23.073 – Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID)

Die Digitale Gesellschaft hat die gesellschaftliche, politische und technische Debatte zum ersten E-ID-Gesetz eng begleitet und das Referendum sowie die Volksabstimmung massgeblich geprägt. Die Hauptkritikpunkte des Gesetzes betrafen den Zweck und die Herausgeberschaft sowie den mangelnden Datenschutz. Die Digitale Gesellschaft wie auch das E-ID-Referendum begrüssen daher die Neuausrichtung des E-ID-Gesetzes.

Jedoch ist der Schutz der Persönlichkeit und der Personendaten im nun vorliegenden Entwurf zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (BGEID) noch unzureichend umgesetzt sowie der Schutz vor Missbrauch der Daten noch unzureichend gewährleistet. Dies betrifft insbesondere die **Identitätsprüfung** und die drohende **«Überidentifikation»** (Art. 22). Zudem ist für uns nicht nachvollziehbar, wieso der Quellcode der Vertrauensinfrastruktur nicht unter einer anerkannten **Open Source Lizenz** veröffentlicht werden soll.

Art. 7 Anwendung zur Aufbewahrung und Vorweisung von elektronischen Nachweisen

Aus dem Wortlaut von Art. 7 Abs. 2 ergibt sich noch nicht eindeutig, dass der Zugriff auf die Sicherheitskopien durch andere Personen – inkl. Mitarbeiter:innen des BIT – technisch unterbunden sein soll.

Art. 7 Abs. 2 letzter Satz: «Das BIT stellt sicher, dass die Kopien vor dem Zugriff *durch das BIT sowie* durch Dritte geschützt werden.»

Art. 11 Quellcode der Vertrauensinfrastruktur

Gemäss Botschaft soll mit der Veröffentlichung des Quellcodes der Vertrauensinfrastruktur allen Interessierten ermöglicht werden, den offen gelegten Code zu *testen*. Da rund um die E-ID ein Ökosystem mit möglichst tiefen Eintrittshürden geschaffen werden soll, ist es unverständlich, dass der Quellcode nur zum *Testen* und nicht generell unter einer anerkannten Open Source Lizenz veröffentlicht werden soll. Dies betrifft insbesondere den Quellcode zur Aufbewahrung und zur Prüfung der Nachweise; soll aber nicht darauf beschränkt sein. Die vorgesehene Regelung würde zudem Art. 9 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) vom 17. März 2023 widersprechen.

Art. 11 Abs. 1 erster Satz: «Das BIT veröffentlicht den Quellcode der folgenden Elemente der Vertrauensinfrastruktur *als Open Source Software*:»

Art. 16 Identitätsprüfung

Die seit dem Vorentwurf klarer geregelte Identitätsprüfung inklusive dem Ausstellungsprozess und die nun zusätzlich mögliche persönliche Ausstellung (neben dem Online-Ausstellungsprozess), ist zu begrüssen. Dennoch möchten wir nochmals nachdrücklich darauf hinweisen, dass eine Untersuchung des deutschen Chaos Computer Club (CCC) 2022 gezeigt hat, dass sämtliche gängigen Systeme zur «Video-Identifikation» Schwachstellen aufweisen, die einen Identitätsdiebstahl möglich machen. Auch wenn ein Identitätsdiebstahl durch einen «Deep-Fake» in Verbindung mit dem Abgleich des Gesichtsbild aus dem ISA oder dem ZEMIS allenfalls schwieriger durchzuführen ist, wäre eine erfolgreiche Demonstration eines Identitätsdiebstahls verheerend für das Vertrauen und die Akzeptanz der E-ID.

Aus diesem Gesichtspunkt ist auf ein reiner Online-Ausstellungsprozess zu verzichten. Zudem muss der Ausstellungsprozess gemäss Art. 16. Abs. 2 für die persönliche Ausstellung (beispielsweise an die Ausstellung einer herkömmlichen ID) angepasst werden, da in diesem Fall ein (Online-)Abgleich des Gesichtsbildes nicht notwendig ist («Privacy-by-Design»; und diese Daten auch nicht aufbewahrt werden müssen).

Art. 22 Sorgfaltspflicht der Verifikatorinnen

Für den Persönlichkeitsschutz ist es essentiell, dass die Verifikatorinnen nicht frei über die Erfordernis des elektronischen Nachweises und deren Umfang bestimmen können sollen – sondern dies gesetzlich auf das unbedingt Erforderliche beschränkt wird. Wir begrüssen, dass seit dem Vorentwurf Bestimmungen ergänzt worden sind, welche die drohende «Überidentifikation» adressieren und dieser damit den geforderten Prinzipien «Privacy-by-Design» und Datensparsamkeit näher kommt. Wir sehen jedoch weiterhin zwei Mängel:

1. Definition der Einschränkung

Die Einschränkung nach Art. 22 Abs. 1 lit. b («die Zuverlässigkeit der Transaktion davon abhängt, insbesondere um Missbrauch und Identitätsdiebstahl zu verhindern») ist zu weit formuliert. Dies bestätigt auch die Botschaft, welche hier ebenfalls einen erheblichen Interpretationsspielraum einräumt (und leider mit den angeführten Beispielen nicht überzeugt).

Art. 22 Abs. 1 lit. b: «*diese unbedingt erforderlich sind*, insbesondere um Missbrauch und Identitätsdiebstahl zu verhindern»

2. Rechtsfolgen

Bei einer Missachtung der Sorgfaltspflicht droht den Verifikatorinnen gemäss Art. 22 Abs. 2 lediglich einen Eintrag in das (Nicht-)Vertrauensregister. Aus Sicht der betroffenen Personen wäre mindestens eine Warnung in der App, wenn eine Verifikatorin nicht zulässige Personendaten abfragt und im Verzeichnis aufgeführt ist, zu erwarten. Besser wären strafrechtliche Sanktionen. Weitgehend unklar bleibt auch, wie es zum Eintrag kommt, was dies konkret bedeutet und wie sich betroffene Verifikatorinen wehren können. Dies sollte im Gesetz und nicht erst in der Verordnung geregelt werden.

Im Dezember 2023 hat die EU den Gesetzestext zur neuen eIDAS-Verordnung im Trilog verabschiedet. Die Verordnung sieht in Art. 6b vor, dass sich die Verifikatorinnen (Relying Parties) registrieren lassen und den Grund sowie die Personendaten angeben müssen, die sie aus der E-ID abfragen wollen. Ein solches Positiv-Register ist einem (Nicht-)Vertrauensregister, wie es das E-BGEID versieht, vorzuziehen. Das bereits vorgesehene Vertrauensregister (Art. 3) könnte problemlos als ein solches Register für private Verifikatorinnen vorgeschrieben werden.

Basel, 15. Januar 2024

Digitale Gesellschaft
4000 Basel
Schweiz

www.digitale-gesellschaft.ch
office@digitale-gesellschaft.ch

E-ID-Referendum
c/o Public Beta
Postfach 1853
4001 Basel

info@e-id-referendum.ch