piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Stellungnahme der Piratenpartei Schweiz zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID)

Sehr geehrter Frau Bundesrätin
Sehr geehrte Damen und Herren

Bezugnehmend auf Ihre Vernehmlassungseröffnung vom 29.06.2022 nehmen wir gerne Stellung.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

Gerne nehmen wir wie folgt Stellung:

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Die Piratenpartei ist erfreut, darüber, dass der Bund den Ball aufgenommen hat und deutliche Schritte in Richtung Wahrung der Digitalen Integrität macht. Leider beinhaltet der aktuelle Vorschlag Punkte, welche mit dieser nicht vereinbar sind und deshalb ist auch die in diesem Gesetz geplante E-ID in der jetzigen Form abzulehnen. Zwar wird im Gesetz ausdrücklich Datenschutz durch Technik, Datensicherheit und Datensparsamkeit als verbindlich erklärt, jedoch wird es im Detail diesen Anforderungen nicht gerecht.

Unbedingt korrigiert werden müssen:

Art. 4 Keine Ausstellung per Liveness-Check (Gesichtsvideo) und besonders keine Speicherung der Daten auf viele Jahre (Art. 11)

Art. 4 Analoge Ausstellungsmöglichkeit

Art. 10 Einsatz nur, wenn der Gesetzgeber eine Ausweispflicht vorsieht

Art. 2 Selbstbestimmte Auswahl der Daten, die in der E-ID gespeichert werden

Unsere Stellungnahme zu den einzelnen Artikeln:

Art. 2 Form und Inhalt

Abs. 2
Forderung:
Abs. 2 neu: Sie kann die folgenden Personenidentifizierungsdaten enthalten:

Die Absätze 2 und 3 enthalten eine lange Auflistung aller Daten, die bei Ausstellung zwangsweise in der E-ID hinterlegt werden. Für die Identifikation mit der E-ID mag dies insbesondere für die Behörden angenehm sein, widerspricht allerdings der Datensparsamkeit (Art. 1 Abs. 2 Ziff. 3) gänzlich.
Aus Gründen der Datensparsamkeit, -sicherheit und Selbstbestimmung des Bürgers muss dieser entsprechend selbst auswählen können, welche Daten er überhaupt auf seiner E-ID gespeichert haben möchte. So lange er beispielsweise mit der E-ID nur online Alkohol kaufen möchte, sollte es reichen auf der E-ID abzuspeichern, ob die Person das 18. Lebensjahr vollendet hat.

Abs. 3
Forderung:
Streichung lit a. AHV-Nummer

Der dritte Absatz unterscheidet sich vom zweiten theoretisch darin, dass die aufgezählten Daten keine "Personenidentifizierungsdaten" sein sollten. Dieser Punkt wird im Moment der Zusammenführung jedoch gänzlich hinfällig. Bei gesetzlicher Nutzung der E-ID ist die Illusion, dass die Daten in Abs. 3 nicht zur Identifizierung genutzt werden

können, schon schwierig aufrechtzuerhalten. Aber bei einmaligem widerrechtlichem Auslesen der E-ID sind mehrere Daten in Absatz 3 alles andere als harmlose "zusätzliche Informationen". So wird insbesondere die AHV-Nummer einmalig ausgestellt und bleibt ein Leben lang unverändert. Was Personendaten angeht, gibt es nur wenig Wertvolleres.
Eine Verknüpfung widerspricht auch generell dem Konzept der AHV-N13, denn "die 13-stellige AHV-Nummer ist völlig anonym, zufällig generiert und nicht sprechend. Sie wird nur einmal vergeben und bleibt ein Leben lang unverändert, auch wenn der Zivilstand, etwa durch Heirat, ändert." [1] Ferner ist die AHV-Nummer auf anderen amtlichen Ausweisen nicht gespeichert.
Nicht zuletzt verspricht der Bund, es darf erneut erwähnt werden, die E-ID datensparsam umzusetzen (Art. 1 Abs. 2 Ziff. 3), was mit der Speicherung der AHV-Nummer sicher nicht eingehalten wird.
Eine Verknüpfung der E-ID mit der AHV-Nummer ist entsprechend vollumfänglich auszuschliessen.

Art. 4 Ausstellung

Liveness-Check
Forderung:
1. Auf unsichere Methoden und die darauffolgende Datenspeicherung ist zu verzichten.
2. Explizites Anbieten einer E-ID-Erstellung ohne Liveness-Check

Bei der Eröffnung des Vernehmlassungsverfahren hat Michael Schöll (Direktor BJ) den Ausstellungsprozess der E-ID nach Art. 4 genauer beschrieben und dabei einen "Liveness-Check", ein Videogesichtsbild, als Grundkomponente hervorgehoben (Abs. 4) [2]. Auf Nachfrage wurde bestätigt, dass eine Software den Abgleich mit den hinterlegten Gesichtsbildern vornehmen wird. Nicht nur Menschen, sondern auch Maschinen lassen sich allerdings von Deep-Fakes und anderen technischen Umgehungsversuchen nachweisbar täuschen. So gibt der Bund faktisch selbst zu, dass der Liveness-Check nicht sicher ist, indem das fedpol die Gesichtsvideos bis 5 Jahre nach Gültigkeit zur Missbrauchsverhinderung/-analyse speichern darf (siehe Art. 11 Abs. 2b), um bei Verdacht die Daten erneut kontrollieren zu können.

Aus Datenschutzgründen ist es äusserst problematisch vom Antragstellenden ein Gesichtsvideo zu fordern. Zum einen können daraus detaillierte 3D-Gesichtsmodelle aller

erstellt werden, was beispielsweise für die Identifikation bei Videoüberwachung genutzt werden kann. Zum anderen werden diese Daten jahrelang zentral gespeichert werden, was diese Daten wiederum selbst zu einem lukrativen Ziel für Cyberangriffe macht. Sämtliche Daten in Bezug auf die E-ID sind besonders wertvoll und da inzwischen andauernd über Hacks, auch gegenüber staatlichen Stellen, berichtet (oder auch verschwiegen) wird, muss davon ausgegangen werden, dass mittel- bis langfristig eine sichere Datenhaltung nicht garantiert werden kann.

Viele Menschen werden aus oben genannten Gründen eine E-ID auf dem Weg des Liveness-Checks nicht beantragen. Wir halten es für zwingend notwendig, dass gleichwertig eine E-ID-Erstellung auch bei einer staatlichen Stelle wie dem Passbüro oder Gemeindeverwaltung ermöglicht wird. Eine solche analoge Option hätte die oben genannten Probleme des Liveness-Checks nicht und wäre eine zweckdienliche Alternative.

Art. 10 Vorweisen einer E-ID

Forderung:
1. Abs. 1 neu: Das Vorweisen der E-ID darf nur verlangt werden, wenn die Ausweispflicht in einem Gesetz vorgesehen ist.
2. Streichung des letzten Teilsatzes

Der Artikel wird mit "Vorweisen einer E-ID" betitelt, bietet inhaltlich aber nur eine unvollständige Regelung, unter welchen Umständen die E-ID statt anderen Ausweismöglichkeiten vorgewiesen werden muss. Es fehlt somit im ganzen Gesetz ein konkreter Grundsatz zur Vorweisung. Der Artikel sollte entsprechend einen neuen ersten Absatz erhalten, der die Vorweisung generell regelt und gleichzeitig einer inflationären Ausweispflicht vorbeugt.
Deswegen neu Abs. 1: Das Vorweisen der E-ID darf nur verlangt werden, wenn die Ausweispflicht in einem Gesetz vorgesehen ist.

Der Artikel, wie er im Entwurf steht, sieht vor, dass grundsätzlich andere Ausweismöglichkeiten weiterhin gleichwertig benutzbar bleiben sollen. Der letzte Teilsatz des Artikels relativiert aber alles Vorhergehende mit einem schwammigen Verweis auf "Anforderungen insbesondere an die Sicherheit des Prozesses". Wenn die Ausweise vor der Einführung der E-ID den Anforderungen genügt haben, sollte man davon ausgehen,

dass dies danach auch noch so sein sollte. In jedem Fall ist der Verweis auf "Anforderungen insbesondere an die Sicherheit des Prozesses" zu nichtssagend und offen, um als Grund herzuhalten.

Art. 11 Informationssystem zur Ausstellung und zum Widerruf der E-ID

Forderung:
1. Keine Speicherung der Daten aus dem Verifikationsprozess (Streichung von Abs. 2 lit. b).
2. Senkung der Aufbewahrungsfrist

Abs. 2
Der Artikel bestimmt, dass das fedpol ein "Informationssystem zur Ausstellung und zum Widerruf der E-ID" betreibt.
Abs. 2 legt sodann fest, welche Daten darin festgehalten werden. Darunter fallen unter anderem "die Daten zum Ausstellungsprozess" (lit. b). Wie in unserer Stellungnahme zu Artikel 4 ausgeführt, werden die Daten aus dem Verifikationsprozess selbst zu einem möglichen Ziel für Cyberkriminalität.

Abs. 5
Eine Aufbewahrungsfrist von fünf Jahren erscheint exzessiv. Sie sollte auf ein deutlich tieferes Minimum begrenzt werden.

Art. 16 Vorweisen von elektronischen Nachweisen

Forderung:
Der Verifikator darf nur die minimal nötigen Daten abfragen, muss diese beim erstmöglichen Zeitpunkt wieder löschen und darf diese, unter Strafe, nicht anderweitig bearbeiten.
Verwendung von Zero-Knowledge Proofs

Abs. 1 bestimmt, dass der Inhaber oder die Inhaberin des Nachweises bestimmt, welche Daten an die Verifikatorin übertragen werden. Auch wenn dieser Ansatz grundsätzlich gut ist, ignoriert er ein mögliches Machtgefälle zwischen den Parteien. Der Inhaber kann so u.U. dazu gedrängt oder getäuscht werden, mehr Daten herauszugeben, als tatsächlich nötig wären.

Um der Datensparsamkeit (Art. 1 Abs. 2 lit. b) und dem Datenschutz durch Technik (Art. 1 Abs. 2 lit. a) zu genügen, sollte ausserdem, wo immer möglich, auf Zero-Knowledge Proofs gesetzt werden. Dies bedeutet, dass auch die vorhandenen Informationen nicht übergeben werden, wenn der Nachweis durch anonymere Angaben erreicht werden kann. Beispielsweise genügt es bei Alkoholkauf der Verifikatorin ein "erlaubt/volljährig" anzuzeigen, statt das Geburtsdatum selbst.

Art. 17 Basisregister

Forderung:
Entzug der Gültigkeit des Nachweises statt Widerruf

Der Bund führt ein Basisregister, um u.a. die Echtheit der Nachweise zu bestätigen. Nach Abs. 1 lit. c bzw. Abs. 2 lit. d wird auch der Widerruf von elektronischen Nachweisen festgehalten. Aus dem erläuternden Bericht ist leider nicht ersichtlich, wieso nicht stattdessen schlicht die Gültigkeit entzogen werden kann. Wenn ein Nachweis mit Widerruf markiert ist, lässt dies immer noch darauf schliessen, dass die Daten vermutlich echt waren, was den Wert von diesen für Cyberkriminelle (oder Datenkraken) erhöht.

Der erläuternde Bericht erwähnt ausserdem die Verwendung von Blockchain als mögliche Grundlage für das Basisregister. Einerseits sind Blockchains lange nicht so manipulationssicher, wie häufig dargelegt. Andererseits gibt es bis jetzt keinen Anwendungsfall, den die Blockchain-Technologie besser löst als herkömmliche Alternativen. Auf eine Blockchain ist entsprechend zu verzichten, insoweit es hier nur aus modischen Gründen Erwähnung fand.

Art. 19 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Forderung:
1. Die Anwendung muss hohen Sicherheitsstandards genügen.
2. Das Anbieten einer externen Speicherung der Daten sollte angeboten werden.

Der Bund sieht eine sogenannte Wallet-App vor, um die elektronischen Nachweise aufzubewahren. Hierbei vermissen wir die Anerkennung des Schutzbedürfnisses der Daten, welche insbesondere gegenüber Malware und physischem Verlust zu schützen sind.
Durch unterschiedliche Sicherheitslevels von Handys, veralteten Systemen oder schlicht

durch die durchgehende Verfügbarkeit auf einem ständig vernetzten Gerät ist es aus unserer Sicht fragwürdig, ob genügend sichergestellt werden kann, dass die Daten auch sicher bleiben. Es sollte deshalb die Möglichkeit geboten werden, die Daten auf einem Offline-Speicher, wie einer verschlüsselten NFC-Chipkarte, getrennt aufzubewahren.

Art. 20 Anwendung zur Prüfung von elektronischen Nachweisen

Forderung: Der Bund stellt in jedem Falle eine solche Anwendung zur Verfügung. Die optionale Formulierung ist durch eine obligatorische zu ersetzen.

Art. 21 System für Sicherungskopien

Abs. 2
Forderung:
E2E Verschlüsselung der Sicherheitskopien

Die Sicherheitskopien der E-ID müssen aus Sicherheitsgründen explizit mit einer Ende-zu-Ende-Verschlüsselung geschützt werden, sodass nur die Inhaberin oder Inhaber.

Art. 22 Missbrauch

Forderung:
Der Bund informiert nicht nur über (Verdachts-)Missbrauch der Vertrauensinfrastruktur, sondern über sämtliche Fälle im Ökosystem E-ID.

Nur mit Transparenz kann Vertrauen geschaffen werden. Und der Steuerzahler/Nutzer hat ein Recht darüber informiert zu werden, ob es in diesem sensiblen Bereich zu einem Datenreichtum oder Manipulation gekommen ist.

Art. 26 Gebühren

Abs.2
Forderung:
Keine Gebühren für Sicherheitskopien
Der Absatz sieht Gebühren für Sicherheitskopien vor. Die Datenmenge ist überschaubar und eine Sicherung der E-ID sollte kostenfrei sein, da allein schon der administrative Aufwand des Inkassos in keinem Verhältnis zu den eigentlichen Kosten steht.

Darüber hinaus:
Dem E-ID-Gesetz sollte ein neuer Absatz über Strafbestimmungen hinzugefügt werden, der Strafandrohungen bei Missbrauch der Daten vorsieht (vgl. z.B. Art. 16). Das Datenschutzgesetz alleine reicht nicht aus.

Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontaktdetails für Rückfragen finden Sie in der Begleit-E-Mail.

Quellen:
[1] www.bsv.admin.ch/bsv/de/home/sozialversicherungen/ahv/grundlagen-gesetze/ahv-nummer.html
[2] https://www.youtube.com/watch?v=epW4xEqr3mw&t=689s

———

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 17. Oktober 2022