**Epizentrum – Plattform für grundrechtsbasierte Zukunftspolitik (vormals AKVorrat)**

**Annagasse 8/1/8, 1010 Wien**
**team@epicenter.works**
**www.epicenter.works**
**ZVR: 140062668**

**Wien, 22. Mai 2017**

**Betreff:**

**Stellungnahme im Begutachtungsverfahren[1] zum Ministerialentwurf des Bundeskanzleramtes, mit dem das E-Government-Gesetz geändert wird (E-ID Gesetz) (XXV. GP 316/ME)**

Für epicenter.works:
Dipl.-Ing. Dr. iur. Walter Hötzendorfer, Mag.iur. Alexander Czadilek, Thomas Lohninger

**epicenter.works nimmt zu dem Entwurf wie folgt Stellung:**



[1] https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00316/index.shtml

# Kurzfassung

Unsere Stellungnahme bezieht sich insbesondere auf folgende Punkte:

- Eine wirkungsorientierte Folgenabschätzung (WFA) hinsichtlich der grundrechtlichen Auswirkungen der vorgeschlagenen Änderungen des E-Government-Gesetzes, insbesondere im Hinblick auf den Schutz der Privatsphäre und den Datenschutz wurde nicht durchgeführt.
- Die vorgeschlagene Gesetzesnovelle schafft die Gefahr eines umfassenden staatlichen Einblicks in Online- und Offlineaktivitäten der Bürgerinnen und Bürger. Maßnahmen, um dies wirksam zu verhindern, sind im Entwurf nicht ersichtlich.
- Im Entwurf sind keine konkreten Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit ersichtlich, insbesondere im Hinblick auf das Schutzziel der Beschränkung der Beobachtbarkeit des Verhaltens der Betroffenen.
- Laut dem Entwurf soll die Ausstellung eines Reisepasses offenbar verpflichtend mit der Registrierung eines E-ID einhergehen.

# Grundsätzliche Bemerkungen

## Vorbemerkungen

Initiativen auf dem Gebiet des Identitätsmanagements sind grundsätzlich zu begrüßen. Die Möglichkeiten für Nutzerinnen und Nutzer, bei Bedarf ihre Identität und/oder bestimmte persönliche Eigenschaften via Internet zu belegen, sind heute nach wie vor unzureichend, und zwar in den Dimensionen **Sicherheit, Nachweisbarkeit, Komfort (Usability), Datenschutz sowie Transparenz und Kontrolle**.

Es werden Systeme benötigt, die es ermöglichen, nur jene Identitätsinformationen zu übermitteln und zu verarbeiten, die für den jeweiligen Zweck unbedingt erforderlich sind, und den Nutzerinnen und Nutzern die Kontrolle darüber zu geben, wann sie anonym oder pseudonym und wann sie identifiziert auftreten. Dies ist rechtlich geboten, denn es verstößt gegen den **datenschutzrechtlichen Grundsatz der Zweckbindung**, dass im Zuge der Identifikation und Authentifizierung via Internet mehr Daten übermittelt werden, als für den Zweck der Identifikation bzw. Authentifizierung unbedingt erforderlich sind.

Seit der Popularisierung der Web-Nutzung um die Jahrtausendwende wurden auf dem Gebiet des Identitätsmanagements Systeme und Standards entwickelt und zum Teil auch

ausgerollt. Es dominiert jedoch nach wie vor der Wildwuchs an Benutzerkonten, die unter Angabe selbst behaupteter Attribute und eines Passworts für die Nutzung jedes einzelnen Service im Internet neu angelegt werden müssen. Die meisten Nutzerinnen und Nutzer haben den Überblick über „ihre" Benutzerkonten und Passwörter längst verloren, von den zahlreichen grundsätzlichen Unzulänglichkeiten des Konzepts Passwort ganz zu schweigen. Hinzu kommt in den letzten Jahren die Dominanz einiger weniger Player auf dem Identitätsmarkt, wie insbesondere Facebook und Google.

## Zentrale Beobachtbarkeit des Nutzerverhaltens

Die soeben angesprochenen Unternehmen belegen am deutlichsten das Kernproblem, das mit zentralisierten Identitätsmanagementsystemen untrennbar verbunden ist: Zentralisierte Identitätsmanagementsysteme, wozu auch das vorgeschlagene Konzept E-ID zu zählen ist, bergen stets die Gefahr, dass an zentraler Stelle ein oder mehrere Akteure Einsicht in die Interaktionen und Transaktionen der Nutzerinnen und Nutzer erhalten und somit in der Lage sind, deren Verhalten zu überwachen und zu analysieren.

Die Wissenschaft spricht diesbezüglich vom Schutzziel der **Unbeobachtbarkeit** (engl. *unobservability*) bzw. **beschränkten Beobachtbarkeit** (engl. *limited observability*)[2], das neben den klassischen Schutzzielen der Informationssicherheit, Vertraulichkeit, Integrität und Verfügbarkeit existiert. Innerhalb des Systems dieser Schutzziele der Informationssicherheit kann die Unbeobachtbarkeit auch als Vertraulichkeit des Verhaltens angesehen werden.[3]

Während die physische Nutzung eines Ausweises grundsätzlich als Vorgang keine Aufzeichnung erfährt und insbesondere ohne Beteiligung und Kenntnis des Ausstellers des Ausweises erfolgt, **generiert jede Nutzung elektronischer Identifizierungsmittel Daten und erfolgt regelmäßig unter Einbindung des Ausstellers**. Deswegen sind Identitätsmanagementsysteme wie E-ID so zu gestalten, dass durch faktische Maßnahmen die Beobachtbarkeit des Verhaltens der Nutzerinnen und Nutzer mittels der laufend anfallenden (Meta-)Daten verhindert wird. Andernfalls entsteht ein System, in dem es wie in Benthams Panopticon möglich ist, das Verhalten der Nutzerinnen und Nutzer im System von zentraler Stelle aus lückenlos zu beobachten.

**Das im vorliegenden Gesetzesentwurf vorgeschlagene System E-ID birgt exakt diese Gefahr einer zentralen Beobachtbarkeit des Nutzerverhaltens**, wobei im vorliegenden Entwurf keine Maßnahmen ersichtlich sind, um dies wirksam zu verhindern. Bei jeder Verwendung des E-ID im öffentlichen oder im privaten Bereich erstellt die Stammzahlenregisterbehörde eine Personenbindung und ist somit als zentraler Akteur in jede Verwen-

[2] Vgl. *Pfitzmann/Hansen*, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, 2010, abrufbar unter http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

[3] Vgl. *Bock/Rost*, Privacy By Design und die Neuen Schutzziele, Datenschutz und Datensicherheit - DuD 2011, 30–35, S. 32.

dung des E-ID im elektronischen Verkehr involviert. Die Stammzahlenregisterbehörde erlangt dadurch Kenntnis von jeder Verwendung des E-ID im elektronischen Verkehr und damit auch von einer im Entwurf nicht näher spezifizierten Menge an personenbezogenen Daten und Metadaten. **Insbesondere ist nicht ersichtlich, durch welche gesetzlich angeordneten technischen und organisatorischen Maßnahmen verhindert wird, dass die Stammzahlenregisterbehörde diese Daten einsehen, sammeln und auswerten kann.** Im Gegenteil unterliegt die Stammzahlenregisterbehörde datenschutzrechtlichen Protokollierungspflichten, die bis zu einem gewissen Grad die Protokollierung des Nutzerverhaltens sogar erfordern. Das Vorhandensein eines zentralen Akteurs ist daher auch aufgrund der daraus folgenden zentralen Protokollierung abzulehnen. Die Protokollierung wird auch in § 18 Abs 3 des Entwurfs angesprochen, worauf unten noch eingegangen wird.

## Das verfassungsmäßig gewährleistete Grundrecht auf Datenschutz

Das eben Gesagte bedeutet nicht notwendigerweise, dass die Stammzahlenregisterbehörde und/oder ggf. andere involvierte Akteure das Nutzerverhalten tatsächlich überwachen. **Dass dies überhaupt möglich ist, verstößt jedoch bereits gegen den datenschutzrechtlichen Grundsatz der Datenminimierung und den mit Art 25 DSGVO neu eingeführten Grundsatz des Datenschutzes durch Technik (Privacy by Design/Data Protection by Design) sowie den Grundsatz, Eingriffe in schutzwürdige Geheimhaltungsinteressen nur mit dem gelindesten zur Verfügung stehenden Mittel vorzunehmen,** d.h. von mehreren geeigneten und erforderlichen Datenverwendungen jene durchzuführen, die am wenigsten in die Geheimhaltungsinteressen der Betroffenen eingreift, wobei dies alle Dimensionen der Datenverwendung betrifft, also die Form der Datenverwendung sowie Art, Inhalt und Umfang der verarbeiteten Daten und auch die zeitliche Dimension.[4]

Es ist daher durch das verfassungsmäßig gewährleistete Grundrecht auf Datenschutz geboten, ein Identitätsmanagement-System wie E-ID so zu gestalten, dass die Beobachtbarkeit durch technische und organisatorische Maßnahmen ausreichend beschränkt ist. Solche Maßnahmen sind jedoch im vorliegenden Entwurf nicht ersichtlich.

Welche Maßnahmen dies sein könnten und dass dies faktisch möglich ist, zeigen zahlreiche in den letzten Jahren entwickelte Identitätsmanagement-Konzepte, die die Umsetzung des Schutzziels der Beschränkung der Beobachtbarkeit ermöglichen, in Verbindung mit der – auch im Konzept E-ID vorgesehenen – Möglichkeit, beispielsweise nur die Volljährigkeit nachzuweisen, ohne weitere Identitätsdaten preiszugeben.[5]

[4] Vgl. *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, Verlag Österreich, Wien 2014, S. 411.

[5] Siehe z.B. die Ergebnisse des Projekts ABC4Trust, abrufbar unter https://abc4trust.eu sowie *Hötzendorfer*, Datenschutz und Privacy by Design im Identitätsmanagement, Verlag der Österreichischen Computer Gesellschaft (OCG), Wien 2016.

Es ist nicht ausgeschlossen, dass das System E-ID im Rahmen der Bestimmungen des vorliegenden Entwurfs so umgesetzt werden kann, dass der Beschränkung der Beobachtbarkeit des Nutzerverhaltens zumindest bis zu einem gewissen Grad Rechnung getragen wird. **Im Kontext des Grundrechts auf Datenschutz ist es jedoch geboten, bereits im Gesetz (und nicht bloß in einer zu erlassenden Verordnung) ausdrücklich zu determinieren, dass und wie das System in Einklang mit dem verfassungsmäßigen Grundecht auf Datenschutz umgesetzt wird.**

# Weitere Kritikpunkte im Einzelnen

## Verpflichtende Registrierung

In § 4a ist die amtswegige Registrierung der Funktion E-ID für Staatsbürger im Rahmen der Beantragung eines Reisedokumentes nach dem Passgesetz 1992 vorgesehen. Dies würde bedeuten, dass mit jeder Ausstellung eines Reisepasses automatisch eine Registrierung des E-ID einhergehen würde. Sollte dies so zu verstehen sein, ist dies abzulehnen. Andernfalls bedarf die Regelung einer diesbezüglichen Klarstellung.

Die Ablehnung einer verpflichtenden Registrierung des E-ID für Staatsbürger im Rahmen der Beantragung eines Reisepasses ist insbesondere wie folgt zu begründen: **Das Begehren, einen Reisepass zu erhalten, darf auf keinen Fall dazu ausgenützt werden, Betroffene zur Registrierung des E-ID zu drängen**.[6] Die Registrierung des E-ID umfasst die Erhebung von personenbezogenen Daten des Betroffenen und überdies besteht bei jedem technischen System die Gefahr der Kompromittierung sowie des Missbrauchs. Es sollte daher die Entscheidung jedes und jeder Einzelnen sein, ob man mit der Erhebung dieser Daten einverstanden ist und sich den – mit jedem informationstechnischen System einhergehenden – Risiken aussetzt. Ein verpflichtendes E-ID-System würde überdies mittelfristig zu einer Situation führen, in der Personen diskriminiert werden könnten, die die Verwendung des E-ID aufgrund persönlicher Einschränkungen oder mangelnder technischer Anwenderkenntnisse nicht nutzen können oder die Nutzung – aufgrund von Datenschutzbedenken oder sonstigen Risiken – ablehnen.

Darüber hinaus wirft die verpflichtende Registrierung des E-ID für Staatsbürger im Rahmen der Beantragung eines Reisepasses praktische Fragen auf: Was sind die Konsequenzen, wenn ein Passwerber die Registrierung des E-ID ablehnt und die entsprechende Mitwirkung daran verweigert? Sofern kein Passversagungsgrund vorliegt (§ 14 PassG), besteht nichtsdestotrotz ein Rechtsanspruch zur Ausstellung eines Reisepasses. Die Ausstellung darf daher auch im Fall der Verweigerung der Mitwirkung an der Ausstellung des E-ID nicht versagt werden.

[6] Umgekehrt sei angemerkt, dass man mit einer solchen fragwürdigen Maßnahme das allfällige Ziel einer flächendeckenden Ausrollung des E-ID trotzdem nicht erreicht, da jene Staatsbürger nicht erfasst werden, die keinen Reisepass beantragen.

## Polizeilicher Zugriff

In § 4b letzter Satz ist die Verwendung der personenbezogenen Daten der Nutzerinnen und Nutzer zu anderen Zwecken als der Verwaltung des E-ID bereits ausdrücklich angesprochen.

Es lässt sich vermuten, dass hierbei an die Verwendung der personenbezogenen Daten für polizeiliche Zwecke und Zwecke der Strafermittlung gedacht ist. Dies ist nicht generell abzulehnen, sollte jedoch mit entsprechenden rechtsstaatlichen Mechanismen ausgestaltet sein, um die Grundrechte der betroffenen Personen zu wahren, was jedoch derzeit nicht abzusehen und im Lichte der jüngeren Gesetzgebungsinitiativen auf dem Gebiet der Polizeibefugnisse nicht zu erwarten ist. Es besteht daher die Gefahr, dass es durch die vorgeschlagene Gesetzesänderung zu einer zweckwidrigen Verquickung von polizeilichen bzw. justiziellen Interessen und Interessen des staatlichen Identitätsmanagements kommt.

## Protokollierung

§ 18 Abs 3 macht Vorgaben über die Protokollierung der Datenübermittlung. Dies betrifft allerdings nach dem Wortlaut nur die Datenübermittlung aus den Registern und somit nicht grundsätzlich die Verwendung der Funktion E-ID und umfasst nicht die Übermittlung von Daten an Dritte in Erfüllung einer gesetzlichen Ermächtigung zur amtswegigen Datenermittlung nach § 18 Abs 1 Z 3 des Entwurfs. Auch die ausdrückliche Regelung der Protokollierung dieser Vorgänge ist geboten, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt.

Die Regelung, dass die Protokollfunktion durch den E-ID-Inhaber deaktiviert werden kann, ist grundsätzlich zu begrüßen, nicht jedoch, dass diese ebenfalls der oben genannten Einschränkung auf die Datenübermittlung aus den Registern unterliegt. Überdies sollte ausdrückglich geregelt werden, dass die Deaktivierung der Protokollfunktion bedeuten muss, dass die Daten überhaupt nicht mehr aufgezeichnet werden.

# Conclusio

## Rechtspolitische Überlegungen

Wie ausführlich dargelegt wurde, ist die Einführung eines E-ID-Systems, das eine zentrale Beobachtbarkeit des Nutzerverhaltens innerhalb des Systems ermöglicht, generell abzulehnen. Dies gilt umso mehr in Zeiten eines fortschreitenden Überwachungsstaats, angesichts dessen es dringend erforderlich wäre, eine „Überwachungsgesamtrechnung“[7] zu erarbeiten bevor weitere Instrumente zur tatsächlichen oder potenziellen Überwachung der Bevölkerung eingeführt werden. Der Aufgabe, eine „Überwachungsgesamtrechnung“ zu erarbeiten, haben sich bislang weder Parlament noch Regierung gestellt.[8]

Zwar ist nicht ausgeschlossen, dass das System E-ID im Rahmen der vorgeschlagenen Bestimmungen so umgesetzt werden kann, dass den oben kritisierten Punkte in gewissem Maße Rechnung getragen wird. Es ist jedoch verfassungsmäßig geboten, gesetzlich zu determinieren, dass und wie das System in Einklang mit dem verfassungsmäßigen Grundecht auf Datenschutz umgesetzt wird.

Über diese grundsätzlichen Erwägungen hinaus sind auch die oben im Einzelnen angesprochenen Regelungen in der vorliegenden Form verbesserungsbedürftig. Insbesondere ist es abzulehnen, dass die Ausstellung eines Reisepasses offenbar verpflichtend mit der Registrierung eines E-ID einhergeht.

## Fehlende Wirkungsfolgenabschätzung

Es ist nicht einzusehen, dass dem Ministerialentwurf keine wirkungsorientierte Folgenabschätzung (WFA) zugrunde liegt, die auf die grundrechtlichen und gesellschaftlichen Auswirkungen der vorgeschlagenen Änderungen des E-Government-Gesetzes eingeht, insbesondere im Hinblick auf den Schutz der Privatsphäre und den Datenschutz, obwohl es sich – wie gezeigt wurde – um eine grundrechtssensible Materie handelt.

[7] Im Urteil zur nationalen Umsetzung der Vorratsdatenspeicherung des deutschen Bundesverfassungsgerichts 1 BvR 256/08 ua wird erstmals von einem europäischen Höchstgericht die Idee und die Notwendigkeit einer „Überwachungsgesamtrechnung“ ausgedrückt.

[8] Ermutigt vom Erfolg der Abschaffung der EU-Richtlinie zur Vorratsdatenspeicherung (VDS), hat das Team von epicenter.works die von der Regierung noch unerfüllte zweite Forderung der BürgerInnen-Initiative „zeichnemit.at“ in die eigenen Hände genommen und eine umfassende Analyse und Evaluation aller Anti-Terror-Gesetze in Österreich erstellt. Für dieses Anliegen hatten 106.067 Österreicher/innen unterschrieben. Siehe dazu: *Tschohl/Scheucher/Kargl/Luksan/Czadilek/Waloschek/Kreissl/Klinger/Hötzendorfer*, HEAT (Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich), abrufbar unter: https://epicenter.works/thema/heat.