EJPD - Bundesamt für Justiz
Bundesrain 20
3003 Bern

PDF und Word-Version per E-Mail
an: rechtsinformatik@bj.admin.ch

Zürich, 25. Februar 2021

Vernehmlassung zum Entwurf eines Bundesgesetzes über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Am 11. November 2020 wurde die Vernehmlassung zum oben genannten Entwurf eröffnet. Die Schweizerische Sektion der Internationalen Juristenkommission (ICJ-CH) setzt sich für die Prinzipien des Rechtsstaates und die Grundrechte der Einzelnen ein. Der vorgelegte Entwurf berührt diese Themen. Wir danken Ihnen deshalb für die Einladung zur Vernehmlassung und nehmen gern Stellung innert der angesetzten Frist bis 26. Februar 2021.

Die Digitalisierung der Kommunikation mit und unter den Justizorganen der Zivil- und der Strafrechtspflege in der Schweiz ist geeignet, die Effizienz der Gerichtsverfahren zu verbessern. Sie liegt im Interesse der Rechtsuchenden und dient damit dem öffentlichen Interesse. Das Ziel der Vorlage ist daher aus der Sicht der ICJ-CH sehr unterstützungswürdig. Die ICJ-CH möchte jedoch auf einige problematische Aspekte der Vorlage eingehen, wo sie Klärungsbedarf und Verbesserungspotential sieht. Zunächst stellt sich die Frage, ob die Vorlage mit der bundesstaatlichen **Kompetenzverteilung** der Bundesverfassung in Einklang steht. Die ICJ-CH sieht hier einen erheblichen Klärungsbedarf und weist auf Argumente für und gegen die Kompetenzmässigkeit hin (Ziff. 1). Weiter bringt die Vorlage in der jetzigen Fassung die Beschränkung von mehreren grund- und menschenrechtlichen Garantien mit sich, bei welchen Klärungs– und Verbesserungsvorschläge eingehend geprüft werden sollten (Ziff. 2). Diese Vorschläge beziehen sich insbesondere auf die Beschränkung der **Wirtschaftsfreiheit** für berufsmässig handelnde Personen durch das vorgesehene Obligatorium der elektronischen Übermittlung und auf die Wahrung des **Berufsgeheimnisses** nach Art. 321 StGB und Art. 47 BankG. Klärungen sind zudem aufgrund des grund- und menschenrechtlichen Anspruchs auf einen **effektiven Rechtsschutz** angezeigt. Zu-

Schweizerische Sektion der Internationalen Juristenkommission
c/o KnoeAG, Wiesen 2488
9100 Herisau
www.icj-ch.org

dem sieht die Vorlage keine wirksamen **datenschutzrechtlichen Sicherungen** vor. Schliesslich soll mit der Plattform eine riskante **«kritische Infrastruktur»** geschaffen werden, wofür ebenfalls weitere Sicherungen geprüft werden sollten (Ziff. 3).

1. Fragliche Kompetenz des Bundes

In den Erläuterungen zum Vorentwurf wird in Bezug auf die Kompetenzen des Bundes zum Erlass des Bundesgesetzes über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) ausgeführt, dass sich die Vorlage zum einen auf Art. 92 BV über das Post- und Fernmeldewesen stütze, da eine Körperschaft mit der Aufgabe gegründet werde, eine Plattform für die elektronische Kommunikation in der Justiz aufzubauen. Zum anderen stützt sich nach den Erläuterungen das Obligatorium für den elektronischen Rechtsverkehr auf Art. 122 Abs. 1 und Art. 123 Abs. 1 BV, die den Bund zur Gesetzgebung auf dem Gebiet des Zivil-, Straf- und Militärstrafprozessrechts ermächtigen. Soweit das Obligatorium auch Private erfasse, sei der Bund gemäss Art. 95 Abs. 1 BV zuständig (vgl. Erläuterungen VE-BEKJ, S. 48).

In Bezug auf die Einführung des unmittelbar geltenden Obligatoriums für den elektronischen Rechtsverkehr in der Zivil- und Strafrechtsjustiz für die Kantone stellt sich jedoch die Frage, ob dieses von den Kompetenzen des Bundes in Art. 122 und 123 BV gedeckt ist. Zu dieser Frage nehmen die Erläuterungen nicht eingehend Stellung, weshalb hier Klärungsbedarf besteht.

Für das Bestehen der Kompetenz des Bundes kann auf die umfassende bundesrechtliche Zuständigkeit zur Gesetzgebung auf dem Gebiet des Zivil- und Strafprozessrechts gemäss Art. 122 Abs. 1 und Art. 123 Abs. 1 BV verwiesen werden. Diese Kompetenzen können so interpretiert werden, dass sie auch die Zuständigkeit zur Bestimmung des Mediums der Kommunikation (mündlich, Papierform, elektronisch) umfassen. Es kann argumentiert werden, dass die elektronische Kommunikation auch in den zulässigen Regelungsbereich gehört. Zudem sprechen für die Kompetenz des Bundes die Gesetzesvorbehalte in Art. 122 Abs. 2 BV und Art. 123 Abs. 2 BV. Diese gesetzliche Grundlage wird mit dem BEKJ geschaffen. Die Verneinung einer Bundeskompetenz würde im Ergebnis zu einer teilweisen Rückkehr zu einer kantonalen Zivil- und Strafprozessordnung führen.

Gegen das Bestehen der bundesrechtlichen Kompetenz spricht, dass die Bundesverfassung in Art. 122 Abs. 2 und in Art. 123 Abs. 2 primär die Kantone für die Organisation der Gerichte und die Rechtsprechung in Zivilsachen und in Strafsachen zuständig erklärt. Die regionale Gliederung, die Festlegung der Zuständigkeiten, die Bestellung der Gerichte sowie deren Organisation ist Sache der Kantone (vgl. Christoph Leuenberger, in: Ehrenzeller et al., Hrsg., Die schweizerische Bundesverfassung, St. Galler Kommentar (St. Galler Kommentar BV), 3. Aufl., Zürich/St. Gallen 2014, Art. 122, Rz. 23; Giovanni Biaggini, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Aufl., Zürich 2017, Art. 122, Rz. 6). Die Gerichtsorganisation umfasst insbesondere auch die Festlegung der konkreten Arbeitsweise der Gerichte (Tarkan Göksu, in: Waldmann et al., Hrsg., Basler Kommentar Bundesverfassung (BSK BV), Basel 2015, Art. 122, Rz. 30), was deren technische und finanzielle Ausstattung mitumfasst. Diese kantonalen Zuständigkeiten sind Ausdruck der in Art. 47 BV garantierten kantonalen Autonomie, welche die Aufgaben-, Organisations- und Finanzautonomie umfasst (Biaggini, a.a.O., Art. 122, Rz. 6 oder Hans Vest, St. Galler Kommentar BV, Art. 123, Rz. 10). Art. 122 Abs. 2 und Art. 123 Abs. 2 BV ermöglichen es dem Bundesgesetzgeber zwar, in die kantonale Organisationsautonomie der Justiz einzugreifen, jedoch ist diese Möglichkeit mit Blick auf die Materialien eng auszulegen (mit entsprechenden Hinweisen vgl. Leuenberger, a.a.O., Art. 122, Rz. 26; Biaggini, a.a.O., Art. 122, Rz. 6). Nach der

Praxis des Bundesgerichts und der Lehre soll dies nur in Fällen erfolgen, in denen die richtige und einheitliche Anwendung des Bundesrechts einen solchen Eingriff erfordert (Leuenberger, a.a.O., Art. 122, Rz. 26; Biaggini, a.a.O., Art. 122, Rz. 6; Göksu, a.a.O., Art. 122, Rz. 32; Patricia Egli, St. Galler Kommentar BV, Art. 47, Rz. 21, unter anderem mit Verweis auf BGE 128 I 254 E. 3.8.2, 264 f.). Dass eine bundesrechtliche Harmonisierung einer Frage im Allgemeinen wünschbar oder sachgemässer und vernünftiger ist, genügt entsprechend nicht (Göksu, a.a.O., Art. 122, Rz. 32). Mit Blick auf die verfassungsrechtliche Aufgabenteilung ist daher die Kompetenz des Bundes vorliegend fraglich, denn es geht mit der generellen Verpflichtung der Justiz im Bund und den Kantonen zur Digitalisierung nicht um die Gewährleistung der einheitlichen Anwendung des Bundeszivilprozessrechts und des Bundesstrafprozessrechts. Deshalb besteht in diesem Punkt Klärungs- und Verbesserungsbedarf. Der verfassungsrechtlich mögliche Weg wäre eine durch den kantonalen Gesetzgeber geschaffene interkantonale Vereinbarung, mit der sich der Bund verbinden kann (vgl. Art. 48 Abs. 1 – 4 BV).

2. Grund- und menschenrechtliche Probleme

Mit Blick auf die Schaffung einer öffentlich-rechtlichen Körperschaft als Trägerschaft der geplanten Plattform sollte verdeutlicht werden, dass diese **staatliche Aufgaben wahrnimmt und damit gestützt auf Art. 35 Abs. 2 BV an die Grundrechte gebunden** ist. Dies gilt auch, wenn sie weitere Dienstleistungen im Sinne von Art. 5 VE-BEKJ anbietet. Es geht namentlich um folgende Grund- und Menschenrechte:

a) Um die Berufs- und Wirtschaftsfreiheit der Anwältinnen und Anwälte oder Notarinnen und Notare und Personen weiterer Rechtsberufe.
b) Um den Schutz des Berufsgeheimnisses, welches menschenrechtlich aus dem Persönlichkeitsschutz von Art. 8 EMRK und Art. 14 UNO-Pakt II abgeleitet wird.
c) Um den grund- und menschenrechtlichen Anspruch auf einen effektiven Zugang zu den Gerichten, der namentlich aus Art. 29 und 30 BV, aus Art. 6 und 13 EMRK und Art. 14 UNO-Pakt II sowie den entsprechenden Garantien der EU-Grundrechtscharta, welche die Schweiz etwa im Anwendungsbereich des Freizügigkeitsabkommens über den freien Personenverkehr mitbeachten muss.
d) Um das Grund- und Menschenrecht auf informationelle Selbstbestimmung und den Persönlichkeitsschutz nach Art. 13 BV und Art. 8 EMRK sowie nach der von der Schweiz ratifizierten, revidierten Datenschutzkonvention des Europarates (SR 0.235.1), samt Zusatzprotokoll (SR.0.235.11) sowie der für die Schweiz vielfach massgeblichen DS-GVO Datenschutz-Grundverordnung der EU.

2.1. Eingriff in die Berufs- und Wirtschaftsfreiheit der Personen in der Rechtsberatung

Das vorgesehene Obligatorium der elektronischen Übermittlung für berufsmässig handelnde Personen stellt eine **Beschränkung ihrer Wirtschaftsfreiheit** (Art. 27 BV) dar. Diese hat für ihre Rechtmässigkeit den Grundsatz der Verhältnismässigkeit zu wahren und muss insbesondere für die Erreichung des öffentlichen Interesses notwendig sein. Staatliche Eingriffe in Freiheitsrechte haben zu unterbleiben, wenn sie für die Erreichung des angestrebten Ziels nicht erforderlich sind. Falls also eine gleich geeignete, aber mildere Massnahme für den angestrebten Zweck ausreichen würde, muss diese angewendet werden. Eingriffe dürfen in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht über das Notwendige hinausgehen (vgl. Rainer Schweizer, St. Galler Kommentar BV, Art. 36, Rz. 39; Häfelin et al., Schweizerisches Bundesstaatsrecht, Zürich 2020, 10. Aufl., Rz. 322.). Im erläuternden Bericht zum Entwurf wird nicht klar, weshalb die Möglichkeit der freiwilligen elektronischen Kommunikation für alle Personen nicht eine mildere

Massnahme als das Obligatorium darstellt. Die derzeitig noch seltene Nutzung der elektronischen Kommunikation hängt auch von unterschiedlichen Faktoren auf Seiten der Behörden ab, z.B. mangelnde elektronische staatliche Infrastruktur, mangelnde Datensicherheit und nicht effiziente staatliche Be- resp. Weiterverarbeitung der elektronischen Eingaben. Mit einer Verbesserung dieser staatlichen Rahmenbedingungen ist auch mit einer Zunahme der Nutzung der elektronischen Kommunikation der privaten Parteien zu rechnen, ohne dass dafür ein Obligatorium für die berufsmässig handelnden Personen notwendig wäre. Das Potential von milderen Massnahmen scheint daher in diesem Bereich noch nicht ausgeschöpft. Als Verbesserungsmöglichkeit sollte daher die vorerst freiwillige Nutzung der elektronischen Kommunikation auch für berufsmässig handelnde Personen geprüft werden.

2.2. Gefährdung des Berufsgeheimnisses nach Art. 321 StGB und Art. 47 BankG

Im Übrigen ist das Obligatorium ein schwerer Eingriff für alle Personen in Rechtsberatungsberufen, weil viele heute jedenfalls sehr berechtigte Bedenken haben wegen der Gefahr von Verletzungen des Berufsgeheimnisses durch und in der digitalen Kommunikation. Nun hat die Vorlage zur Folge, dass die Kommunikation mit der Justiz in hängigen und abgeschlossenen Verfahren wesentlich über die Plattform verläuft oder über sog. Gruppenadministratoren (vgl. Art. 17 – 24 VE-BEKJ). Voraussetzung, dass das Berufsgeheimnis von Art. 321 StGB seitens einer Anwältin oder eines Anwalts (oder das von Bankmitarbeitenden nach Art. 47 BankG) gegenüber der oder dem Geheimnisträger/in eingehalten werden kann, ist aber, dass die Personen, denen «die Information zur Kenntnis gebracht werden, zum Kreis der zum Wissen Berufenen gehören», was nur «dann der Fall ist, wenn die Offenbarung des Geheimnisses gegenüber diesen Personen für die sachgerechte Erledigung der vom primären Geheimnisträger unabdingbar und für den Geheimnisherrn voraussehbar ist.» (Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), 2016, S. 32); das muss jedenfalls bei **Gruppenverwaltern**, welche ja private Geschäftsleute sein werden, sehr bezweifelt werden.

2.3. Gewährleistung der grund- und menschenrechtlichen Garantie eines wirksamen Zugangs zum Gericht

Um die grund- und menschenrechtliche Garantie eines wirksamen Zugangs zum Gericht zu gewährleisten, muss als Klärung ausdrücklich festgehalten werden, dass in allen Verfahren und Instanzen das Recht gewahrt ist, **bis zum Endentscheid physisch** und nicht digital mit der Justiz kommunizieren zu können und dass daraus diesen Personen **keine zusätzlichen Kosten** entstehen. Insbesondere sollte – analog Art. 138 Abs. 1 ZPO nach VE-BEKJ – klargestellt werden, dass die Zustellung von Vorladungen, Verfügungen und Entscheiden bei Personen, die nicht über die E-Justiz-Plattform kommunizieren, durch eingeschriebene Postsendungen oder auf andere Weise gegen Empfangsbestätigung erfolgt. Aus der in Art. 28 VE-BEKJ vorgesehenen Digitalisierung bei physisch eingereichten Eingaben bei der Justiz dürfen keine zusätzlichen Kosten für die Parteien entstehen.

2.4. Erhebliche Beeinträchtigungen des Datenschutzes

Es wird argumentiert, dass der VE das Datenschutzgesetz vorbehält. Dieser Verweis allein genügt aber nicht, um einen wirksamen Datenschutz zu gewährleisten, weil das Datenschutzrecht verschiedene qualifizierte Schutzregeln vorsieht, die durch das jeweilige bereichsspezifische Gesetz überhaupt erst zur Anwendung gebracht werden müssen. Das gilt nicht nur für das neue Datenschutzgesetz des Bundes vom 25. September 2020, sondern auch für alle kantonalen Datenschutzgesetze, denn die Justiz in den Kantonen, die einen zentralen Teil der kantonalen

Staatstätigkeit ausmacht, untersteht den kantonalen Datenschutzrechten (vgl. Art. 26 Abs. 5 VE-BEKJ). Diese Feststellung ist besonders deshalb wichtig, weil den kantonalen Datenschutzbehörden volle Kontrollkompetenzen obliegen, die ihrerseits der kantonalen parlamentarischen Oberaufsicht unterstehen.

In Bezug auf die betroffenen Personen ist klar, dass im Rahmen der elektronischen Kommunikation in der Justiz selbstverständlich und vor allem Personendaten im Sinne des revDSG (Bundesgesetz über den Datenschutz vom 25. September 2020) bearbeitet werden, d.h. Angaben, die sich auf eine bestimmte oder eine bestimmbare natürliche Person beziehen (Art. 5 lit. a rev DSG). Und es ist auch selbstverständlich davon auszugehen, dass sehr oft **besonders schützenswerte Personendaten** (Art. 5 lit. c revDSG) Gegenstand der elektronischen Kommunikation sein werden. Wenn die Personendaten zudem automatisiert bearbeitet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, ist die Bearbeitung als Profiling im Sinne von Art. 5 lit. f revDSG zu werten. Bringt das Profiling ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, liegt zudem ein Profiling mit hohem Risiko vor (Art. 5 lit. g revDSG). Für die Bearbeitung besonders schützenswerter Personendaten und das Profiling durch ein Bundesorgan bedarf es einer ausdrücklichen Einwilligung nach entsprechender Information (Art. 6 Abs. 7 revDSG). Dabei gilt es zu beachten, dass gerade durch den Austausch und die Verknüpfung von Daten, die für sich allein genommen (noch) nicht als besonders schützenswert erscheinen müssen, eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben können und daher ein Profiling mit hohem Risiko darstellen (vgl. Olivier Heuberger, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Diss. 2020, S. 43 ff., 123 ff.). Das Bearbeiten aller dieser Daten stellt einen Eingriff in die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar und bedarf daher immer einer gesetzlichen Grundlage (Art. 36 Abs. 1 BV, Art. 5 Abs. 1 BV); wenn es um besonders schützenswerte Personendaten geht, ist dies in aller Regel ein schwerer Grundrechtseingriff nach Art. 36 Abs. 1 2. Satz BV. Zudem muss jedes Bearbeiten im öffentlichen Interesse sein und das Verhältnismässigkeitsprinzip sowie den Kerngehalt des Grundrechts wahren (Art. 36 Abs. 2-4 BV) (vgl. dazu eingehend Rainer Schweizer/David Rechsteiner, Grund- und menschenrechtlicher Datenschutz, in: Passadelis/Rosenthal/Thür, Hrsg., Datenschutzrecht, Basel 2015, § 2 Rz. 2.2 ff.).

Auch wenn mit dem vorgeschlagenen Bundesgesetz eine gesetzliche Grundlage vorliegen würde**,** so müssen dennoch weitere Grundsätze beachtet werden, die sich zum einen aus der Bundesverfassung und zum anderen aus den Grundsätzen des DSG ergeben. Dazu zählen (vgl. auch Eva-Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, § 12 Rz. 94; Astrid Epiney/Daniela Nüesch, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis/Rosenthal/Thür, Hrsg., Datenschutzrecht, Basel 2015, § 3 Rz. 3.58 ff.):

Verhältnismässigkeit (Art. 5 Abs. 2 BV, Art. 36 Abs. 3 BV, Art. 6 Abs. 2 revDSG): Die Bearbeitung von Personendaten muss den Anforderungen des Verhältnismässigkeitsgrundsatzes genügen. Ein Verhalten ist verhältnismässig, wenn die staatliche Massnahme geeignet ist, das angestrebte Ziel zu erreichen und sie die privaten Interessen sowohl in sachlicher, räumlicher, zeitlicher wie auch in persönlicher Hinsicht bestmöglich schont. Schliesslich muss auch eine geeignete und notwendige Massnahme durch überwiegende staatliche Interessen gerechtfertigt und für den Einzelnen zumutbar sein. Gerade weil vorliegend die gesetzlichen Vorgaben der Datenbearbeitung sehr allgemein gehalten sind, kommt dem Verhältnismässigkeitsprinzip eine wichtige Stellung zu (Belser/Epiney/Waldmann, a.a.O., § 13 Rz. 49). Allein eine strikte Anwendung des Ver-

hältnismässigkeitsprinzips vermag die Unbestimmtheit der Erlaubnisnorm in gewissem Umfang zu kompensieren (BGE 132 I 49 E. 6.2). Entsprechend dürfen nur diejenigen Personendaten weiterbearbeitet werden, die für die Erfüllung der spezifischen gesetzlichen Aufgabe in persönlicher, sachlicher und zeitlicher Hinsicht geeignet und erforderlich sind. Dem Grundsatz zuwider läuft insbesondere die Datenbekanntgabe und –bearbeitung **„auf Vorrat"**. Daten dürfen also grundsätzlich nur im tatsächlich notwendigen Umfang bekanntgegeben und bearbeitet werden. Diese Forderungen aus dem Grundsatz der Verhältnismässigkeit kommen in der Regelung zu wenig zum Ausdruck. Insbesondere finden sich keine klaren Einschränkungen in Bezug auf die Möglichkeiten des Zugriffs auf die Daten, welche geeignet und notwendig zur Erreichung des gesetzlich vorgegebenen Zwecks sind. In diesem Zusammenhang erscheint auch die Möglichkeit einer Gruppenverwaltung in Art. 24 VE-BEKJ problematisch.

Zweckidentität und Transparenz: Die Grundsätze der Zweckidentität (oder Zweckbindung) und der Transparenz bilden Kernelemente des Datenschutzes. Das konkrete Ziel jeder Bearbeitung von Personendaten muss im Voraus bestimmt und für die betroffene Person erkennbar, transparent sein (Art. 6 Abs. 3 revDSG). Die Behörde ist sodann bei der Datenbeschaffung wie auch bei allen darauffolgenden Datenbearbeitungsvorgängen daran gebunden. Für die Bekanntgabe von Personendaten gilt daher, dass diese dem Zweck der ursprünglichen Beschaffung entsprechen und für die Person transparent sein muss, was sich schliesslich auch aus dem **Gebot von Treu und Glauben** ergibt (Art. 6 Abs. 2 revDSG). Wo die Behörde sich nicht an das einmal bestimmte Ziel der Datenbearbeitung hält, liegt eine unzulässige Zweckentfremdung von Personendaten vor (Epiney/Nüesch, a.a.O., § 3 Rz. 3.81 ff.; Belser/Epiney/Waldmann, a.a.O., § 12 Rz. 86). Ein wirksamer Datenschutz setzt daher grundsätzlich voraus, dass die bei den verschiedenen staatlichen Organen vorhandenen Personendaten im Sinne einer „informationellen Gewaltenteilung" getrennt und unverknüpft bleiben (Belser/Epiney/Waldmann, a.a.O., § 12 Rz. 86). Im Rahmen des vorgeschlagenen Gesetzes sind die Daten daher einzig für die elektronische Kommunikation in einem bestimmten Verfahren an die angegebenen Adressaten zu bearbeiten. Diese Beschränkung in der Bearbeitung ist im Gesetz selbst klarzustellen.

Für das **Profiling**, z.B. von einer bestimmten privaten Partei, einem Anwalt oder einem sonst beteiligten Menschen **fehlt** den Justizbehörden in Bund und Kantonen, mit Ausnahme der Staatsanwaltschaften in dem strafprozessualen Ermittlungs- und Untersuchungsverfahren, **eine gesetzliche Grundlage;** und eine Einwilligung der betroffenen Person ist auch in den Zwängen eines Gerichtsverfahrens oft nicht rechtmässig zu bekommen, wenn auf die Fairness im Verfahren geachtet wird. Wir empfehlen, dass jegliches Profiling - ausserhalb eines laufenden Strafverfahrens, das Vergehen und Verbrechen betrifft -, explizit als unzulässig erklärt wird. En d'autres termes : En particulier, pour ce qui concerne la protection de données : à l'art. 26 de la loi devrait être ajouté un alinéa qui exclut expressément la faculté de la corporation de faire du profilage, y compris du profilage à risque élevé, au sens de la loi fédérale du 25 septembre 2020 sur la protection des données (LPD) et à rendre des décisions individuelles automatisées selon l'art. 21 LPD.

Das **Gebot der Richtigkeit und Vollständigkeit der Datenbearbeitung** wird in der Justizarbeit besonders wichtig: Die bearbeiteten Daten müssen richtig und nach Massgabe der Verwendung vollständig sein (Art. 6 Abs. 5 revDSG). Mit Blick auf die Vollständigkeit ist problematisch, dass gemäss Art. 28 Abs. 1 VE-BEKJ physisch eingereichte Dokumente, die sich aus technischen Gründen nicht dafür eignen, nicht digitalisiert und daher auch nicht elektronisch übermittelt werden können (physische Beweismittel, übergrosse Dokumente, Pläne, handschriftliche Dokumente).

2.5. Datenschutzdefizit im internationalen Justizverkehr, insbesondere mit der EU

Die Vorlage wurde offenbar erstellt, ohne das rechtliche Umfeld der Schweiz genau anzuschauen. Der digitale Informationsverkehr über Personen in einem EU-Mitgliedstaat mit der Schweiz muss im Einzelnen die Anforderungen von **Art. 44 – 49 DS-GVO** Datenschutz-Grundverordnung VO (EU) 2016/679 sowie der für den Sicherheitsraum von Schengen massgeblichen Richtlinie 2016/680 (vgl. dazu SR 0.362.380.079) erfüllen. Es fehlen nach Art. 47 DS-GVO namentlich Sicherungen für eine strikte Zweckbindung, präzise gesetzlich festgelegte Bearbeitungsbefugnisse sowie Begrenzungen der Speicherdauer. Besonders kritisch ist Art. 48 DS-GVO, der verlangt, dass ein Gericht oder eine Verwaltungsbehörde (also Staatsanwaltschaften) in einem Drittstaat wie der Schweiz nicht eine Offenlegung von personenbezogenen Daten von einem Verantwortlichen oder Auftraggeber in der EU verlangen darf, es sei denn, es bestehe ein völkerrechtlicher Vertrag für die Übermittlung oder es liege ein Ausnahmefall nach Art. 49 DS-GVO vor. Im Lichte der Erwägungsgründe von Art. 104 – 155 DS-GVO bietet die geplante Plattform wohl kaum einen dem EU-Datenschutzrecht entsprechenden Datenschutz und wird somit kaum eine Bestätigung der Äquivalenz des Datenschutzes durch die EU-Kommission bekommen (vgl. Peter Gola, Hrsg., Datenschutz-Grundverordnung VO [EU] 2016679, Kommentar, 2. Aufl. 2018, Art. 48 passim). Und weil mit den EU-Mitgliedstaaten keine Staatsverträge für die Gerichtskommunikation bestehen, wie sie Art. 48 DS-GVO fordert, abgesehen von speziellen Amts- und Rechtshilfeabkommen, lässt sich der Verkehr, etwa bezüglich der Sozialversicherungen (dazu Stephan Breitenmoser/Robert Weyeneth, Europarecht. Unter Einbezug des Verhältnisses Schweiz-EU, 4. Aufl., 2021, 217/8) zwischen der Justiz in der Schweiz und den EU-Mitgliedstaaten bzw. deren Justizorganen, Anwaltschaft, Privatpersonen und Unternehmen kaum digitalisieren, auch nicht, wenn die Ausländerinnen und Ausländer ein Zustelldomizil oder Gruppenadministratoren in der Schweiz dazu vorsehen.

3. Cybersicherheit

Die geplante Plattform ist von vorneherein ein riesiges Projekt, das als hoch riskant zu qualifizieren ist. Sie stellt für die Schweiz eine neue, ganz **zentrale kritische Infrastruktur** dar und sie bietet zugleich auch besonders heikle digitale Dienste an (vgl. Klaus Beucher/Maike Fromageau/Theresa Ehlen, in: Dennis-Kenji Kipker, Hrsg., Cybersecurity, München 2020, S. 355 ff.). Zum Begriff der "kritischen Infrastruktur" ist anzumerken, dass die geplante Plattform nach den internationalen Definitionen auf jeden Fall in diese Kategorie fällt, weil sie Dienstleistungen für mehr als 500'000 Menschen anbietet. Zudem muss sie als eine "kritische Infrastruktur im besonderen öffentlichen Interesse" bezeichnet werden. Die EU hat für eine solche IT-Infrastruktur und einen solchen Dienstanbieter namentlich die Richtlinie 2016/1148 vom 6.7.2016 über die Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen sowie danach die Cybersecurity-Verordnung 2019/881 der EU erlassen, die im vorliegenden Projekt hätte beachtet werden müssen; das geltende Recht, wie z.B. die auf das RVOG abgestützte Bundesinformatikverordnung von 2000 bietet nicht genügende Sicherheitsregeln. Das BEKJ müsste ein Bündel spezieller gesetzlicher Schutz- und Sicherheitsvorschriften zur Abwehr von Cybercrime enthalten, analog dem auf Bundesebene für grosse Informationssysteme geltenden System. Zum Vergleich sei auf die Sicherheitsanforderungen von eu-LISA, dem Betriebssystem des erneuerten Schengen-Informations-System (SIS) hingewiesen (Art. 15-18 der Verordnung (EU) 2018/1861 vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS), Fassung gemäss ABl. L 312 vom 7.12.2018, S. 14; vgl. dazu Notenaustausch vom 20. Dezember 2018 zwischen der Schweiz und der EU betreffend die Übernahme der Verordnung (EU) 2018/1861 über die Einrichtung, den Betrieb und die Nutzung des SIS im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung

des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (Weiterentwicklung des Schengen-Besitzstands), SR 0.362.380.079).

Erhebliche internationale Risiken, die zu bedenken sind, bestehen durch den jetzt erfolgenden Ausbau des Schengen-Systems: Das Schengen-Informations-System (SIS) wird in seiner eigenen Architektur und insbesondere durch die Interoperabilität gänzlich umgestaltet und ausgeweitet. Dazu haben alle Endbenutzer in allen Schengen-Mitglied- und assoziierten Staaten Zugriffs- und Bearbeitungsrechte (vgl. Art. 34-50 der Verordnung (EU) 2018/1861 vom 28. November 2018). Berechtigte Benutzer sind u.a. Polizistinnen und Polizisten ebenso wie Verwaltungsangestellte in verschiedenen Behörden aller Schengen-Staaten; die ausländischen Stellen werden auf das digitale Justizsystem der Schweiz direkten Zugriff haben.

Gerne nehmen wir an, dass unsere Vorschläge zum Klärungs- und Verbesserungsbedarf in Ihre weiteren Arbeiten Eingang finden. Dafür danken wir Ihnen im Voraus bestens.

Namens des Vorstandes

Dr. Susanne Leuzinger
Präsidentin ICJ-CH

Prof. Dr. Patricia Egli
Vorstandsmitglied ICJ-CH