

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail:
rechtsinformatik@bj.admin.ch

Bern, 12. Oktober 2022

Vorentwurf des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID); Vernehmlassungsverfahren

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zum Vorentwurf für ein E-ID-Gesetz (VE-BGEID) Stellung nehmen zu können. Aus datenschutzrechtlicher Sicht ergeben sich folgende Hinweise:

1. Allgemeine Bemerkungen

Wir begrüßen die neue Initiative zur Einführung eines elektronischen Identitätsnachweises (E-ID) auf der Basis einer staatlich betriebenen Infrastruktur und den Grundsätzen des Schutzes der Privatsphäre durch Technik («privacy by design»), der Datensparsamkeit und der dezentralen Datenspeicherung.

2. Bemerkungen zu den einzelnen Artikeln des VE-BGEID

Art. 2 Abs. 2 Bst. b – Gesichtsbild

In Art. 4 Abs. 4 VE-BGEID und den zugehörigen Erläuterungen wird der Bedarf nach einem biometrischen Gesichtsbild nur für den Ausstellungsprozess begründet. Demgegenüber wird der Bedarf nach einem biometrischen Gesichtsbild in der E-ID selbst weder in den Erläuterungen zu Art. 2 Abs. 2 Bst. g – der auf die Informationssysteme nach dem Ausweisgesetz (AwG) und dem Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA) verweist, die beide biometrische Gesichtsbilder enthalten können (vgl. Art. 11 i. V. m. Art. 2^{bis} AwG und Art. 1 i. V. m. Art. 4 Abs. 1 Bst. a^{bis} BGIAA) – noch anderswo erklärt. Es bleibt deshalb nicht nachvollziehbar, weshalb auf einer ID für den Einsatz in der digitalen Welt ein biometrisches Gesichtsbild enthalten sein soll. Dafür ist entweder eine zwingende Begründung zu liefern oder es ist darauf zu verzichten.

Art. 2 Abs. 3 Bst. a – Verwendung der AHV-Nummer

Der Vernehmlassungsentwurf sieht vor, dass die E-ID auch die AHV-Nummer enthalten soll (Art. 2 Abs. 3 Bst. a VE-BGEID). In den Erläuterungen wird nicht ersichtlich, weswegen die AHV-Nummer enthalten sein muss. Der Zweck des Gesetzes in Art. 1 Abs. 2 Bst. a VE-BGEID, die sichere Identifizierung mittels E-ID unter Privaten und mit Behörden zu gewährleisten, kann auch ohne die AHV-Nummer erreicht werden. In diesem Sinne genügt die Verwendung der AHV-Nummer dem im Gesetz selbst verankerten Grundsatz der Datensparsamkeit nicht (Art. 1 Abs. 2 Bst. b Ziff. 3 VE-BGEID). Auf die Verwendung der AHV-Nummer in der E-ID ist zu verzichten. Wenn die AHV-Nummer nicht systematisch verwendet werden darf, muss das anwendbare Recht dies gemäss Art. 153c Abs. 2 AHVG explizit ausschliessen. Eine entsprechende Bestimmung ist in das Gesetz aufzunehmen.

Art. 3 und Art. 4 – Prüfung der Identität bei der Ausstellung der E-ID

Die Erläuterungen zu den persönlichen Voraussetzungen für die E-ID (Art. 3 VE-BGEID) und der Ausstellung der E-ID (Art. 4 VE-BGEID) besagen, dass bei der Ausstellung der E-ID auf eine erneute Prüfung der Identität der antragstellenden Person aufgrund der Kosten, Benutzerfreundlichkeit und Geschwindigkeit verzichtet wird. Vorgesehen sei lediglich eine Verifikation der Identität anhand der eingereichten Informationen und der Gesichtsbildverifikation. Gemäss Art. 6 Abs. 5 des neuen Datenschutzgesetzes (nDSG) muss, wer Personendaten bearbeitet, sich über deren Richtigkeit vergewissern. Dieselbe Bestimmung verlangt, dass die Angemessenheit der Massnahmen von der Art und dem Umfang der Bearbeitung sowie vom Risiko abhängt, das die Bearbeitung für die Grundrechte der betroffenen Personen mit sich bringt. Eine nicht korrekt ausgestellte E-ID bringt ein erhebliches Risiko für die Grundrechte der betroffenen Person mit sich (Identitätsdiebstahl). Entsprechend müssen die Massnahmen zur Verhinderung dieses Risikos tief greifen. Kosten, Benutzerfreundlichkeit und Geschwindigkeit sind keine Argumente, um ein solches Risiko für die Grundrechte nicht angemessen zu adressieren. Die entsprechenden Ausführungen in den Erläuterungen sind zu streichen. Das Risiko muss mit gesetzlich festgehaltenen Massnahmen reduziert werden. Sollte auf Stufe des formellen Gesetzes auf zusätzliche Massnahmen verzichtet werden, dann ist die Delegationsnorm in Art. 4 Abs. 5 VE-BGEID dahingehend zu konkretisieren, dass der Bundesrat Massnahmen zur korrekten Feststellung der Identität erlässt.

Art. 7 und Art. 8 – Sorgfaltspflicht und Unterstützung durch die Kantone

Die Verankerung der Sorgfaltspflichten bei der Inhaberin oder beim Inhaber der E-ID nach Art. 7 VE-BGEID muss mit Massnahmen begleitet werden, welche die Inhaberinnen und Inhaber der E-ID bei der Wahrnehmung der Sorgfaltspflichten unterstützen. Die Pflicht für die Kantone in Art. 8 VE-BGEID, Anlaufstellen zur Unterstützung bei der Ausstellung und dem Einsatz der E-ID einzurichten, erachten wir als sinnvoll aufgrund der Nähe der kantonalen Behörden zu den Bürgerinnen und Bürger. Zusätzlich möchten wir anregen, Massnahmen zur Wahrnehmung der Sorgfaltspflichten übersichtlich und gut zugänglich in der Applikation mit der E-ID darzustellen.

Art. 10 – Wahlfreiheit

Wir begrüssen die in Art. 10 VE-BGEID festgehaltene Wahlfreiheit zwischen E-ID und einem anderen Ausweisdokument und den damit einhergehenden Grundsatz der Nichtdiskriminierung zwischen Personen, die eine E-ID nutzen wollen, und Personen, die keine E-ID nutzen wollen.

Art. 10 und Art. 16 – Umsetzung der Datensparsamkeit auf Seite Verifikatorin

Bei der Verwendung von elektronischen Identitätsnachweisen stellt die Überidentifikation ein Problem dar. Der Begriff Überidentifikation bezeichnet die Bearbeitung zu vieler Personendaten bei der Identifikation einer Person für einen bestimmten Zweck. Die Überidentifikation steht im Widerspruch zum Grundsatz der Datensparsamkeit. Das Vorweisen einer E-ID und das Vorweisen von (anderen) elektronischen Nachweisen ist in zwei Bestimmungen der Vorlage geregelt (Art. 10 und Art. 16 VE-BGEID). Hinsichtlich der Überidentifikation erwähnt Art. 10 VE-BGEID zwar die Möglichkeit die E-ID *oder Teile davon* vorzuweisen, der eigentliche Regelungsgegenstand von Art. 10 VE-BGEID ist aber die Pflicht zur Akzeptanz von physischen Ausweisdokumenten. In Art. 16 Abs. 1 VE-BGEID wird geregelt, dass die Inhaberin oder der Inhaber eines elektronischen Nachweises (also auch der E-ID) bestimmt, welche Bestandteile des Nachweises oder davon abgeleiteten Informationen an die Verifikatorin übermittelt werden. Jedoch wird dies in den Erläuterungen von Art. 16 VE-BGEID dahingehend relativiert, dass die Verifikatorin festlegt, welche Daten für den Zugang zu ihren Diensten erforderlich sind und dass dies den Handlungsspielraum der Inhaberin oder des Inhabers begrenzt. Die Erläuterungen bringen klar zum Ausdruck, dass ein Dienst nicht genutzt werden kann, wenn die Inhaberin oder ein Inhaber beschliesst, die von der Verifikatorin verlangten Elemente nicht zu übermitteln. Zwar wird in den Erläuterungen auf den «Grundsatz der Beschränkung der Datenbearbeitung auf das strikte Minimum» (Datenvermeidung und Datensparsamkeit) verwiesen. Weil es sich dabei um einen allgemeinen Grundsatz zum Schutz von Personendaten handle, müsse er im Gesetz nicht erwähnt werden.

Gemäss den Erläuterungen besteht keine Absicht, das Verhalten der Verifikatorin im VE-BGEID weiter zu regulieren. Das Verhalten der Verifikatorin ist datenschutzrechtlich einzig den Regeln des nDSG unterstellt. Dabei öffnet sich allerdings ein Widerspruch zum Zweck des VE-BGEID. Gemäss Art. 1 Abs. 2 Bst. b Ziff. 3 VE-BGEID hat das Gesetz zum Zweck, die Grundrechte von Personen zu gewährleisten, über die im Zusammenhang mit der Verwendung der E-ID Daten bearbeitet werden und soll dies durch die *Umsetzung des Grundsatzes der Datensparsamkeit* tun. Das Gesetz selbst sieht also vor, dass der Grundsatz der Datensparsamkeit umgesetzt werden muss, wenn bei der Verwendung der E-ID Personendaten bearbeitet werden. Der Zweck in Art. 1 VE-BGEID beschränkt sich dabei nicht auf die Datensparsamkeit auf Seite der Ausstellerin. Zudem braucht es Regeln zur Einhaltung der Datensparsamkeit durch die Verifikatorin. Ein Verweis in den Erläuterungen reicht nicht aus. Es braucht unter Art. 10 VE-BGEID weitere Regeln für das Vorweisen der E-ID: Einerseits soll die Verifikatorin verpflichtet sein, die E-ID nur dann zu verlangen, wenn dies absolut notwendig ist, und andererseits soll die Verifikatorin verpflichtet sein, nur diejenigen Teile der E-ID abzufragen, auf die sie nicht verzichten kann. Die Konkretisierung von datenschutzrechtlichen Grundsätzen im VE-BGEID ist gerechtfertigt, weil die Möglichkeit zur einfachen Identifikation auf elektronischem Weg einen Anreiz für neue und unnötige Identifikationspflichten und Datensammlungen setzt, welche bei der analogen Identifikation gar nicht aufgetreten wären. Zusätzlich soll die Verifikatorin verpflichtet sein, die Daten der Identifikation weder zu speichern noch weiterzugeben noch sonst wie zu bearbeiten, ausser eine anderweitige Pflicht verlangt dies. Eine zusätzliche Sammlung der Daten durch die Verifikatorin zu anderen Zwecken als der Identifikation basierend auf der datenschutzrechtlichen Grundlage der Einwilligung einer Person im privatrechtlichen Kontext wäre in einem zweiten, separaten Schritt nach der Identifikation immer noch möglich. Diese Einwilligung müsste dann in der Form einer freiwilligen Willensäusserung ausserhalb des Identifikationsvorgangs eingeholt werden.

Art. 11 Abs. 4 – Keine Aufbewahrung der über Schnittstellen abgerufenen Daten

Das Informationssystem zur Ausstellung und zum Widerruf der E-ID verfügt zum Bezug der Personenidentifizierungsdaten nach Art. 2 Abs. 2 VE-BGEID über Schnittstellen zu verschiedenen Informationssystemen (Art. 11 Abs. 3 VE-BGEID). Die Erläuterungen halten fest, dass die aufgerufenen Daten weder dupliziert noch im Informationssystem des Fedpols gespeichert werden. Dies geht aus dem Normtext nur implizit hervor, weil die Aufzählung der im Informationssystem zur Ausstellung und zum Widerruf der E-ID enthaltenen Daten die Personenidentifizierungsdaten nach Art. 2 Abs. 2 VE-BGEID nicht enthält (Art. 11 Abs. 2 VE-BGEID). Es ist wünschenswert, wenn dieser essentielle Punkt, dass die abgerufenen Daten nicht aufbewahrt werden im Informationssystem zur Ausstellung und zum Widerruf der E-ID, im Normtext explizit zum Ausdruck kommt. Dazu könnte Art. 11 Abs. 4 VE-BGEID ergänzt werden: Die via Schnittstellen bezogenen Daten werden ausschliesslich zum Zweck der Ausstellung der E-ID bearbeitet und nicht im Informationssystem aufbewahrt. Diese Ergänzung würde die Umsetzung des Prinzips der dezentralen Datenhaltung rechtlich klar verankern.

Art. 16 Abs. 3 – Keine Datenspur bei der Prüfung durch die Verifikatorin im System zur Bestätigung von Identifikatoren

Die Prüfung der E-ID oder anderer elektronischer Nachweise durch die Verifikatorin im System zur Bestätigung von Identifikatoren in Art. 18 VE-BGEID darf keine Personendaten hinterlassen. Es darf nicht ersichtlich sein, wann, wo und für was eine Nutzerin oder ein Nutzer der E-ID oder eines anderen elektronischen Nachweises ihre E-ID oder ihren elektronischen Nachweis eingesetzt hat. Art. 16 Abs. 3 VE-BGEID hält fest, dass die Betreiberin der Systeme keine Kenntnis des Inhalts der vorgewiesenen elektronischen Nachweise hat und möglichst keine Rückschlüsse auf deren Verwendung und die Beteiligten ziehen kann. Es ist nicht klar, warum die Systeme nicht so gestaltet werden müssen, dass gar keine Rückschlüsse gezogen werden können. Auf das Wort «möglichst» ist im Text von Art. 16 Abs. 3 VE-BGEID zu verzichten. Falls aus technischen oder rechtlichen Gründen nicht darauf verzichtet werden kann, ist in den Erläuterungen klar darzulegen, warum eine Ausgestaltung eines Systems, dass keine Rückschlüsse über die Verwendung der E-ID oder anderer elektronischer Nachweise zulässt, nicht möglich ist.

Art. 17 Abs. 3, Art. 18 Abs. 2 und Art. 22 – Verifizierung der Identität von privaten Ausstellerinnen und Verifikatorinnen

Die Öffnung des Systems zur Bestätigung von Identifikatoren für die Zuordnung von Identifikatoren und Schlüsseln von privaten Ausstellerinnen und Verifikatorinnen bedingt begleitende Massnahmen. Insbesondere ist eine Verifizierung der Identität der privaten Ausstellerinnen und Verifikatorinnen vorzusehen. Entsprechend ist Art. 17 Abs. 3 VE-BGEID zu ändern, dass die Ausstellerinnen und Verifikatorinnen ihre Daten nicht ohne Verifikation selbst in das Basisregister eintragen können. In den Erläuterungen wird das Risiko ausgewiesen, dass Ausstellerinnen oder Verifikatorinnen mit vorgetäuschter Identität elektronische Beweismittel ausstellen könnten. Weil jedoch ein Zulassungsverfahren ressourcenintensiv wäre und zu einem teuren und unnötigen Flaschenhals führen würde, soll auf eine Verifikation verzichtet werden. Art. 22 VE-BGEID sieht vor, dass der Bund öffentlich über Fälle von begründetem Verdacht auf Missbrauch der Vertrauensinfrastruktur informiert. Die Erläuterungen nennen dies als risikomindernde Massnahme. Ein nachträglicher Kommunikationsweg ausserhalb der Systeme der VE-BGEID erscheint jedoch ungenügend, dem benannten Risiko zu begegnen. Die hohen Kosten des Zulassungsprozesses dürfen zudem kein Argument sein, die Risiken des Missbrauchs der Vertrauensinfrastruktur zu erhöhen. Von einer Vertrauensinfrastruktur kann zudem nur gesprochen werden, wenn die Risiken

des Missbrauchs mit allen möglichen Mitteln reduziert werden. Deswegen ist ein Verifizierungsprozess bei der Öffnung für Private vorzusehen.

Art. 23 – Open Source Software

Wir unterstützen die Veröffentlichung des Quellcodes der vom Bund zur Verfügung gestellten Elemente der Vertrauensinfrastruktur zur Umsetzung der E-ID in Art. 23 VE-BGEID. Open Source Software und die damit einhergehende Transparenz trägt zum Vertrauen in technische Lösungen bei, was gerade im sensiblen Bereich des Nachweises der Identität von natürlichen Personen essentiell ist.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Ueli Buri
Präsident privatim