Aspekte der zentralisierten E-ID in Österreich (ID Austria)

24. Jänner 2025

Worum es in diesem Dokument geht:

In diesem Dokument geht es nicht um die 2-Faktor-Authentifizierung, die bei der ID Austria eingesetzt und in vielen Systemen Standard ist. Es geht um die Zentralisierung der E-ID, die viele Risiken birgt und deshalb nie aufgezwungen werden darf, aber wird. Hier werden Aspekte genannt, derer man sich bewusst sein sollte.

Verwiesen wird auch auf die Ausarbeitungen von epicenter.works, die Datenschutzfolgeabschätzung (DSFA) des Research Institute – Digitial Human Rights Center, und des Grünen Vereins für Grundrechte und Informationsfreiheit (GGI); Links dazu nachfolgend im Dokument.

Inhalt:

Die ID Austria „ist ja nur ein Schlüssel“

Vorweg eine Klarstellung zur Aussage, dass die ID Austria ja nur ein Schlüssel sei, wie mancherorts propagiert wird:

Dass die ID Austria "nur ein Schlüssel" ist, stimmt in gewisser Weise. Aber eben ein besonderer Schlüssel, der letztlich viele Türen, Tresore, Berechtigungen zugänglich macht, und der, wenn er in falsche Hände kommt, entsprechend viel Schaden anrichtet. Besonders bei diesem Schlüssel ist auch, dass sich mehrere zentrale Stellen in jedes dieser Schlösser hineinsetzen: IT-Unternehmen wie Google & Co. und US-Behörden schauen immer mit; weltweite Infrastruktur muss immer funktionieren, damit man mit dem elektronischen Schlüssel aufsperren kann; das jeweils verantwortliche Ministerium schaut immer mit und kann zentral steuern, ob der Schlüssel überhaupt sperrt oder nicht - mit entsprechenden Möglichkeiten, wie der verfügten Einschränkung von Grundrechten bis hin zu staatlichem Missbrauch. Dies führt in all den Lebensbereichen, in denen die ID Austria zwingend vorgeschrieben wird, zu einer Abhängigkeit von wenigen staatlichen Organen und privaten Konzernen. Die meisten der vielfältigen Daten in verschiedensten Systemen

selbst sind zwar nicht an zentraler Stelle gespeichert, aber alle Daten sind mit der selben Schlüsselnummer verbunden (vorerst noch bereichsspezifisch) und somit genügt ein gesetzlicher Auftrag oder ein Hackerangriff auf diese Daten, um alle Daten miteinander zu verbinden und den gläsernen Menschen zu perfektionieren.

Irreführende Aussagen von Anfang an – Aussagen demnach nicht vertrauenswürdig

Die Vorbereitung und Einführung der ID Austria war von vielen mutmaßlich bewusst irreführenden Aussagen begleitet.

Zuständige ÖVP-Minister und –Staatssekretäre betonten öffentlich immer die garantiert freiwillige Nutzung, setzten jedoch den vielfachen Zwang vom ersten Tag an um. (https://ggi-initiative.at/wp/id-austria-versprechen-und-realitaet/)

Die DSFA verlangt: „So sind allfällige Tendenzen eines potenziellen gesellschaftlichen Ausschlusses oder einer möglichen Ungleichbehandlung als Folge des Technologieeinsatzes kritisch zu beobachten und durch entsprechende Maßnahmen zu adressieren. Dabei geht es insb um Konsequenzen für jene Personen bzw Bevölkerungsgruppen, welche die E-ID aus verschiedenen Gründen nicht verwenden möchten oder können.“. (https://researchinstitute.at/veroeffentlichung-des-berichts-zur-id-austria-datenschutz-folgenabschaetzung/)
Seitens der Regierung wird suggeriert, der DSFA und somit auch diesem Passus entsprochen zu haben, was offenkundig falsch ist.

Auch verspricht das Gesetz einen gewissen Schutz gegen Missbrauch in Gestalt der Datenschutzbeauftragten. Dieses Versprechen scheint ebenfalls wenig Substanz zu haben, wenn man an ein Ereignis in Deutschland denkt. Die faktische Abhängigkeit des Datenschutzes von einzelnen Personen, die in der Theorie unabhängig und in der Praxis der Gefahr politischer Sanktionen und Einflussnahme ausgesetzt sind: (OFFENER BRIEF – Protest gegen die Beschädigung des Amtes des/der Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI))

Nutzen für Bürger geringer als für andere – daher wird künstlich durch Druck motiviert

Wäre die Gesamtbilanz für die einzelnen Bürger und Inhaber der ID Austria eindeutig positiv, würde die Nutzung automatisch zunehmen. Druck, um mehr Menschen zur Nutzung zu bewegen, deutet einerseits auf das Fehlen überzeugender Argumente hin und andererseits darauf, dass die wahren Nutznießer andere sind. Das Pseudoargument, wonach die Bevölkerung tendenziell aus unmündigen Menschen besteht, die von der Regierung und Behörden angewiesen und zu ihrem Glück gezwungen werden müssen, lassen wir nicht gelten – da es doch letztlich von Teilen derselben Bevölkerung kommt und sich somit selbst entkräftigt.

Der Druck ist ganz offensichtlich massiv:

- Bereits im ersten Jahr der Einführung wurde vielen Berufsgruppen, Vereinen oder Privatpersonen der Zugang und das Recht auf finanzielle Mittel oder auch Sozialleistungen nur mehr über ID Austria gewährt – was oftmals einem Zwang gleichkam;
- Für Steuerberater und Unternehmer wurde die ID Austria zum Teil Bedingung für die Berufsausübung;
- Für Lehrer und Kindergärtner wurden Schikanen bei der Lohnverrechnung geschaffen und die ID Austria für administrative Dateneinsicht und Eintragungen verpflichtend;
- In manchen Bereichen mussten gewisse Prozentzahlen an Anträgen mit ID Austria eingereicht werden, auch wenn dadurch Bürgern unter Vorspiegelung falscher Tatsachen ihr Recht auf einen analogen Antrag verweigert wurde.
- Details zu diesen Beispielen siehe: https://ggi-initiative.at/wp/id-austria-versprechen-und-realitaet/ sowie https://epicenter.works/content/id-austria-zwang

Der „Grüne Pass“ der Corona-Zeit wurde ausdrücklich positiv als „Hebel“ und „Selbstläufer“ in dem Sinn, dass man zu einer E-ID gezwungen wird, betrachtet. Aber auch der digitale Schülerausweis ist bereits als faktisch alternativlose Variante für Schüler – und damit als weiteres Druckmittel in Vorbereitung. (https://ggi-initiative.at/wp/id-austria-moegliche-folgen-fuer-nichtanwender/)

Wie auch schon im ersten Jahr der ID Austria Einführung als manche Angestellte mit Jobverlust bedroht wurden, wenn sie keine persönliche ID Austria wollten, werden nun aktuell auch Lehrkräfte mit Jobverlust bedroht: ab 1. März 2025 soll die ID Austria für Lehrende in Höheren Schulen „verpflichtend“ gelten. Die ID Austria wird von der Bildungsdirektion als „alternativlos“ und als „Dienstpflicht“ bezeichnet, was beides falsch ist.

Der offenkundige faktische Zwang und die privaten Risiken, die er mit sich bringt, werden aktuell vom Direktor der Bundeshandelsakademie, Mag. Jörg Hopfgartner, in einem Werbevideo zur ID Austria in die Worte verpackt: "Mit Neugier den Mehrwert für sich selbst nutzen; dann ist die ID Austria bald eine Selbstverständlichkeit" (https://ida.bhakwien10.at/)

Kein sicherer Schutz vor Datenzusammenführung

Persönliche Daten werden heute bereits bereichsspezifisch und *getrennt* voneinander gespeichert.

Dieses Konzept des **bereichsspezifischen Personenkennzeichens** ist Teil der ID Austria. Entsprechend werden die persönlichen Daten, die z.B. im Gesundheitsbereich gespeichert sind, nicht mit denen im Bildungsbereich oder im Wirtschaftsbereich verbunden. Aber: diese Trennung ist nicht technisch abgesichert und eine Verbindung der Daten kann durch Gesetzesänderung jederzeit umgesetzt werden.

Dieses Konzept ist zwar auch für den privaten Sektor angedacht, also sinngemäß je Firma ein Bereich, jedoch lassen die Formulierungen hier Spielraum und stellen somit die sinngemäße Umsetzung nicht sicher.

Bei der angestrebten europäischen E-ID ist von Haus aus kein solches Konzept mehr angedacht – soweit bekannt.

Daher besteht der Schutz vor Zusammenführung aktuell nur in Gesetzestexten und nur dann, wenn sie vom betroffenen IT-Personal sorgfältig und sinngemäß umgesetzt werden. IT-Personal mit enger Bindung an den Dienstgeber, den Staat, das Land, die Bevölkerung, mit daraus erwachsendem Verantwortungsgefühl ist dafür eine Mindestvoraussetzung. Die großen Rechenzentren des Bundes oder auch von Kommunen wie Wien können dies jedoch wegen massiver Personalauslagerung immer weniger bieten. Ausgelagertes Personal wechselt häufig, lebt zum Teil im Ausland, hat oftmals weniger Bindung zum Staat oder zur Bevölkerung, wird wegen Personalnotstand selten kontrolliert, bleibt der Personalleasingfirma oder dem IT-Konzern verpflichtet, manchmal mehr als dem öffentlichen Dienstgeber. Auch werben IT-Konzerne bei der zuständigen Politik immer wieder massiv für eine vollständige Auslagerung – und damit verbunden für ein Ende jeder engen Bindung und eine faktische Datenhoheit für (ausländische) Konzerne, die wiederum nur durch vertragliche Regelungen eingeschränkt wird, welche aber geduldig sind.

Keine Krisentauglichkeit

Die Politik warnt regelmäßig vor Gefahren, auf die man vorbereitet sein sollte: Stromausfälle und Shutdowns, Hackerangriffe, Schädigung von Infrastruktur durch terroristische oder militärische Angriffe. Auch wurde schon vor ungünstigen Entwicklungen in Folge geänderter US-Politik und damit zusammenhängender US-Konzernpolitik gewarnt.

Die ID Austria selbst jedoch bietet in all diesen Fällen keine Lösung und wäre in solchen Fällen völlig unbrauchbar – mit potentiellem Schaden für zwingend davon abhängige Menschen.

Keine Barrierefreiheit

Barrierefreiheit hat in der Verwaltung hohen Stellenwert. Oftmals wird sehr viel Geld investiert, wenn auch nur eine Hand voll Menschen profitieren könnte und ein Amtsweg, eine Handlung, ein Weg erleichtert wird. Die EU-weiten Vorschriften werden immer strenger, aktuell auch innerhalb der Verwaltung.

Die verpflichtende Nutzung der ID Austria kommt dem künstlichen Schaffen einer Barriere gleich für nicht-IT-affine Menschen, für Menschen, die sich beim Umgang mit Smartphones grundsätzlich schwer tun, für Menschen, die (noch) nicht dazu bereit sind, für Menschen, die keinen persönlichen Vorteil erkennen können, wie auch für Menschen, die gerade angesichts der wirtschaftlichen Auswirkungen der Corona- und Energiepolitik keine weiteren Fixkosten tragen können. Sie fördert eine 2-Klassen-Gesellschaft.

Keine wirtschaftliche Unabhängigkeit mehr von ausländischen Firmen

… und damit einhergehend keine wirtschaftliche Wahlfreiheit mehr, sondern gesetzlich vorgeschriebener Konsum, sofern die Nutzung verpflichtend ist. Vorgegeben sind bestimmte Android- oder iOS-Versionen für Smartphones, bestimmte Ausstattungsmerkmale der Smartphones, bestimmte Fido-Token, und damit einhergehend die Notwendigkeit zur Erneuerung, je nach

aktueller Marktstrategie der gewinnorientierten Hersteller. (https://www.oesterreich.gv.at/app-digitales-amt/faq/app_digitales_amt.html#system)

Weniger Datenschutz durch neue Anreize zum Missbrauch

Über eine zentralisierte E-ID wie der ID Austria, deren Nutzung als alternativlos dargestellt wird, und durch die Abhängigkeit von US-Konzernen wurden künstlich Anreize zum Missbrauch geschaffen. Zum viel gepriesenen Nutzen für das eigene Leben kommen sehr zweifelhafte Nutznießer, die man sich damit einhandelt:

Mit dem E-ID System wird erstmals eine Möglichkeit eröffnet, hoheitlich qualifizierte personenbezogene Daten niederschwellig digital an Dritte, insbesondere Private, weiterzugeben. Dies kann auch bewusst von den Daten empfangenden Dritten sogar herbeigeführt werden, denn diese haben einen Anreiz, an die über das E-ID System bereitgestellten hochqualitativen Daten heranzukommen. (laut Datenschutzfolgenabschätzung, siehe https://ggi-initiative.at/wp/id-austria-neues-risiko-fuer-datenmissbrauch/)

Google und Apple, bei denen man sich entsprechende Konten/Accounts anlegen bzw. mit ihnen kontrahieren muss. Über die Nutzung deren App Stores kann es zu einer Datenverarbeitung zu inkompatiblen Zwecken, wie etwa die Verwendung für Werbezwecke, kommen, da eine derartige Verwendung personenbezogener Daten als ein zentraler Bestandteil der Geschäftsmodelle dieser Unternehmen gilt. (laut Datenschutzfolgenabschätzung, siehe https://ggi-initiative.at/wp/id-austria-die-abhaengigkeit-von-google-co/)

Aufgrund des notwendigen transatlantischen Datentransfers wird US-Sicherheitsbehörden der Zugriff ermöglicht.

Letztlich ist dieses zentralisierte System besonders dann, wenn eine verpflichtende Nutzung besteht, auch für einen Staat, der seine Hauptaufgabe nicht mehr in der Wahrung der Grundrechte sieht, von zweifelhaftem Nutzen. Er kann damit diskriminierende Praktiken und eine autoritäre Disziplinierung der Bevölkerung leichter umsetzen. In der Literatur ist auch von „Policy Windows“ in Zeiten gesellschaftspolitischer Krisen die Rede, welche die Ausrollung staatlicher ID-Systeme und deren Nutzung zu Überwachungszwecken begünstigen. Heute aktuell ist jedenfalls die zentrale Nachverfolgung aller Anmeldeaktivitäten in allen angebundenen Systemen möglich. Das beschriebene Risiko ist laut Datenschutzfolgenabschätzung (DSFA) des Research Institutes Digitial Human Rights Center realistisch. Sie nennt als Begründung für das Risiko einerseits ein vorsätzliches Handeln politischer Entscheidungsträger*innen, welche die Risiken potentieller Überwachung sehen, aber potentielle Schäden für die Betroffenen billigend in Kauf nehmen, und andererseits ein vorsätzliches Handeln staatlicher Institutionen und Nachrichtendienste, die zum Zweck der Strafverfolgung und Prävention auf das ID Austria System zugreifen. (https://ggi-initiative.at/wp/id-austria-als-machtinstrument-fuer-regierende/)

Keine angemessene Einstellung der Auftraggeber

Eine ID Austria sollte eine Erleichterung für Menschen und gleichzeitig Einsparungen in der Verwaltung bringen. Jeder Mensch sollte dort, wo es für ihn Vorteile bringt, die Möglichkeit der

Nutzung haben. So kann sie ein Vorteil für alle Beteiligten werden. Alles darüber Hinausgehende ist vielleicht gut gemeint, aber nicht mehr gut.

Die erzwungene Verwendung und damit das erzwungene Eingehen eines persönlichen Risikos, steht dem Staat und staatsnahen Organisationen nicht zu und deutet auf eine Grundhaltung hin, die im öffentlichen Dienst keinen Platz zu haben hat.

Die Entscheidung von Menschen, die aufgrund rationaler Überlegungen eine zentrale E-ID (ID Austria) nicht möchten, aber auch von Menschen, die sich überrumpelt fühlen und nicht bereit dazu sind, sind zu respektieren!

Die Grundaussagen von Gesetzen müssen jedenfalls sinngemäß interpretiert werden. Eine juristische Anregung diesbezüglich: „*Es gilt Artikel 8 EMRK (Europäische Menschenrechtskonvention) , ganz besonders bezüglich sensibler Daten. Ein Grundrecht ist ein Grundrecht ist ein Grundrecht. Jemand muss daher nicht begründen, warum er oder sie jede Gefahr für ein Grundrecht NICHT will. Die anderen müssen begründen, warum eine potenzielle Grundrechts-gefährdende Regelung ohne Alternative - also zwingend - notwendig ist …*“

Auch wenn das private Risiko, das bei einer Verpflichtung zur ID Austria entsteht, alternativlos ist, ist die ID Austria selbst nicht alternativlos. Weder im privaten Kontakt mit Behörden und staatsnahen Organisationen, wo der analoge Zugang leicht umgesetzt werden kann, noch innerhalb von Organisationen wie im Bildungsbereich oder Landesregierungen, wo es nur um eine 2-Faktor-Anmeldung geht, die auch ohne zentralisierte ID realisiert werden kann.

Kurzer technischer Hintergrund, wie die ID Austria konkret funktioniert

Zur Frage, ob ein Token alleine nicht besser wäre, oder ob alle Daten im Hintergrund bereits jetzt an einer Stelle gespeichert werden:

Am Beispiel des in Schulen verwendeten Systems „Sokrates“: Bei einem System wie Sokrates sind bestimmte User berechtigt, damit zu arbeiten. Die Daten des Users sind in einer Datenbank gespeichert und pro User kann z.B. dokumentiert werden, was er alles macht, wann er sich eingeloggt hat, …. Dies erfolgt im System, hier im Beispiel in Sokrates.

Wenn die ID Austria in das System integriert wird, dann werden die Daten des Users mit einem zentralen Schlüssel verbunden bzw. der Schlüssel, also das bereichsspezifische Personenkennzeichen (bPK), wird ebenfalls in dieser Datenbank gespeichert. Letztlich, in einigen Jahren, wenn die ID Austria in sehr viele Systeme integriert wurde und die Anwender zur Nutzung gezwungen wurden, würde dies dazu führen, dass dieses bPK in **allen** Systemen, wo man sich mit ID Austria anmeldet, beim den Daten des Users in der betreffenden Datenbank mitgespeichert wird. Dadurch können die Daten leichter verbunden werden - man braucht nur Zugang zu diesen Datenbanken, sei es per gesetzlichem Auftrag, durch Gesetzesänderung, oder durch Hackerangriff bzw. auf kriminellem Weg. Das ist ohne ID Austria bzw. ohne bPK schwieriger.

Die Anmeldung in einem System erfolgte bisher mit dem spezifischen User. Die Anmeldung konnte nur mit Passwort (wie es bei Sokrates ist) oder zusätzlich mit SMS, Handy-App oder Token erfolgen (2. Faktor, und damit 2 Faktor Authentifizierung). Das Token ist also nicht in der

Datenbank gespeichert, sondern die Daten des Users sind gespeichert und die Rechte, die er in z.B. Sokrates hat. Das Token ist ein Gerät, das man besitzen muss, analog zum Handy, um sich authentifizieren zu können.

Bei der ID Austria gibt es zusätzlich eine zentrale Datenbank, wo wieder die Stammdaten des Users, wie Name oder Geburtsdatum, und eine Stammzahl pro Person gespeichert sind. In diesem Fall meldet man sich zuerst bei ID Austria an, wieder mit den klassischen Methoden, derzeit mit 2-Faktor. Dabei gibt es wieder die Variante Handy-App oder Token. Letztlich wird damit der zentrale User identifiziert. Danach schickt das ID Austria-System die Daten der Person, also vor allem das bPK, an das ursprüngliche System, also z.B. Sokrates. Dort können mit Hilfe der bPK die Daten des Users in der Datenbank gefunden werden und man bekommt den Zugang zu Sokrates mit den jeweils individuellen Rechten, wie auch schon bisher.

Neu ist deshalb bei einer Integration der ID Austria auch, dass jeder Anmeldevorgang über eine zentrale Stelle laufen muss, was alle Handlungen vom Funktionieren dieser Stelle abhängig macht, was dieser Stelle die Möglichkeit gibt, alle Anmeldeaktivitäten in allen betroffenen Systemen aufzuzeichnen, und was diese Stelle ermächtigt, zentral in alle Anmeldevorgänge einzugreifen – und sie bei Bedarf auch zu verhindern.