Antrag 05

an die Kammer für Arbeiter und Angestellte für Wien

zur Tagung der Vollversammlung am 27.05.2025

der Fraktion

FAIR UND TRANSPARENT

zum Thema

Freiwilligkeit und Wahlmöglichkeit bei Registrierung und Nutzung ID-Austria und anderer eIDs

---

Das AK-Team FAIR UND TRANSPARENT beantragt:

Die Arbeiterkammer Wien setzt sich dafür ein, dass Registrierung und Nutzung elektronischer Identitäten (eIDs) in Europa und insbesondere auch der ID-Austria in Österreich freiwillig bleiben, kein impliziter oder expliziter Zwang dazu ausgeübt wird und es stets Wahlmöglichkeiten und einfach zu handhabende Alternativen dazu gibt.

Bei einer etwaigen Entscheidung dafür müssen Registrierung und Nutzung auch analog und Smartphone-unabhängig möglich und einfach handhabbar sein.

Ein starker Datenschutz muss gewährleistet sein und darf auch nicht von außer-europäischen Behörden oder Organisationen umgangen werden können. Dienste, erforderliche Apps oder Anwendungen müssen deshalb jedenfalls auch von europäischen Plattformen aus einfach installiert, erreicht und genutzt werden können. Plattformen mit US-amerikanischem oder anderem nicht-europäischem Hintergrund wie Google oder Apple sollen nicht Anspruch genommen werden müssen. Entsprechende europäische Alternativen sind zur Verfügung zu stellen.

Begründung:

eIDs in Europa wie die ID-Austria stellen die offizielle elektronische Identität einer Person dar, die den Austausch von persönlichen Daten über die Mitgliedsstaaten hinweg ermöglichen. Dadurch können nunmehr viele Datenbasen des Behördensektors, des Bildungssektors und mittlerweile auch des Privatsektors miteinander verknüpft werden. D.h. über die persönliche Identität können persönliche Informationen wie Führerschein, Bankdaten, Ausbildungen, uvm. elektronisch ausgetauscht werden.

Die ID-Austria ist somit viel mehr als eine digitale Unterschrift, sie ist die offizielle, elektronische Identität einer Person in Österreich. Sie ist nicht einfach nur ein Ersatz für die vorhergehende Handy-Signatur, wie viele Menschen denken.

Die ID-Austria gibt nicht nur Zugang zu vielen Anwendungen, sondern ermöglicht insbesondere auch den Austausch persönlicher Daten, weit über die Identifizierungsdaten hinaus. Dies bringt Vorteile, aber auch Risiken. Nutzer sollen frei entscheiden können, ob sie Verknüpfung und Austausch von persönlichen Daten zustimmen wollen und insbesondere auch welche ihrer Daten verwendet werden dürfen.

Mittlerweile gibt es bereits über 500 Anwendungen für die ID-Austria, künftig könnten noch erheblich mehr dazukommen.
Haupt-Anwendungsmöglichkeiten sind derzeit:

- Digitale Behördenwege
- Elektronische Unterschrift, z.B. für Verträge
- Elektronisches Postamt für Briefe und Co
- Digitaler Ausweis

Aktuell in heftiger Diskussion ist, dass Lehrkräfte in Schulen Zugang zu einem wichtigen Schulsystem seit März 2025 nur noch über ID-Austria erhalten. In dieses System müssen sie selbst Informationen eintragen, erhalten Informationen, und selbst ihren Gehaltszettel können sie nur über dieses System einsehen und downloaden. Die derzeitige Alternative des Tokens ist keine wirklich praktikable Lösung. Implizit stellt diese Vorgehensweise einen Zwang zur persönlichen ID-Austria dar. Ähnliches könnte auf weitere Bereiche und auch in private Unternehmen Einzug halten und damit die Arbeitnehmer nicht nur als Bürger, sondern auch am Arbeitsplatz treffen.

In solchen Fällen wäre es beispielsweise notwendig, dass sich die Arbeiterkammer Wien dafür einsetzt, dass Unternehmen und Behörden auch Zugänge zu Systemen bieten, die nicht auf die offizielle elektronische Identität einer Person zurückgreifen.

Da die ID-Austria – sie ist auch vorgesehen in die eID der EU eingebunden zu werden – wie der offizielle persönliche Identitätsausweis (Reisepass, Personalausweis) fungiert, jedoch aufgrund der elektronischen Basis erheblich mehr Möglichkeiten bietet, sind natürlich auch erhebliche Gefahren mit der ID-Austria bzw. eID verbunden. Dies insbesondere dann, wenn die Menschen hauptsächlich die ID-Austria bzw. eID über ihr Smartphone registrieren und nutzen (können/müssen), weil sie mit dem derzeit verfügbaren Token (FIDO-Sicherheitsschlüssel), der auf einem speziellen USB-Stick gespeichert wird, nicht umgehen können oder von dessen Möglichkeit gar nichts mitbekommen.

Wird die ID-Austria/eID über Smartphone verwendet, sind die erforderlichen Apps wohl über die Smartphone-Stores zu installieren. Diese Stores haben jedoch in der Regel US-amerikanischen oder anderen außer-europäischen Hintergrund. Damit wäre jedoch (indirekt) die Möglichkeit von (unbemerkten) Zugriffen von US-Behörden oder anderen nicht-europäischen Staaten oder Organisationen auf die persönlichen und personenbezogenen Daten des Nutzers gegeben.

Während derzeit unterschiedliche, meist kleinere Systeme mit unterschiedlichen Zugangsdaten zu erreichen sind, bringt die ID-Austria/eID einen einzigen zentralen Zugang, deren Daten wiederum in einem einzigen zentralen System gespeichert sind. Während Ausfälle, Fehler, Cyberangriffe oder andere

Probleme bei kleinen, dezentralen Systemen schon beachtliche Stillstände und Schäden verursachen können, so sind die Auswirkungen bei einem einzigen System de facto nicht abschätzbar.

Doch nicht nur die Systeme selbst, sondern insbesondere auch die darin gespeicherten Daten sind Gefahren und Begehrlichkeiten ausgesetzt.
Die ID-Austria steht auch für eine massive Vernetzung der persönlichen und personenbezogenen Daten. Während es heute eben viele kleinere, begrenzte, bis nicht vernetzte Systeme gibt, so ist mittels der ID-Austria der Zugriff auf alle in diesen Systemen gespeicherten Daten möglich. Ein solcher Zugriff soll zumindest EU-weit und, im Fall entsprechender Abkommen, auch darüber hinaus möglich sein.

In diesem Zusammenhang steht natürlich auch, dass Cyberkriminelle sowohl im zentralen System der ID-Austria/eID als auch bei mit ID-Austria/eID vernetzten Systemen viel mehr und größere Möglichkeiten erhalten, Schaden anzurichten und/oder die persönlichen Daten abzusaugen und zu missbrauchen. Schon jetzt finden laufend Einbrüche in einzelne Datensysteme von Bund, Gemeinden, Behörden, Unternehmen etc. statt, die immer wieder erheblichen Stillstand, Aufwand und gestohlene Daten bewirken. Die Abwehrmechanismen können gar nicht so schnell entwickelt werden, wie Cyberkriminelle Einbruchsvarianten finden.

Willigt ein Nutzer bei einem Service-Provider der ID-Austria/eID ein, können Transaktionen auch mit Daten aus behördlichen Registern (wie z. B. Staatsbürgerschaft, Adress- und Meldedaten, Führerschein, Firmenbuch oder weitere Register) angereichert werden!
Dies eröffnet ein hohes Potential unerwünschter Nutzung persönlicher Daten, (permanenter) Überwachung, Kontrolle oder gar Einschränkung der persönlichen Freiheiten und Fremdbestimmung, nicht nur von Behörden, sondern auch von privaten Unternehmen oder Personen. Als ein stellvertretendes Beispiel für viele zu nennen wären Zugriff-Beschränkungen oder gar Sperren für die Nutzung von Internet und Social Media. Die aktuell geplanten Alterskontrollen für den Zugriff auf bestimmte Webseiten stellen dafür einen Einstieg dar.

Letztendlich besteht die Gefahr, mit Hilfe der ID-Austria den chinesischen Weg mit einer Art Social-Credit-Score (Sozialpunktesystem), also den Weg in einen digitalen Überwachungs- und Kontrollstaat, auch in Österreich zu ebnen.

Zentrale Forderungen für eine positive und menschengerechte Digitalisierung am konkreten Beispiel ID-Austria

1. Wahlfreiheit, ob eine Nutzung der ID-Austria erfolgt (auch kein indirekter Zwang zur Nutzung); Umsetzung der bereits rechtlich festgehaltenen, niederschwelligen, analogen Alternativen
2. Wahlfreiheit der technischen Systeme bei Nutzung der digitalen Dienste;
   kein Smartphone-Zwang oder Zwang zur Nutzung von nicht-europäischen Systemen (Zwänge, direkt oder indirekt, sind ein No-Go).
3. Systeme einer digitalen Identität haben unabhängig vom Gerät und auch unabhängig von den Systemen bestimmter Anbieter zu sein. Zudem haben sie einfach und kostengünstig, idealerweise sogar kostenlos zu sein.
   Solche Systeme haben daher auch mit PCs oder Laptops und auch mit Open-Source-Betriebssystemen nutzbar zu sein.
4. Vermeidung zentralisierter Systeme, Forcierung dezentraler Systeme aus Gründen der Sicherheit, Redundanz, und natürlich des Privatsphäre- und Datenschutzes.

5. 2-Faktor- (2FA) bzw. Multi-Faktor-Authentifizierung (MFA) sind in der heutigen Zeit besonders bei sensiblen Inhalten technisch sinnvolle Lösungen.
   Deren Implementierung ist sowohl mit verschiedenen, technischen Systemen möglich, als auch in dezentrale Plattformen.
   Und auch hier gilt, dass es weder Anbieter- noch Geräte- noch Systemzwang geben darf, sondern Technologie-Offenheit zu geben hat und die Möglichkeit, Open-Source-Systeme zu nutzen. Denn eID-freie 2FA/MFA-Systeme sind machbar!

Dieser Antrag entstand aufgrund von Informationen und im Zusammenwirken einer Reihe von interessierten Personen, politisch tätiger Gruppierungen und Organisationen. ■

Angenommen ☐	Zuweisung ☐	Ablehnung ☐	Einstimmig ☐	Mehrheitlich ☐