Chaos Computer Club Wien (C3W)
buero@c3w.at

Chaos Computer Club Wien

Stellungnahme zum Ministerialentwurf 316/ME

„Bundesgesetz, mit dem das E-Government-Gesetz geändert wird“

1. Allgemeines

Wir begrüßen, dass der Gesetzgeber daran arbeitet, Initiativen zur Verbesserung des Identifikationsmanagements, insbesondere im elektronischen Bereich und im Zusammenhang mit anderen EU-Mitgliedstaaten, zu setzen. Allerdings entspricht der vorliegende Ministerialentwurf weitgehend den „Sicherheitsvorstellungen“ einer zentralisierten Überwachungsbehörde.

Eine Abschätzung von Auswirkungen und Risiken für unsere demokratische Gesellschaft fehlt ebenso wie eine Abschätzung der mit einer Umsetzung verbundenen technischen Risiken (siehe Medienberichte „zentrale Hochsicherheitsserver im Innenministerium“).

Wenn darüber hinaus in den Erläutungen zu dem Ministerialentwurf im Rahmen der „vertrauenswürdigen, zentralen Stelle“ gleich von der „Stammzahlenregisterbehörde bzw. bei einem ihrer Dienstleister“ gesprochen wird, deutet dies darauf hin, dass die Überwachungsbehörde in dem Zug gleich wirtschaftsfreundlich auf den freien Markt ausgelagert wird.

Eine Verbesserung der bestehenden Regelung setzt voraus, dass je nach Bedarfsfall und unter Kontrolle der Nutzerinnen und Nutzer, ausschließlich zwingend notwendige Informationen übermittelt werden. Dazu gehört auch, dass Nutzerinnen und Nutzer nach eigenem Entscheiden anonym, pseudonym, identifiziert oder autorisiert auftreten können. Daten, die für den jeweiligen Anwendungsfall nicht benötigt werden, dürfen keinesfalls gespeichert, abgefragt oder übermittelt werden („need to know“)

2. Privacy by Design

Dieser Ministerialentwurf entspricht nicht der Anforderung „Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit

Chaos Computer Club Wien (C3W)
buero@c3w.at

ein schutzwürdiges Interesse daran besteht“ (§ 1 (1) DSG 2000). Der vorliegende Ministerialentwurf widerspricht auch dem Prinzip „Privacy by Design“, das mit der europäischen Datenschutzgrundverordnung festgeschrieben ist, die 2018 auch in Österreich umgesetzt wird.

3. Föderale Ansätze statt Nischenlösungen

Es ist als problematisch anzusehen, dass Wirtschaftsunternehmen, die nicht dem europäischen Datenschutzrecht unterliegen, den Markt für Identitätsmanagement im Internet (derzeit Facebook ID-Management) dominieren. Ebenso dürfen in Europa - und damit auch in Österreich - keine Systeme entstehen, die nicht dem Grundsatz der größtmöglichen Sicherheit von Freiheit und Privatsphäre entsprechen. Wünschenswert wären Vorgaben durch diese Gesetzesänderung, die Lösungen mehrerer, dezentraler Anbieter fördern würden, anstelle eines Gesetzes, das offensichtlich auf lokale Nischenanbieter und einen „single point of control“ = single point of failure maßgeschneidert wurde.

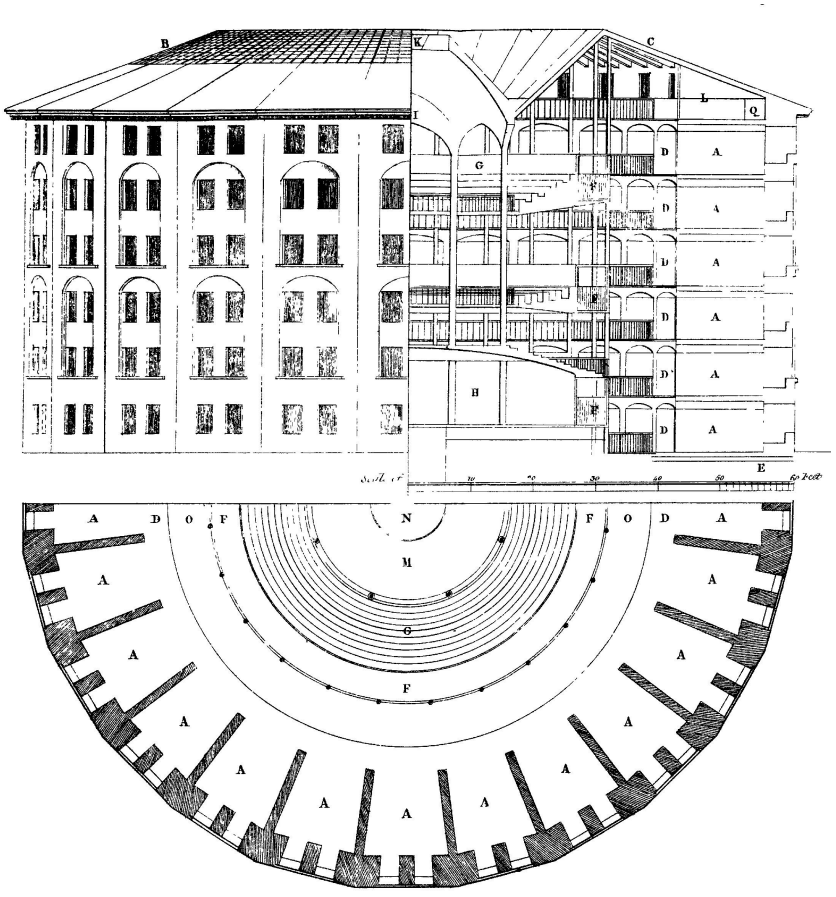

Abbildung: Panopticon-Skizze von Jeremy Bentham (1791)

Chaos Computer Club Wien (C3W)
buero@c3w.at

Chaos Computer Club Wien

4. Globales Denken statt engmaschige Totalüberwachung

Der vorliegende Ministerialentwurf entspricht dem Gedankengut des 19. Jahrhundert: zentrale Überwachung der Bürgerinnen und Bürger ohne Kontrollmöglichkeit durch Betroffene. Dieses Denken ist angesichts unserer heutigen vernetzten, stetig globaler agierenden Welt in allen Bereichen des Lebens, insbesondere auch der Wirtschaft und Politik, nicht mehr haltbar.

5. Datenreichtum

Im vorliegenden Ministerialentwurf sind Merkmale zur Abfrage und Speicherung vorgesehen, die zur Feststellung einer digitalen Identität nicht benötigt werden und außerdem wechseln können (z.B. Mobiltlefonnummer, E-Mail-Adresse, …) .

§ 4b. Die mit der Registrierung des E-ID betrauten Behörden haben als Auftraggeber

1. den Namen,
2. das Geburtsdatum,
3. den Geburtsort,
4. das Geschlecht,
5. die Staatsangehörigkeit,
6. das bPK,
7. die Zustelladresse,
8. das Lichtbild,
9. das Registrierungsdatum,
10. die Telefonnummer eines Mobiltelefons,
11. die E-Mail-Adresse,
12. die Registrierungsbehörde und
13. den Identitätscode des ausgestellten Zertifikats gemäß § 4 Abs. 4

in der Datenanwendung gemäß § 22b Passgesetz 1992 zu verarbeiten.)

Die automatische Weitergabe etwa der E-Mail-Adresse und Mobiltelefonnummer an das Bundesministerium für Inneres, welches diese wiederum an Dritte weitergeben darf, entbehrt jeder Rationale wie auch Grundlage und lässt eindeutig auf den Wunsch kommerziellen Adresshandels, der Schaffung weiterer Märkte für die Österreichische Staatsdruckerei und den „Vertrauensdiensteanbieter“ A-Trust, sowie ein Interesse des BMI selbst an diesen Daten schließen.

Zusammen mit der im Gesetz festgeschriebenen Pflicht, diese Daten auch an das BMI weiterzuleiten, wird der Eindruck erweckt, dass geplant ist, über diese Parameter

Chaos Computer Club Wien (C3W)
buero@c3w.at

nicht nur eine Personenidentifikation, sondern auch über die Ortungsfunktion eines Mobiltelefons den Aufenthaltsort derselben Person lückenlos über den Tagesverlauf (nach)verfolgbar zu machen.

Die Erfassung von E-Mail-Adresse und Mobiltelefonnummer ergibt nur dann einen Sinn, wenn diese Informationen auch aktualisiert und gepflegt werden. Beide Datenpunkte sind hochgradig volatil. Wie und durch wen diese aktualisiert werden sollen und ob für die Bürgerinnen und Bürger daraus eine „erweiterte Meldepflicht" erwächst, wird durch diesen Ministerialentwurf in keinster Weise berücksichtigt. Ein Lösungungsansatz für dieses Problem, dass beispielsweise Mobilfunkanbieter verpflichtet werden, ihre Kundendatenbanken mit staatlichen Stellen zu teilen, wird in dem Gesetzesvorschlag nicht erwähnt und wäre auch ausdrücklich nicht wünschenswert. Eine alternative manuelle Wartung und Pflege dieser Datenpunkte verursacht in jedem Fall weit mehr Aufwand - und damit Kosten - als diese jemals Nutzen bringen könnten.

Ebenfalls geflissentlich ignoriert wurde durch die Verfasser dieses Gesetzesvorschlags, dass diese Datensätze für manche Menschen überhaupt nicht zutreffend sind. Es gibt zahlreiche Bürgerinnen und Bürger, die entweder gar keine eigene E-Mail-Adresse oder (Mobil-)Telefonnummer besitzen bzw. diese aus diversen Gründen nicht publik machen möchten oder auch regelmäßig wechseln. Wird gar künftig auch für Minderjährige oder andere vertretungsbedürftige Personen ein mobiles Telefon verbindlich erforderlich sein?

6. Zugriffskontrolle

Im vorliegenden Ministerialentwurf ist eine zentrale Speicherung jeder Verwendung der digitalen Identität vorgesehen und damit die Möglichkeit, anhand dieser Protokollierung einen lückenlosen Nachweis über das Verhalten aller erfassten Individuen zu führen. Identitätsmanagementsysteme, dazu zählt E-ID, sind aus unserer Sicht grundsätzlich so zu gestalten, dass durch technische Maßnahmen die Beobachtung des Nutzerverhaltens ausgeschlossen ist, um weitreichenden Missbrauch zu verhindern. Zulässige Zugriffe sind hierfür taxativ aufzuzählen, ein darüber hinausgehender Zugriff ist unzulässig und zu verhindern. Die Möglichkeit des Bundesministers für Inneres, Dritten nach die Nutzung des E-ID-Systems zu eröffnen, sehen wir kritisch. Diese „Dritten" sind zu benennen und bereits im Gesetz auf wenige Möglichkeiten einzuschränken.

Chaos Computer Club Wien (C3W)
buero@c3w.at

7. Schutzmaßnahmen

Schutzmaßnahmen gegen unzulässigen, missbräuchlichen oder überschießenden Zugriff auf Verwendungsdaten fehlen im vorliegenden Ministerialentwurf völlig bzw. sind, wenn sie genannt werden, unzureichend.

So wird beispielsweise in den Erläuterungen ausgeführt, dass es bei Single Sign On Lösungen wie einem Portal zu „keiner Speicherung von bPK in der Portalanwendung kommen darf." Im vorgeschlagenen Gesetzestext fehlt dieser Passus in dieser klaren Formulierung hingegen komplett. Genauso wie die Anweisungen, wie mit den im Portal angezeigten Daten aus den diversen Anwendungen umzugehen ist. Hier sehen wir deutlichen Bedarf für Nachbesserungen.

In § 4 Abs. 6 wird - laut den Erläuterungen zum vorliegende Gesetzesvorschlag - die Möglichkeit der zeitlich begrenzten Speicherung weiterer Merkmale durch den E-ID-Inhaber zu seiner E-ID vorgesehen, um auch ohne Internetanbindung bestimmte Merkmale Dritten gegenüber nachweisen zu können.
Abgesehen davon, dass laut der österreichischen Bundesregierung und dem Bundeskanzleramt ab dem Jahre 2020 mit 5G drahtloses Internet flächendeckend in Österreich vorhanden sein wird, fehlen auch bei diesem Punkt klare Vorgaben über beispielsweise Speicherdauer, notwendige Datenschutzmaßnahmen wie beispielsweise Datenverschlüsselung oder zugriffsberechtigte Dritte.

Offensichtlich sollen hier Lösungen wie etwa „MIA" der Österreichischen Staatsdruckerei GmbH bedient werden, damit Jugendliche über eine App auch im Keller ohne Internetempfang am Disko-Eingang ihre Identität nachweisen können.

Die Vergangenheit hat gezeigt, dass Mobiltelefone ein denkbar schlechter Ort sind, um vertrauliche oder sicherheitsrelevante Informationen - *und damit auch staatliche Ausweisdokumente* - abzulegen oder abzurufen:

- **Die Tücken der digitalen Ausweise**
  `http://orf.at/stories/2204173/2204174/`
- **Sicherheitslücken beim Fintech-Startup N26**
  `http://t3n.de/news/33c3-n26-781238/`
- **pushTAN-App der Sparkasse nach wie vor angreifbar**
  `https://heise.de/-3056667`
- **Hacker räumten Bankkonten leer**
  `http://derstandard.at/2000056893783/`

Chaos Computer Club Wien (C3W)
buero@c3w.at

Durch die Wesenseigenheit von Smartphones als portable Computer mit Internetanschluss und Telefonfunktion sind zum Einen „Offlineverbrechen“ wie Diebstahl und Auslesen der gespeicherten Daten möglich, aber ebenso „Onlineverbrechen“ wie beispielsweise eine Übernahme der Geräte oder einzelner darauf gespeicherter Daten, womit auch ein Identitätsdiebstahl vereinfacht wird.

Ohne klare Vorgaben und Sicherheitsrichtlinien für Lösungsanbieter zur Nutzung der E-ID ist ein datenschutztechnischer Super-GAU damit vorprogrammiert.

Hinsichtlich der „Vertrauensdiensteanbieter“ sei noch einmal an 2015 erinnert, als der „Vertrauensdiensteanbieter“ A-Trust sein Zertifikat nicht zeitgerecht in den Browsern aktualisierte und damit das halbe österreichische E-Government „offline“ nahm. `https://futurezone.at/-/-/147.690.445`

Ein Funktionieren der Infrastruktur muss zuerst garantiert und auch bewiesen werden, ehe es um weitreichende Entscheidungen über deren Verwendung gehen kann, zumal diese unvermittelte Auswirkungen auf jeden einzelnen Menschen im Land haben.

8. Demokratieverständnis

Der Ministerialentwurf ermöglicht die Schaffung einer vollständigen Überwachungsstruktur, wie es eines demokratischen Staates unwürdig ist. Ein Missbrauch dieser Überwachungstruktur unter geänderten politischen Verhältnissen ist mangels entsprechender Sicherungsmaßnahmen nicht auszuschließen.

9. Zwingende Verknüpfung von Reisepass und E-ID

> *§ 4a. (1) Die Registrierung der Funktion E-ID ist für Staatsbürger im Rahmen der Beantragung eines Reisedokumentes nach dem Passgesetz 1992, BGBl. Nr. 839/1992, von Amts wegen durch die Passbehörde oder durch eine nach § 16 Abs. 3 Passgesetz 1992 ermächtigte Gemeinde vorzunehmen.*

Zunächst einmal stellt sich die Frage, wozu diese Verknüpfung dienen soll, werden hiermit unter anderem doch die technischen Voraussetzungen für Prozesse wie automatisierte Grenzkontrollen, etc. geschaffen.

Weiters fehlt eine Zustimmung Betroffener als Voraussetzung zu Datenverarbeitung. Eine „Opt-Out“ Möglichkeit analog zu beispielsweise ELGA muss bestehen, eine „Opt-In“ Regelung wie bisher bei der „Bürgerkarte“ ist zu bevorzugen.

Chaos Computer Club Wien (C3W)
buero@c3w.at

Im Rahmen dieses Paragraphen ist völlig ungeklärt, wie Passbehörde und Gemeinden mit Anträgen umzugehen haben, deren Daten gemäß Passgesetz vollständig sind, aber für die Austellung einer E-ID nicht ausreichen, zumal es ein gesetzlich festgeschriebenes Recht auf die Ausstellung eines staatlichen Ausweisdokuments gibt.
Ungeklärt ist hier weiters, wie mit der Ausstellung von E-IDs für Säuglinge, Kinder und noch nicht volljährige Jugendliche oder Personen, die schwer pflegebedürftig, dement oder in anderer Art nicht mehr in der Lage sind, ihre Angelegenheiten selbst wahrzunehmen, umgegangen werden soll.

Bei etwa acht Behördenkontakten im Jahr (Angabe laut Gemeindebund 2014) hat sich die Akzeptanz der bisherigen Bürgerkartenfunktion in Form der e-Card bzw. Handy-Signatur sehr in Grenzen gehalten. Auch hier erweckt der Gesetzesvorschlag wieder einmal den Anschein, dass zu Gunsten des „Vertrauensdiensteanbieters“ A-Trust eine Zwangbeglückung der Bevölkerung mit der E-ID durch die Verknüpfung mit dem Passantrag vorgenommen werden soll.

Anstelle eines Zwanges zur E-ID sollte diese, wie ihr Namensvorläufer „Bürgerkarte“, für die Bürgerinnen und Bürger optional bleiben und die Akzeptanz über sinnvolle Dienste der Behörden und Unternehmen anstelle von Zwangsmaßnahmen geschaffen werden, auch wenn Österreich dadurch in dem einen oder anderen „Ranking“ zurückbleiben sollte.

Vorwegnahme der Gesetzwerdung durch Behörden gegenüber Medien: z.B.:

> *Bei Polizeikontrollen nicht mehr den Führerschein, sondern das Handy vorweisen? Das Innenministerium bereitet eine revolutionäre App vor. Ab Sommer werden erste Feldversuche laufen, staatliche Dokumente durch Apps zu ersetzen, erklärte Markus Popolari, Leiter der Abteilung IKT-Sicherheit und E-Government im Innenministerium.*
> `http://m.heute.at/wirtschaft/news/story/43662446`

Hier werden augenscheinlich Politik und Gesetze gemacht, die die zu bereits vorhandenen, kommerziellen Lösungen betriebswirtschaftlich agierender Unternehmen passen sollen und somit deren Wertschöpfungs-Portfolio aus Steuermitteln ergänzen.

10. Versäumnisse bei technischen Definitionen

Es wurde verabsäumt, die technischen Rahmenbedingungen, etwa bei der Berechnung der bPK, auf zeitgemäße technische Standards zu heben. So wird etwa SHA1 für

Chaos Computer Club Wien (C3W)
buero@c3w.at

die Brechnung von cryptografischen Hash-Wertern nicht mehr als kollisionsfrei und sicher angesehen. Hier wäre SHA256 oder besser zu definieren. Auch RSA-Schlüssel mit einer Länge von 1024 Bit gelten nicht mehr als sicher. Hier sollten 4096 Bit als Minimum definiert und vorzugsweise auch gleich ein Wechsel auf zeitgemäßere Algorithmen wie Elliptic Curve vorbereitet werden.

Fazit

Der vorliegende Ministerialentwurf enstpricht eindeutig nicht den europäischen Grundwerten und wirkt wie der Versuch, das Schutzniveau der kommenden Datenschutzgrundverordnung kurz vor deren Inkrafttreten zu unterlaufen, sowie staatsnahen Unternehmen neue Geschäftsfelder zu eröffnen.

Der Ministerialentwurf 316/ME ist aus Sicht des C3W daher abzulehnen.

Ergeht an:
Präsidium des Nationalrats
begutachtungsverfahren@parlament.gv.at

Bundeskanzleramt
Abteilung I/11
Ballhausplatz 2
1010 Wien
i11@bka.gv.at