.

Die vorgeschlagene Regelung ist weiter auch deshalb problematisch, weil der Zeitpunkt, an dem die Plattform wieder „erreichbar“ ist, nicht in jedem Fall nachträglich und objektiv erstellt werden kann und unter Umständen auch nicht für jeden Plattform-Benutzer derselbe ist. So ist denkbar, dass die Aktivitäten eines Nutzers zur vorübergehenden Sperrung seiner IP-Adresse führen (Schutz der Plattform vor Hackern), womit die Plattform nur für diese Teilnehmer nicht mehr erreichbar ist. Solche individuellen Nicht-Erreichbarkeiten können nicht über generelle gesetzliche Fristen geregelt werden.

Ist hingegen die Plattform für alle Teilnehmenden nicht erreichbar, werden alle betroffenen Teilnehmer in regelmässigen Abständen testen müssen, ob die Plattform nun wieder erreichbar ist, da dieser Zeitpunkt die Frist auslöst. Dies führt zu häufigen Anfragen an das System, die dieses unter Umständen zusätzlich belasten können.

Zu Absatz 3

Auch diese Bestimmung ist weder zielführend noch sinnvoll.

Ein Upload über die geplante Plattform kann aus unterschiedlichen Gründen fehlschlagen. Ein Browser kann im Austausch mit der Plattform Probleme verursachen. Die Plattform kann selbst Funktionsfehler aufweisen. Die Suche nach der Ursache einer Fehlfunktion ist oftmals auch für die Entwickler keine einfache Aufgabe. Für Rechtsanwält*innen ist es deshalb zentral, dass ihnen unter keinen Umständen eine Beweislast für das Nicht-Funktionieren der zentralen Plattform auferlegt wird. Funktioniert die Plattform nicht, muss immer ein alternativer Übermittlungsweg zur Verfügung stehen, der eine fristwahrende Übermittlung (elektronisch und in Papierform) ohne Zeitverlust ermöglicht (siehe Änderungsvorschlag Art 21 Abs 1x). Die Fehlersuche ist Aufgabe der Betreiber der Plattform.

Die Regelung ist auch deshalb nicht zielführend, weil im Streitfall ein Gericht nachträglich darüber entscheiden müsste, ob die Plattform erreichbar war oder nicht, ohne diese Sachfrage selber in unabhängiger Weise überprüfen und beurteilen zu können. Ein solcher Entscheid verstösst unseres Erachtens gegen Art. 30 Abs. 1 BV.

3.12. Zu Artikel 26

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 26 Datenschutz</i></p> <p><i>1 Die Daten auf der E-Justiz-Plattform sind nach schweizerischem Recht in der Schweiz zu halten und zu bearbeiten. Beigezogene Dritte, die Zugang zu den Daten erhalten, müssen schweizerischem Recht unterstehen und ihren Sitz oder Wohnsitz in der Schweiz haben.</i></p> <p><i>2 Die Körperschaft darf diejenigen Personendaten, einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofilen, bearbeiten, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. Sie darf sie nicht zu anderen Zwecken bearbeiten.</i></p> <p><i>3 Die Bestimmungen des anwendbaren Verfahrensrechts zum Datenschutz bleiben vorbehalten.</i></p> <p><i>4 Das Akteneinsichtsrecht und das Auskunftsrecht im Rahmen eines hängigen Verfahrens richten sich nach dem anwendbaren Verfahrensrecht, bei abgeschlossenen Verfahren nach dem anwendbaren Recht der Behörde, die sich zuletzt mit dem Verfahren befasst hat.</i></p> <p><i>5 Soweit die Datenbearbeitung nicht im anwendbaren Verfahrensrecht geregelt ist, richtet sich der Datenschutz: a. nach dem Bundesgesetz vom 19. Juni 1992 über den Datenschutz, wenn eine Bundesbehörde befasst ist; b. nach der kantonalen Datenschutzgesetzgebung, wenn eine</i></p>	<p><i>Art. 26 Datenschutz</i></p> <p><i>1 Die Daten auf der E-Justiz-Plattform sind nach schweizerischem Recht in der Schweiz zu halten und zu bearbeiten. Beigezogene Dritte, die Zugang zu den Daten erhalten, müssen schweizerischem Recht unterstehen und ihren Sitz oder Wohnsitz in der Schweiz haben.</i></p> <p><i>1x Die Daten müssen stets verschlüsselt aufbewahrt werden und mittels gegebener Massnahmen nur durch die berechtigten Parteien einsehbar sein.</i></p> <p><i>2 Die Körperschaft darf diejenigen Personendaten, einschliesslich besonders schützenswerter Personendaten und Persönlichkeitsprofilen, bearbeiten, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. Sie darf sie nicht zu anderen Zwecken bearbeiten.</i></p> <p><i>3 Die Bestimmungen des anwendbaren Verfahrensrechts zum Datenschutz bleiben vorbehalten.</i></p> <p><i>4 Das Akteneinsichtsrecht und das Auskunftsrecht im Rahmen eines hängigen Verfahrens richten sich nach dem anwendbaren Verfahrensrecht, bei abgeschlossenen Verfahren nach dem anwendbaren Recht der Behörde, die sich zuletzt mit dem Verfahren befasst hat.</i></p> <p><i>5 [Hinweis auf geltendes DSG]</i></p>

Zu Absatz 1

Diese Regelung ist so zu begrüssen und stellt eine unabdingbare minimale Erfordernis dar. Bearbeiten heisst hier sowohl austauschen wie auch speichern. Nicht geregelt - und das ist ein Mangel - ist, wer die Datenherrschaft über die Daten hat, welche die Plattform bearbeitet und welche allenfalls vom Betreiber der Plattform gespeichert sind.

Die Daten müssen möglichst sicher gespeichert werden. Keine Dokumente dürfen unverschlüsselt abgelegt werden. Dies erschwert massgeblich den Zugang zu den Daten im Fall einer Sicherheitslücke oder einer internen Datendiebstahls. Die Daten sind nur den für den Rechtsfall freigeschalteten Parteien mittels eines zugänglich privaten-Schlüssels zugänglich.

Absatz 5

Diese Regelung ist weder zielführend noch sinnvoll. Erstens funktioniert eine solche Regelung nie, wenn es um die Zusammenarbeit zwischen Bund und Kantonen geht; deshalb hat man im Geoinformationsgesetz das Bundesgesetz über den Datenschutz als anwendbar erklärt (Art. 11 GeolG). Zweitens schafft diese Regelung eine Lücke dort, wo die Zuständigkeit bestritten ist. Und drittens schafft die Regelung eine Lücke betreffend der Personendaten, welche die Körperschaft für ihren eigenen Betrieb bearbeitet (Art. 26 Abs. 2 BEKJ). Und viertens steht die Regelung bezüglich der Personendaten aus abgeschlossenen Verfahren im Widerspruch zu Absatz 5. Subsidiär muss das Datenschutzrecht des Bundes für Bundesbehörden gelten. In Absatz 5 ist deshalb einzig festzuhalten, dass das Bundesgesetz über den Datenschutz anwendbar ist soweit die Datenbearbeitung nicht im anwendbaren Verfahrensrecht geregelt ist.

3.13. Zu Artikel 27

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 27 Informationssicherheit</i></p> <p><i>1 Der Vorstand legt in einem Bearbeitungsreglement insbesondere die organisatorischen und technischen Massnahmen gegen unbefugtes Bearbeiten der Daten fest und regelt die automatische Protokollierung der Datenbearbeitung und der Dateneinsicht.</i></p> <p><i>2 Er bezeichnet eine Aufsicht für die Informationssicherheit. Diese überprüft die Datensicherheit der E-Justiz-Plattform regelmässig.</i></p> <p><i>3 Der Bundesrat regelt die Anforderungen an die Datensicherheit. Er berücksichtigt dabei allgemein anerkannte Standards.</i></p>	<p><i>Art. 27 Informationssicherheit</i></p> <p><i>1 streichen resp. Aus Abs. 3</i></p> <p><i>Der Bundesrat regelt die Anforderungen an die Datensicherheit. Er berücksichtigt dabei allgemein anerkannte Standards.</i></p> <p><i>2 Er bezeichnet eine Aufsicht für die Informationssicherheit. Diese überprüft die Datensicherheit der E-Justiz-Plattform regelmässig.</i></p> <p><i>3 nach Abs 1 verschoben</i></p>

Absatz 1 und Absatz 3 stehen hier in einem Widerspruch und schaffen Kompetenzkonflikte. Angesichts der Bedeutung der Plattform für das Schweizerische Justizsystem muss die Festlegung von Anforderungen betreffend die Informationssicherheit und Datensicherheit in der Zuständigkeit des Bundesrates liegen. Dies schliesst nicht aus, dass das Gesetz dem Vorstand die Befugnis gibt, *systembezogene* Ausführungsbestimmungen zu den bundesrätlichen Regelungen zu erlassen.

Allgemein anerkannte Standards sind viel zu wage.

3.14. Zu Artikel 28

<i>Entwurf</i>	<i>Änderungsvorschlag</i>
<p><i>Art. 28 Digitalisierung von physischen Dokumenten</i></p> <p><i>1 Die Behörden lesen physisch eingereichte Dokumente elektronisch ein. Ausgenommen sind Dokumente, die sich aus</i></p>	<p><i>Art. 28 Digitalisierung von physischen Dokumenten</i></p> <p><i>1 Die Behörden lesen physisch eingereichte Dokumente elektronisch ein. Ausgenommen sind Dokumente, die sich aus</i></p>

<p><i>technischen Gründen nicht dafür eignen.</i></p> <p><i>2 Sie versehen die elektronischen Dokumente mit einem qualifizierten Zeitstempel nach dem ZertES.</i></p> <p><i>3 Die elektronischen Dokumente gelten im Verfahren als massgebliche Version.</i></p> <p><i>4 Der Bundesrat regelt das Digitalisierungsverfahren.</i></p>	<p><i>technischen Gründen nicht dafür eignen.</i></p> <p><i>2 Sie versehen die elektronischen Dokumente mit einem qualifizierten Zeitstempel nach dem ZertES.</i></p> <p><i>3 Die elektronischen Dokumente gelten im Verfahren als massgebliche Version.</i></p> <p><i>4 Der Bundesrat regelt das Digitalisierungsverfahren.</i></p>
--	--

Die Rechtsetzungs-Delegation an den Bundesrat zur Regelung des Digitalisierungsverfahrens darf nicht bedeuten, dass dieser bezüglich der Art, der Form und des Formats physisch einzureichender Dokumente Vorgaben machen kann. Dies ist im Gesetz selber oder in der Botschaft ausdrücklich festzuhalten.

Die Anwaltschaft geht davon aus, dass die Haftung für durch Behörden fehlerhaft eingescannte Dokumente ausschliesslich bei den Behörden liegt. Daher müssen die physischen Dokumente zwingend bis zum Abschluss des Verfahrens einbehalten werden.

Es muss stets gewährleistet werden das physische Dokument beiziehen zu können.

Es gibt auch Dokumente, die aus rechtlichen Gründen nicht eingesehen werden dürfen.

3.15. Zu Artikel 29

<p><i>Entwurf</i></p> <p><i>Art. 29 Rücksendung von physischen Dokumenten</i></p> <p><i>1 Die physisch eingereichten Dokumente werden nach ihrer Digitalisierung zurückgesendet.</i></p> <p><i>2 Werden die Dokumente im Verfahren benötigt, wird die Rücksendung aufgeschoben.</i></p>	<p><i>Änderungsvorschlag</i></p> <p><i>Art. 29 Rücksendung von physischen Dokumenten</i></p> <p><i>1 Die physisch eingereichten Dokumente werden nach ihrer Digitalisierung einbehalten. Jede Partei kann die Konsultierung im Verfahren jederzeit verlangen.</i></p> <p><i>2 Die Dokumente werden nach Beendigung des Verfahrens zurückgeschickt.</i></p>
---	--

Die physisch eingereichten Dokumente sollen erst nach Beendigung des Verfahrens bzw. Rechtskraft des Entscheides zurückgesendet werden, da es im laufenden Verfahren jederzeit möglich sein muss, allfällige Scanfehler nachvollziehen zu können oder analoge Originale aus anderen Gründen nochmals physisch vorzulegen.