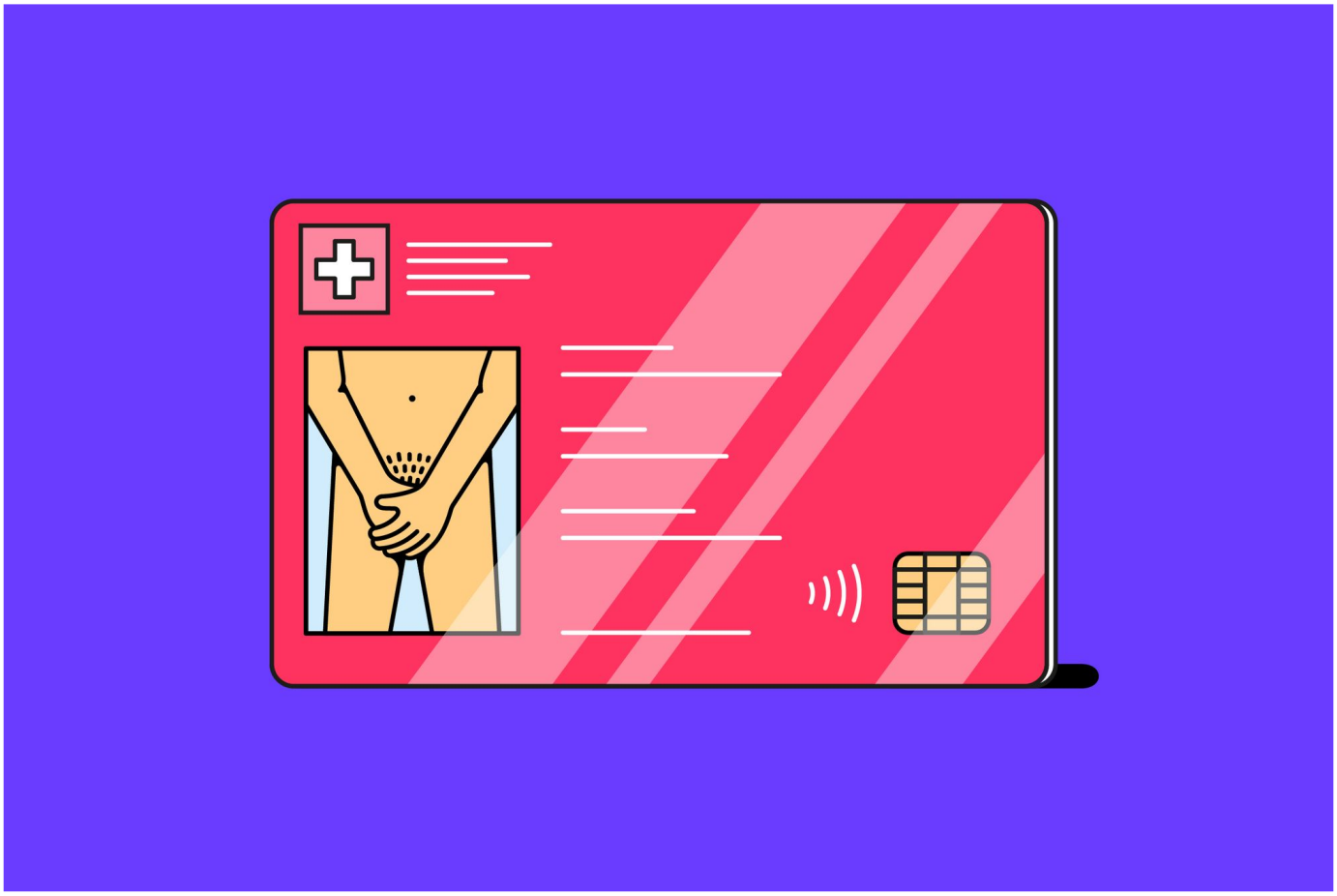

Die Probleme mit der Schweizer E-Identität

Biometrische Daten in den Händen von Privaten, schlechter Datenschutz und fehlende EU-Kompatibilität: Die Schweiz wählt mit dem E-ID-Gesetz einen riskanten Weg.

Von Adrienne Fichter (Text) und Till Lauer (Illustration), 28.01.2021

Mit einem einzigen Log-in soll man online shoppen, Steuererklärungen ausfüllen und in Zukunft auch Volksinitiativen unterschreiben können: Das will die Schweiz mit der elektronischen Identität möglich machen, kurz E-ID.

Am 7. März wird über das dazugehörige Gesetz abgestimmt.

Es ist die erste digitalpolitische Abstimmung der Schweiz, ja gar die erste Abstimmung weltweit über die digitale Demokratie. Einzigartig ist auch das Modell, das in der Schweiz zur Disposition steht: Privatunternehmen sollen im Auftrag des Staats die E-ID herausgeben. Kein anderes europäisches Land verfolgt einen Ansatz dieser Art, der auf reines Outsourcing setzt ohne staatlich herausgegebene E-ID-Lösung als Alternative.

Gegen das Gesetz haben Seniorenverbände, netzpolitische Verbände wie die Digitale Gesellschaft sowie Grüne, Linke und Piratenpartei das Referendum ergriffen. Ihre Forderung: Der digitale Identitätsnachweis soll eine Staatsaufgabe bleiben. Bürgerinnen sollen ein staatliches Produkt erhalten und kein privatwirtschaftliches.

Erfreut sind hingegen eine Reihe von möglichen Anbietern, die bereits in den Startlöchern stehen. An erster Stelle: Swiss Sign, ein Konsortium von Banken, Versicherungen, Swisscom, SBB und Post. Unterstützt wird die Pro-Seite von den bürgerlichen Parteien. Sie beschwichtigen: Die neue E-ID werde «staatlich geprüft» sein und auch sonst bezüglich Sicherheit und Datenschutz völlig unproblematisch.

Unsere Recherche zeigt: Diese Argumentation ist irreführend. Die geplante E-ID weist mindestens vier gravierende Probleme auf:

1. Die Bundesbehörden wollen – anders als ursprünglich angekündigt – die Verordnung zum E-ID-Gesetz nicht vor der Abstimmung publizieren. Damit werden der Stimmbevölkerung zentrale Informationen vorenthalten, weil darin wichtige technische Grundsatzfragen geklärt werden. Denn die Verordnung lässt zu, dass private Anbieter der E-ID in den Besitz von biometrischen Daten der Bürgerinnen gelangen. Das sind unveränderliche Merkmale des menschlichen Körpers wie Fingerabdruck, Iris oder, wie in diesem Fall, das Gesichtsbild.
2. Die E-ID ermöglicht den privaten Anbietern, enorme Datenmengen zu speichern: detaillierte Bewegungsprofile, Browsereinstellungen, digitale Kaufverträge. Gespeichert würden diese Informationen beim Unternehmen Swiss Sign, Stand heute, auf Servern bei der Post, wie die Republik herausgefunden hat.
3. Das Gesetz zwingt Inhabern der E-ID in Missbrauchsfällen die Beweislast auf. Aus Sicht von IT-Expertinnen wie auch des eidgenössischen Datenschutzbeauftragten ist dies unzumutbar: In Fällen von digitalem Identitätsklau wird der Inhaber vermutlich automatisch haftbar.
4. Obwohl in der Botschaft die internationale Anerkennung betont wird, ist die Schweizer E-ID nicht kompatibel mit den Richtlinien der EU. Bürgerinnen europäischer Länder werden keine Schweizer E-ID benutzen können, umgekehrt können Schweizer mit ihrer E-ID im Ausland nichts anfangen. Dafür bräuchte es zuerst einen bilateralen Staatsvertrag.

1. Biometrische Daten liegen bei privaten Firmen

Pässe und Identitätskarten dienen einerseits als international anerkannte Reisedokumente. Und sie sind andererseits für gewisse Transaktionen, wie etwa den Alkoholkauf, auch im eigenen Land unverzichtbar.

Solche Transaktionen sollen künftig auch digital möglich werden, und zwar mithilfe der staatlich anerkannten E-ID. Sie soll im Internet also die Funktion eines amtlichen Ausweises übernehmen – und gewährleisten, dass die Nutzerin Lena Fischer auch tatsächlich die Bürgerin Lena Fischer ist.

Doch was heisst das genau, amtlich? Justizministerin Karin Keller-Sutter sagt im Interview mit der NZZ: «Der Staat hat eine tragende und wichtige Rolle. Er ist und bleibt Herr der Daten. Er reguliert. Er überprüft. Er anerkennt. Und er beaufsichtigt.»

In dieser Formulierung verschweigt die Bundesrätin aber ein entscheidendes Element: die Verifikation. Das ist der Prozess, der sicherstellt, dass sich hinter dem Computer auch ganz sicher Lena Fischer befindet und nicht etwa Max Müller, der sich als Lena Fischer ausgibt. In diesem Verifikations-

prozess werden die privaten Anbieter der E-ID eine entscheidende Rolle spielen.

Wie läuft dieser Prozess genau ab? Als das Gesetz ausgearbeitet wurde, haben sich viele IT-Expertinnen dafür interessiert. Doch bis heute haben sie keine Details dazu erhalten: Die Verordnung zum Gesetz, die eigentlich vor der Abstimmung hätte veröffentlicht werden sollen, wird vom Bundesamt für Justiz bisher unter Verschluss gehalten. Dies mit der Begründung, «die Verordnung ist hinfällig, wenn das Gesetz an der Urne verworfen wird», wie Urs Paul Holenstein, Leiter Rechtsinformatik beim Bundesamt für Justiz, sagt.

Das Vorgehen dürfte taktische Gründe haben. Es sei Holenstein gewesen, der von Anfang an sehr relevante Fragen zu technischen Standards im Gesetz habe aussparen wollen, um sie auf dem Verordnungsweg zu regeln, sagen mehrere Insider. Darunter konkrete Aspekte wie die Interoperabilität (also die Schnittstellen, damit verschiedene E-ID-Systeme miteinander technisch funktionieren), Haftungsfragen oder das Sicherheitsniveau für verschiedene Anwendungen von Geschäftsfeldern.

Erik Schönenberger, Geschäftsführer der Digitalen Gesellschaft, findet dies inakzeptabel: «Der interessierten Stimmbevölkerung bleiben so wichtige Informationen vorenthalten, während die an der Arbeitsgruppe beteiligten Identitätsprovider einen Wissensvorsprung haben.» Die sogenannten Identitätsprovider sind die Anbieter der E-ID, also Firmen wie Swiss Sign, die auch Einsitz in der Arbeitsgruppe für die Verordnung hat.

Wie die E-ID ausgestellt werden soll, hat die Republik beim Bundesamt für Justiz nun erstmals in Erfahrung gebracht. Ein Beispiel:

- Lena Fischer möchte eine staatliche E-ID. Sie wendet sich an den Identitätsprovider ihres Vertrauens, in unserem Beispiel Swiss Sign.
- Das erfordert eine genaue Überprüfung. Swiss Sign leitet die Anfrage weiter ans Fedpol, das Bundesamt für Polizei. Dieses tritt mit Lena Fischer in Kontakt und fragt sie über eine Eingabemaske verschiedene Dinge, etwa ihren Geburtstag oder den Geburtstag ihrer Mutter. Sobald das Bundesamt Lena Fischer in ihren Registern gefunden hat, werden die abgefragten Daten, eine eindeutige E-ID-Registrierungsnummer für Lena Fischer sowie ein Passbild von ihr an Swiss Sign weitergeleitet.
- Swiss Sign fordert daraufhin Lena Fischer auf, sich in einem Videochat zu identifizieren (unklar ist, ob sie auch vor Ort erscheinen kann). Zusätzlich muss Lena Fischer eine Telefonrechnung oder ein Bankdokument einreichen, um zu beweisen, dass sie auch wirklich Lena Fischer ist.

Für die Verifikation von Lena Fischer werden also biometrische Daten an Swiss Sign – und gemäss der Datenschutzerklärung an die Partnerfirma PXL Vision – übermittelt.

Wie wird sichergestellt, dass das Unternehmen diese sensiblen Informationen nicht für kommerzielle Zwecke missbraucht?

Sonja Margelist, Mediensprecherin beim Bundesamt für Justiz, sagt: Dies werde durch die Eidcom, eine neu zu schaffende Kommission, im Rahmen der Aufsicht geprüft. «Fehlbaren Identitätsprovidern kann die Anerkennung entzogen werden.» Lena Fischer selbst kann die Löschung nicht anordnen.

Annett Laube, Informatikprofessorin an der Berner Fachhochschule, kritisiert diese Aufbewahrung von sensiblen Informationen bei den Identitäts-

providern: «Die Speicherung von biometrischen Daten ist grundsätzlich heikel.»

2. Enorme Datensammlungen werden möglich

SVP-Ständerat Hannes Germann war ein Skeptiker der E-ID-Vorlage. Doch man sei Gegnern wie ihm bei der Überarbeitung stark entgegengekommen, sagt er.

Dass der Datenschutz strenger sei als bei anderen Projekten, wird auch in der Ja-Kampagne zum neuen Gesetz argumentiert. Ob diese Auflagen tatsächlich eingehalten werden, darauf können Schweizer Einwohner jedoch nur hoffen. Verschwiegen wird, dass *by design* weitreichende Datensammlungen möglich bleiben.

Die Swiss-Covid-App etwa ist ein Beispiel für *Privacy by design*. Die App ist so konstruiert, dass das Bundesamt für Gesundheit gar nicht wissen kann, wo sich Lena Fischer aufhält und mit wem sie Kontakt hatte. Anders wird dies bei der E-ID sein: Der Betrieb basiert auf reinem Vertrauen in den Identitätsprovider.

Warum? Jede Nutzung, jedes Einloggen spielt sich im Rahmen einer Dreiecksbeziehung ab – zwischen der Bürgerin, dem Identitätsprovider und dem Anbieter einer Onlinedienstleistung, für welche das Log-in genutzt wird.

Die Identitätsprovider tragen dabei eine grosse Verantwortung: Meldet sich Lena Fischer zum Beispiel mit der E-ID bei Galaxus an, so muss sie darauf hoffen, dass Swiss Sign ihre Nutzungsdaten wirklich nach sechs Monaten löscht, wie es das Gesetz vorsieht. Und Galaxus muss darauf vertrauen, dass die Systeme von Swiss Sign einwandfrei funktionieren. (Was keine Selbstverständlichkeit ist: In der Vergangenheit kam es wegen eines Hackerangriffs bei Swiss Sign bereits zu einem Totalausfall.)

Wie der Verein Data Privacy Community in einem Webinar erklärt, werden bei Swiss Sign dabei riesige Datenmengen angehäuft. So erfährt es der Identitätsprovider, wenn Lena Fischer sich etwa bei Digitec einloggt, den Kaufvorgang abbricht, später bei Galaxus weitersurft und danach die Steuererklärung im Kanton St. Gallen ausfüllt – alles mit demselben Benutzerkonto, der digitalen ID von Swiss Sign. Ebenso erfährt Swiss Sign allerlei Metadaten wie etwa die Browsersprache. «Spielchen» mit diesen Daten seien möglich, sagt Thomas Bühler, Sprecher im Webinar.

In Zukunft wird das Bundesgesetz über elektronische Identifizierungsdienste auch den regulatorischen Teil des elektronischen Patientendossiers ablösen. Sprich: Alle zertifizierten E-ID-Anbieter sollen den Zugang zu den Patientendaten verwalten können. Der zu verwaltende Datenschatz wird dadurch riesig.

Ein verantwortungsvoller Umgang mit den Daten ist deshalb zentral. Doch wie steht es um das Vertrauen in die Firmen, die diese Daten verwalten?

Gemäss Recherchen der Republik liegen die Nutzerdaten von Swiss Sign derzeit in einem Datenzentrum der Post. Davon steht jedoch interessanterweise nichts in der Datenschutzerklärung zur digitalen ID. Wird das Gesetz an der Urne angenommen, wird die Post damit zur technischen Hauptverwalterin der E-ID. Es verwundert daher nicht, dass sich die Post zum ersten Mal seit ihrem Bestehen in einen Abstimmungskampf explizit einmischt. Auch ist das Nudging in Richtung Swiss ID heikel, das Produkt von

Swiss Sign. Die Post verlangt von ihren Kundinnen zwingend eine Swiss ID, wie der ehemalige Preisüberwacher Rudolf Strahm im «Tages-Anzeiger» beklagt: «Wenn mir heute die Post die Ablieferung eines Pakets per Internet mitteilt, kann ich das Ablieferungsdatum nur mit der Akzeptierung meiner elektronischen, persönlichen Swiss-ID abändern.»

Eine Sprecherin von Swiss Sign bestätigt die Recherchen auf Anfrage: «Zurzeit betreiben wir zwei Data-Center, wobei eines von der Post gehostet wird.» Bis zum zweiten Quartal 2021 sollen diese Daten in ein anderes Center migriert werden, das nicht von einem Konsortiumsmitglied betrieben wird.

Wer das sein wird? Dazu möchte die Sprecherin keine Auskunft geben.

Gemäss E-ID-Gesetz darf ein Identitätsprovider Einkaufs- und Log-in-Daten nicht kommerziell verwerten oder nutzen. Doch er kann sie sechs Monate lang speichern – zu welchem Zweck auch immer. Wie oft die Eidcom hier Prüfungen durchführen wird, wird erst in der Verordnung geregelt.

Beim Thema Datenschutz gilt somit dasselbe Prinzip wie bei den biometrischen Gesichtsdaten: *Privacy by trust*. Und nicht *by design*.

3. Auf Nutzer kommen Haftungsrisiken zu

Elektronische Identitäten sind immer mit einem «Impersonationsrisiko» verbunden. Damit ist die Gefahr eines Identitätswechsels gemeint: Lena Fischer wird dann auf Galaxus oder beim St. Galler Behördenportal als Max Müller angezeigt – sei es aufgrund technischer Fehler, sei es aufgrund von Hackerangriffen.

In diesem Fall könnte Lena Fischer im Namen des E-ID-Inhabers Max Müller Transaktionen durchführen, die dieser gar nicht gemacht hat.

Natürlich gibt es solche Impersonationsrisiken und Hackerangriffe auch bei einem staatlichen E-ID-System. Doch weil der Bundesrat explizit einen «Wettbewerb» der Identitätsprovider möchte und damit einen E-ID-Pluralismus vorsieht, multipliziert sich die Zahl der möglichen Angriffspunkte.

Kommt es zu Angriffen oder einem Identitätsklau, könnte die Beweislast der Unschuld bei der E-ID-Inhaberin liegen. Das geht aus dem Gesetz hervor.

> Die Inhaberin oder der Inhaber einer E-ID hat die nach den Umständen notwendigen und zumutbaren Massnahmen zu treffen, damit seine E-ID nicht missbräuchlich verwendet werden kann.

Artikel 12.1, E-ID-Gesetz.

Florian Forster, ehemaliger Leiter der Fachgruppe IAM beim Verein eCH und Spezialist für digitale Identitäten, übt Kritik an der Formulierung. «Am Ende muss die Inhaberin nachweisen, dass sie nichts mit dem Missbrauch ihrer E-ID zu hat. Dabei ist der Schaden für sie am grössten.»

Welche «notwendigen und zumutbaren Massnahmen» eine E-ID-Nutzerin genau treffen müsse, um Missbrauch zu verhindern, sei alles andere als klar, sagt auch IT-Sicherheitsexperte Daniel Muster.

Auch der eidgenössische Datenschützer Adrian Lobsiger ist alles andere als glücklich über diesen Gesetzesartikel. Und selbst die SVP warnt. Nationalrat Pirmin Schwander sagte in der Ratsdebatte vom 20. März 2019: «Unser

Anliegen ist hier, dass am Schluss nicht die gesamte Verantwortung auf die Anwender geschoben wird, wenn etwas nicht gut läuft.»

Hinter dem Paragrafen steckt FDP-Nationalrätin Christa Markwalder, die selber einmal Opfer von Identitätsdiebstahl war, wie sie gegenüber der Republik sagte. Weshalb sie trotz dieser Erfahrung den E-ID-Inhabern mehr Pflichten und Verantwortung aufbürden will, bleibt unklar. In der Ratsdebatte verteidigte sie den Paragrafen mit den Worten, den Internetnutzerinnen dürfe «durchaus auch ein zumutbares Mass an Eigenverantwortung im digitalen Raum übertragen werden».

Das Bundesamt für Justiz relativiert: «Wer nun wie genau haftet, muss im Einzelfall geklärt werden», sagt Sprecherin Sonja Margelist. «Wenn sich zum Beispiel nach einer Attacke erweisen sollte, dass der Identitätsprovider den Betrieb seines E-ID-Systems nicht sicher gewährleistet, haftet er.»

Tatsache ist: Man hätte datensparsamere, sicherere E-ID-Lösungen gesetzlich verankern und damit für verbindlich erklären können. Dies, indem man die E-ID wie einen Pass konzipiert hätte: Nicht ein externer Dienstleister würde die E-ID dabei treuhänderisch verwalten, sondern die Bürgerin selbst wäre Trägerin ihrer E-ID – etwa in Form einer Smartcard.

So könnte die Bürgerin tatsächlich dafür verantwortlich gemacht werden, wenn sie ihre Smartcard verlieren würde oder diese missbraucht würde. Ein solches System wird im Fachjargon als «dezentrale Authentifizierung» bezeichnet. Lena Fischer würde in einem solchen System direkt mit Galaxus oder dem Steueramt interagieren – ohne einen Vermittler dazwischen.

«In einem solchen System würden nachweislich auch Impersonationsrisiken minimiert», sagt IT-Sicherheitsexperte Florian Forster. Das sieht auch Erik Schönenberger von der Digitalen Gesellschaft so, der das E-ID-Gesetz als unnötig erachtet: «Mit der elektronischen Identitätskarte hätten wir alle Voraussetzungen gehabt, das Ausweisgesetz hätte gereicht für eine E-ID. Dafür braucht es keinen Zwischenhändler, keinen Intermediär, dem man sich anvertrauen muss.»

Bundesrat und Parlament haben sich bei der Beratung des E-ID-Gesetzes nicht um diese technischen Grundsatzfragen gekümmert. Deshalb wird der Inhalt der Verordnung nun umso mehr zum Politikum – und Transparenz wird umso nötiger. Gerade das Thema «dezentrales versus zentrales Anmeldeverfahren» wird in der Verordnungs-Arbeitsgruppe und der Bundesverwaltung kontrovers debattiert, wie mehrere involvierte Personen bestätigen. Umstritten ist die Frage, welche Sicherheitsanforderungen für den Zugang zum elektronischen Patientendossier oder für die Bestellung einer Betreibungsurkunde erforderlich sind und welche technischen Standards dafür gelten sollen.

IT-Sicherheitsexperten wie Forster, Muster und Schönenberger sind der Ansicht, dass bei einem sogenannten «hohen» Sicherheitsniveau die dezentrale Authentifizierung zwingend Voraussetzung sein muss. Setzt sich diese Meinung in der Verordnung durch, müsste das Konsortium SwissSign sein E-ID-Angebot für eine staatliche Anerkennung vermutlich grundlegend überarbeiten. Schliesslich ist die Swiss ID bisher ein simples Benutzerkonto für den E-Commerce-Handel – mit zentralem Anmeldeverfahren.

4. Die E-ID ist nicht EU-kompatibel

Als die Bundesverwaltung vor fast zehn Jahren beschloss, eine E-ID zu lancieren, spielte ein Aspekt eine grosse Rolle: Die Schweizer Lösung sollte in jedem Fall kompatibel mit EU-Standards sein. So steht in einer Konzeptstudie vom November 2014, die der Republik vorliegt: «Beim Design der E-ID-Lösung müssen die einschlägigen internationalen Standards berücksichtigt und die Interoperabilität zumindest zum europäischen System garantiert sein.»

Dass die Schweizer E-ID in jedem Fall EU-konform sein und dort anerkannt werden soll, steht auch in der Botschaft des Bundesrats zum Gesetz.

Doch das gegenwärtige Modell erfüllt die Anforderungen der E-IDAS-Verordnung, die das Thema in der EU regelt, nicht. Gemäss der EU-Richtlinie braucht es einen nationalen E-IDAS-Hub, also eine Art Herausgeberschaft für die digitale ID, und dieser müsste vom Staat betrieben werden. Die E-ID-Systeme fast aller EU-Staaten sind bereits anerkannt, bisher sind es fast ausschliesslich vom Staat herausgegebene E-ID-Lösungen.

Auch Steffen Schwalm vom deutschen Digitalverband Bitkom und Experte für die digitalen Identitäten schreibt auf Twitter: «Um eIDAS-Konformität zu erreichen, müsste die Schweizer E-ID grundlegend angepasst werden.»

Diesen nationalen Knotenpunkt zu bilden, ist technisch anspruchsvoll, sagt ein gut informierter Insider aus der Bundesverwaltung. Wenn die Schweiz diesen Aufwand betreiben wolle, könne der Staat genauso gut die technische Infrastruktur selbst aufbauen und die E-ID selbst herausgeben.

Was wäre aber die Konsequenz? Da die E-IDAS-Verordnung immer mehr zum Standard wird, werden so manche Bestellungen und Transaktionen im Netz unmöglich oder schwieriger werden. Eine EU-Bürgerin könnte kein Bankkonto bei einer Schweizer Bank online eröffnen, ein Schweizer könnte mit seiner E-ID keinen Umzug nach Frankreich melden.

Die Bundesverwaltung räumt auf Anfrage ein, dass die EU-Kompatibilität nicht mehr zuoberst auf der Prioritätenliste stehe. Man habe kein Notifizierungsverfahren bei der EU eingereicht. Um Kompatibilität zu erreichen, brauche es einen zusätzlichen bilateralen Vertrag.

Sonja Margelist vom Bundesamt für Justiz ergänzt: «Wer für den Betrieb des nationalen E-IDAS-Hubs infrage käme, würde erst im Rahmen eines allfälligen Notifizierungsverfahrens entschieden. Zur Zuteilung dieser Aufgabe müsste das E-ID-Gesetz geändert werden.»

Fazit

Problematisch ist vor allem die Tatsache, dass Privatunternehmen die E-ID herausgeben sollen. Doch auch unabhängig von der Frage, ob der Staat oder Private für eine elektronische Identität verantwortlich sein sollen, wirft das E-ID-Gesetz diverse Fragen auf und birgt in Bezug auf Datenschutz und Sicherheit nicht zu unterschätzende Risiken. Ordnungspolitisch bedenklich ist zudem die Tatsache, dass der Bund wichtige technologische Grundsatzentscheidungen über den Verordnungsweg regeln lässt und dass er die entsprechende Verordnung bewusst erst nach der Abstimmung in die öffentliche Vernehmlassung schickt. Ebenso, dass in der Arbeitsgruppe die potenziellen Herausgeber der E-ID Einsitz haben und Einfluss auf diese

Standards nehmen können. Damit wird das E-ID-Gesetz zu einer Blackbox – sowohl für IT-Expertinnen wie für die Stimmbevölkerung.

In einer früheren Version haben wir unpräzise geschrieben, dass die zertifizierten E-ID-Anbieter die Patientendaten verwalten können. Das hätte man so interpretieren können, dass die E-ID-Anbieter direkten Zugriff auf Patientendaten hätten. Dem ist nicht so. Gemeint ist nur der Zugang zum Patientendossier.