

## **E-Government-Gesetz, Passgesetz, Änderung (56/ME)**

Stellungnahme zum Ministerialentwurf betreffend Bundesgesetz, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden wird.

Herbert Unger – 7000 Eisenstadt  
Zertifizierter Datenschutzbeauftragter und FPÖ Gemeinderat

Eingebracht unter:

[post.i2\\_19@bmdw.gv.at](mailto:post.i2_19@bmdw.gv.at) und [begutachtungsverfahren@parlament.gv.at](mailto:begutachtungsverfahren@parlament.gv.at)

Sg. Damen und Herren im Parlament und im BMDW !

Ich übermittle Ihnen hiermit meine Stellungnahme zum Ministerialentwurf und ersuche um Kenntnisnahme und Berücksichtigung meiner Bedenken sowie um Einarbeitung meiner Verbesserungsvorschläge.

**Der Elektronischen Identitätsnachweis (E-ID) und Anwendungen wie die digitale Immunitätskarte mit der Restart.ID App oder ELGA mit dem neuen Zwangsregister eImpfpass (digitales Impfreister) in Verbindung mit dem Reisepass stellen neue Herausforderungen dar. Sowohl der Staat, die Dienstleister aber vor allem die Bürger sind hier gefordert. Es gilt „Wachsam“ zu sein. Denn auf die Datenwächter (vormals die Grünen), den Datenschutzrat und die Bundesregierung ist kein Verlass mehr wenn es um die staatlichen personenbezogenen Daten der Österreicher geht. Einzig die FPÖ steht hier als Kontrollpartei im Parlament, Land und in den Gemeinden auf der Seite der Bürger. Alles dreht sich um BigData mit personenbezogenen Bürgerdaten aus den staatlichen Registern. Die Drehscheibe dazu ist das Bundesrechenzentrum (BRZ).**

Begutachtungsverfahren läuft im Parlament

In der Covid-19 Krise werden immer weitere neue Überwachungsmaßnahmen durch die **#övpgrüninnenregierung** über den Weg der schnellen Krisen-Gesetzesschaffung durch das Parlament geschleust. Niemand kann diese Vorgänge stoppen. Nicht einmal der SPÖ/FPÖ Verbund im Bundesrat. Der Bundesrat kann nur verzögern. Denn bei Einwänden des Bundesrates folgt sofort ein Beharrungsbeschluss der **#övpgrüninnenregierung** und das Gesetz ist in Kraft. So läuft das aktuell im Parlament. Wer die ÖVP mit Macht ausstattet, muss mit so etwas rechnen.

### **Zum digitalen Überwachungsstaat „Made in Austria“**

Alles soll auf unseren Handys landen und es soll über vereinfachte smartphonebasierte Anwendungen (ID-Apps, Covid-Apps) mit der neuen europaweiten Verwendung des **E-ID (Elektronischen Identitätsnachweis)** funktionieren. Die Drehscheibe dazu ist das BRZ und ihre externen Dienstleister. Mit Anwendungen wie der digitalen Immunitätskarte und der „**Restart.ID App**“ der Firma **younix Identity AG** (ein Unternehmen der Staatsdruckerei) werden die Österreicher in den digitalen Überwachungsstaat geführt. Hinweis: Die **Staatsdruckerei** ist kein staatliches

Unternehmen mehr sondern ein privater Dienstleister mit einer hohen Dichte an staatlichen Aufträgen die uns Bürger direkt betreffen. An der Spitze der Dienstleistungen der Staatsdruckerei steht der **Reisepass** und der **Personalausweis** welche zukünftig mit der E-ID und weiteren staatlichen personenbezogenen Bürgerregistern digital verknüpft werden sollen.

## Digitalisierung gesteuert und geplant über die Gremien in der EU

Begründet wird diese überwachte Digitalisierung mit der Steigerung der Datenqualität und Ausweitung der Nutzungsmöglichkeiten der **E-ID in Österreich** und natürlich in ganz Europa. Weltweit läuft das Projekt unter der Bezeichnung **ID2020**. Die Bluetooth Schnittstellen auf unseren Handys wurden bereits durch die Weltkonzerne Apple und Google aktiviert und funktionieren jetzt sogar ohne Apps.

### Wozu das alles?

**Gesicherte Identitätsfeststellung durch Behörden und ordentliche Gerichte (praktisch in der Covid-Krise) Wer ist wann wo mit wem und ist er ein Covid-Verdachtsfall, Infizierter, unter Quarantäne, Geheilte, Kranker oder Geimpfte?**

Die Optimierung der Verwendung vorhandener Daten für die Beantragung von Reisedokumenten steht dabei ebenfalls auf dem Plan. **Im Jahr 2020 läuft jeder sechste österreichische Reisepass ab.**

#### Hinweise:

- Sie benötigen ein **färbiges EU-Passbild nach den geltenden ICAO Vorschriften**. Informationen erhalten Sie unter [www.bmi.gv.at/passbild](http://www.bmi.gv.at/passbild) oder bei jeder **Passbehörde**.
- **Bitte beachten** Sie, dass aus Platzgründen im Reisepass für Familiennamen und akademische Grade (vor-/nachgestellt) insgesamt 2 Zeilen mit jeweils 33 Zeichen zur Verfügung stehen und dass die Zeile für die Vornamen mit 20 Zeichen begrenzt ist. Bitte füllen Sie daher die im Antragsformular dafür vorgesehenen Felder entsprechend aus, da sonst überlange Namen entweder abgekürzt werden oder ein Name entfallen muss.
- **Zu den Nachweisen:** bei Vorlage eines im Inland ausgestellten Reisepasses sind nur die abweichenden Angaben entsprechend nachzuweisen.
- Reiseinformationen erhalten Sie unter [www.aussenministerium.at](http://www.aussenministerium.at) und den Telefonnummern nat.: 0 50 11 50-3775 Int.: (+43-1) 90 115-3775.

### Antrag auf Ausstellung eines österreichischen Reisepasses

Ich beantrage die Ausstellung eines Reisepasses mit folgenden Daten

akademischer Grad/Standesbezeichnung Ingenieur und Name	
Name	
Familienname zur Zeit der Geburt	frühere Namen
Vorname(n)	besondere Kennzeichen

[www.oesterreich.gv.at](http://www.oesterreich.gv.at)

In der Zukunft unserer Kinder und Enkelkinder wird es kein Reisen, keinen Lokalbesuch und keinen Veranstaltungsbesuch ohne digitale Ausweisung und Überwachung geben. Der digitale Gesundheitsstatus wird wohl bald auch auf den Arbeitsplatz Einfluss nehmen. Home-Office, Kurzarbeit oder Kündigung mit Arbeitslosigkeit hängen am digitalen Personenstatus. Dies betrifft auch unsere Kinder vom Kindergarten, Schule, Internat, Matura bis zum Universitätsabschluss oder Lehrabschluss. Viele Bürger werden sich der digitalen Überwachung beugen, denn die Ausbildung, der Job und das „Überleben“ der Familie wird davon abhängen.

### Ausweitung Datenzugriff auf personenbezogene Staatsregister der Bürger?

Die Zulässigkeit der Verwendung von Attributen aus dem **Identitätsdokumentenregister** sowie aus Registern von Verantwortlichen des

privaten Bereichs über das System des E-ID und Bereitstellung dieser Daten an Dritte soll eingeführt werden. Da sollten bei jedem Bürger und Datenschützer die Alarmglocken läuten. Das **digitalisierte Foto der Bürger** (bereits jetzt in jedem Reisepass digital abgespeichert) soll zur eindeutigen zukünftigen Identifizierung der betroffenen Bürger dienen. Im Zuge der Registrierung zum E-ID (sofern nicht bereits vorhanden) ist zukünftig ein digitales Lichtbild durch die Bürger beizubringen.



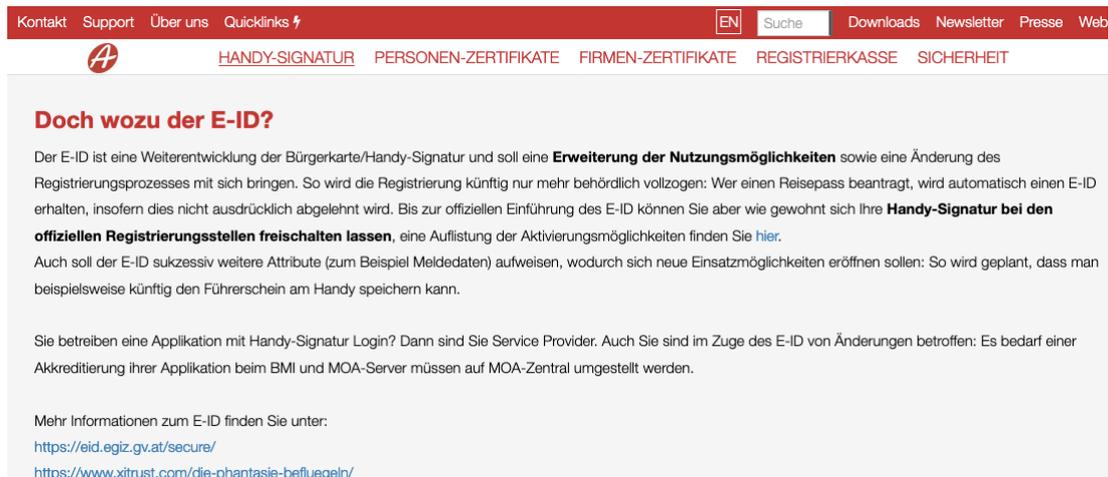
[pixabay.com](https://pixabay.com)

Dazu sollte auch die aktuelle Entwicklung in der digitalen **Gesichtserkennung** beobachtet werden. Dieses Projekt wurde aktuell im BMI unter Federführung eines externen Dienstleisters (ATOS) in den Echtbetrieb gesetzt. ATOS ist auch einer der Top-Dienstleister im Bundesrechenzentrum (BRZ) und stellt mit einem Ex-Mitarbeiter den Digitalisierungskommissar der EU. Die Firma RUBICON hat zwischenzeitlich einen 70 Millionenauftrag für das BMI an Land gezogen. Dabei geht es um das System „**Acta Nova**“ das neue polizeiliche Informations- und Workflowsystem des Innenministeriums. Somit ist klar, dass nicht der Staat, sondern externe Dienstleister und Firmen ihre Finger an der Tastatur zu den Computern, Großrechnern und Servern in den Rechenzentren haben. Zum Thema – **sind unsere Bürgerdaten im Staat sicher** – wird aktuell die **Operation „Edelstein“** mit Verwicklungen zum BRZ, Staat, Ministerien und zur Post im Ibiza-Untersuchungsausschuss behandelt und durchleuchtet.

### **Das staatliche Ergänzungsregister spielt eine zentrale Rolle**

Zur Kenntnis gelangte Änderungen zu Eintragungsdaten im Ergänzungsregister sollen von bestimmten Behörden und Verantwortlichen des öffentlichen Bereichs direkt dem Ergänzungsregister gemeldet werden. Wir wissen noch nicht welche Behörden und Dienstleister auf diese personenbezogenen Staatsdaten von 8 Millionen Österreichern – verteilt auf über 50 Datenregister – Zugriff haben werden. Es werden Ermächtigung von Behörden und ordentlichen Gerichten zur **Abfrage des Identitätsdokumentenregisters** zum Zwecke einfacher, rascher und gesicherter Identitätsfeststellung angeordnet werden. Es wird die Weiterverwendung von Daten, die im Zuge der Registrierung eines E-ID oder der Aufnahme eines Lichtbilds für die e-card verarbeitet wurden, für die Ausstellung von Reisedokumenten ermöglicht. Viele Fragen gilt es dazu noch zu klären. Spannend zu diesem Begutachtungsverfahren im Parlament wird auch die Stellungnahme der Datenschutzbehörde sein. Die

Datenschutzbehörde hat ja bereits beim eImpfpass Einwände erhoben, welche die Bundesregierung wenig interessieren.



Kontakt Support Über uns Quicklinks ↗

EN Suche Downloads Newsletter Presse Web

**A** HANDY-SIGNATUR PERSONEN-ZERTIFIKATE FIRMEN-ZERTIFIKATE REGISTRIERKASSE SICHERHEIT

### Doch wozu der E-ID?

Der E-ID ist eine Weiterentwicklung der Bürgerkarte/Handy-Signatur und soll eine **Erweiterung der Nutzungsmöglichkeiten** sowie eine Änderung des Registrierungsprozesses mit sich bringen. So wird die Registrierung künftig nur mehr behördlich vollzogen: Wer einen Reisepass beantragt, wird automatisch einen E-ID erhalten, insofern dies nicht ausdrücklich abgelehnt wird. Bis zur offiziellen Einführung des E-ID können Sie aber wie gewohnt sich Ihre **Handy-Signatur bei den offiziellen Registrierungsstellen freischalten lassen**, eine Auflistung der Aktivierungsmöglichkeiten finden Sie [hier](#).

Auch soll der E-ID sukzessiv weitere Attribute (zum Beispiel Meldedaten) aufweisen, wodurch sich neue Einsatzmöglichkeiten eröffnen sollen: So wird geplant, dass man beispielsweise künftig den Führerschein am Handy speichern kann.

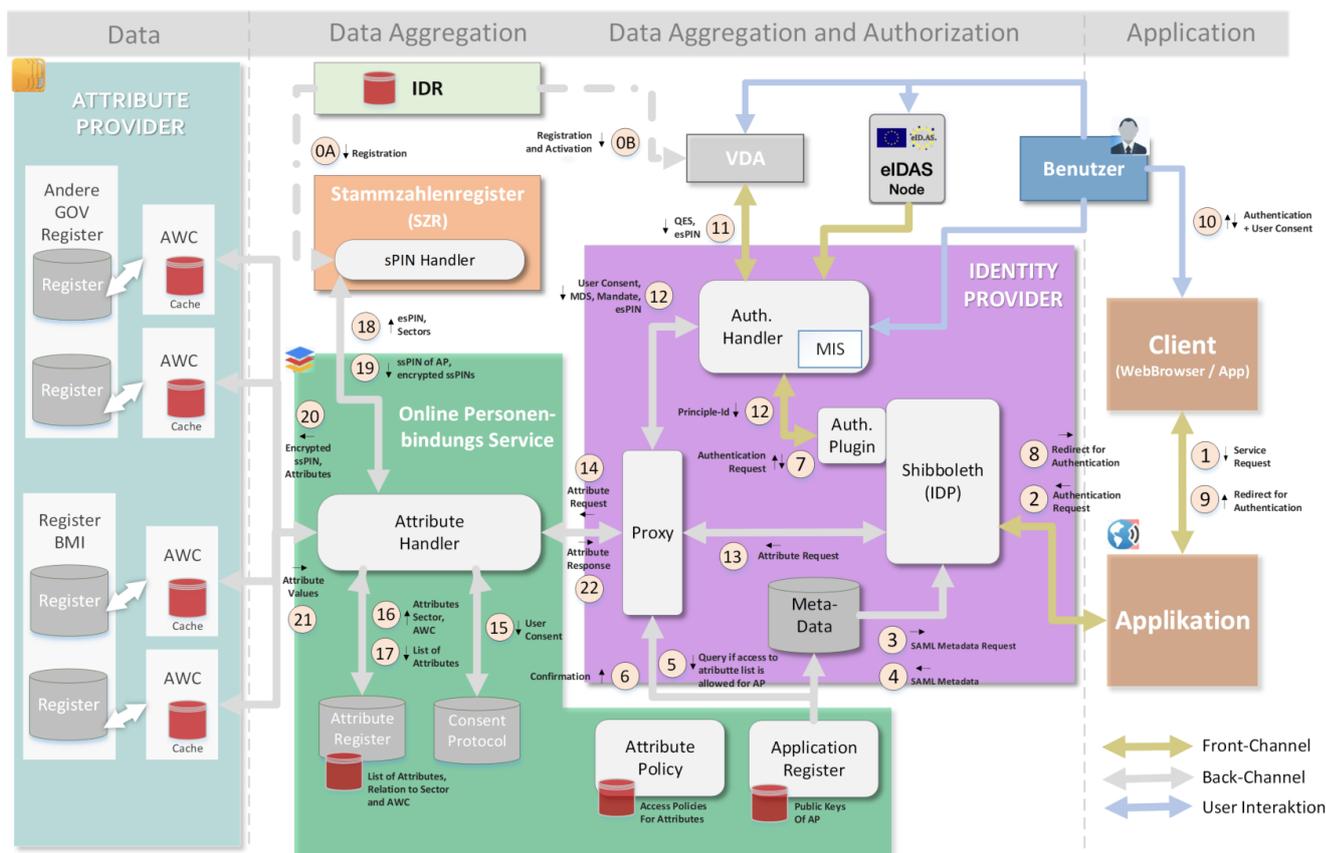
Sie betreiben eine Applikation mit Handy-Signatur Login? Dann sind Sie Service Provider. Auch Sie sind im Zuge des E-ID von Änderungen betroffen: Es bedarf einer Akkreditierung ihrer Applikation beim BMI und MOA-Server müssen auf MOA-Zentral umgestellt werden.

Mehr Informationen zum E-ID finden Sie unter:  
<https://eid.egiz.gv.at/secure/>  
<https://www.xitrust.com/die-phantasie-befluegelv/>

## Die personenbezogenen Register werden verknüpft und weiter verarbeitet

Die vorgeschlagenen Änderungen des Passgesetzes ermöglichen zum einen den Nachweis von personenbezogenen Daten mithilfe des E-ID im Bereich des Passwesens, da eine Rechtsgrundlage für die Übermittlung dieser personenbezogenen Daten an die Stammzahlenregisterbehörde geschaffen werden soll, sofern dieser eine gesetzlich übertragene Aufgabe zukommt. Zum anderen sollen die in der Datenverarbeitung bzw. in der zentralen Evidenz bzw. im Identitätsdokumentenregister (IDR), verarbeiteten Daten aus verwaltungsökonomischen Gründen für Zwecke von Verfahren nach dem Passgesetz weiterverarbeitet werden dürfen.

## Wie soll das zukünftig funktionieren mit der E-ID (elektronische Identität) – Die Personenbindung und die qualifizierte Vertrauensdiensteanbieter (VDA)



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

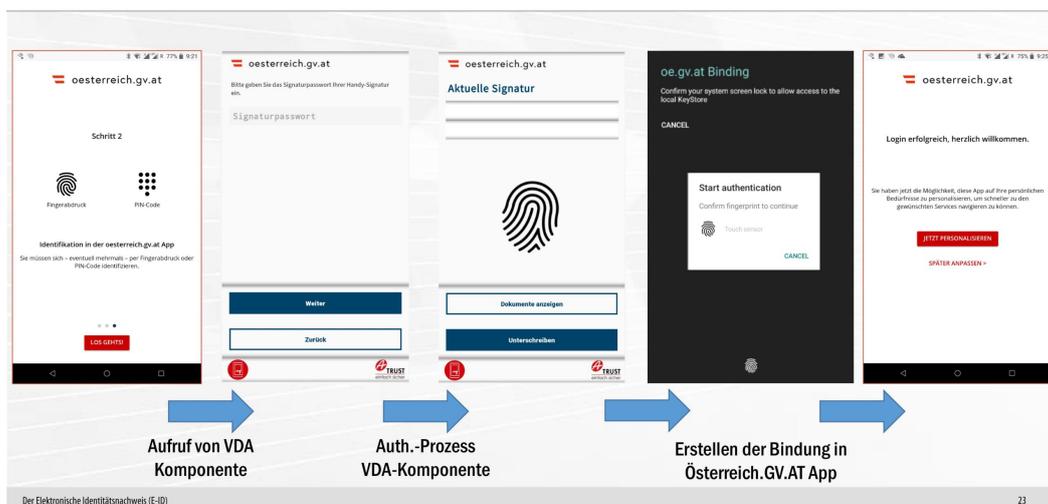
Für Zwecke der Erstellung einer Personenbindung, die bei der Verwendung eines E-ID mittels eines sicherheitstechnisch gleichwertigen Vorgangs, der an eine frühere qualifizierte **elektronische Signatur** des E-ID-Inhabers gebunden ist, ausgelöst wird (§ 2 Z 10a zweiter Fall), ist die **verschlüsselte Stammzahl zum E-ID** dieses E-ID-Inhabers zu speichern. Verwendet der E-ID-Inhaber den E-ID im elektronischen Verkehr gemäß § 10 Abs. 1, ist durch die Stammzahlenregisterbehörde oder die in ihrem Auftrag tätige Behörde eine Personenbindung (Abs. 2), die ein oder mehrere bPK, Vorname, Familienname und Geburtsdatum zum E-ID-Inhaber enthält, zu erstellen, und an die betreffende Datenverarbeitung zu übermitteln. Wird die Erstellung der Personenbindung mittels qualifizierter elektronischer Signatur des E-ID-Inhabers ausgelöst (§ 2 Z 10a erster Fall), hat der **qualifizierte Vertrauensdiensteanbieter (VDA)** die verschlüsselte Stammzahl und die zugehörigen Sicherheitsdaten der Stammzahlenregisterbehörde zur Verfügung zu stellen. Nach Maßgabe der technischen Möglichkeiten können mit Einwilligung des E-ID-Inhabers in die Personenbindung weitere Merkmale zu diesem aus für die Stammzahlenregisterbehörde zugänglichen Registern von Verantwortlichen des öffentlichen oder privaten Bereichs eingefügt werden.“

### Identitätsprüfung der Bürger zur E-ID bei Sicherheits- Personenstands- Staatsbürgerschaftsbehörden und Landespolizeidirektion werden möglich

Die Registrierung des E-ID ist nur zulässig, sofern die Identität des Betroffenen eindeutig festgestellt wurde. In den Fällen des Abs. 1 zweiter Satz und Abs. 2 ist für die Registrierung eines E-ID ein Lichtbild beizubringen, das den Anforderungen gemäß § 4 der Passgesetz-Durchführungsverordnung (PassG-DV), BGBl. II Nr. 223/2006 in der

Fassung der Verordnung BGBl. II Nr. 209/2018 entspricht, sofern der Registrierungsbehörde nicht bereits ein solches vorliegt. Zur **Überprüfung der Identität** und der vorgelegten Dokumente ist die Behörde ermächtigt, Informationen über diese personenbezogenen Daten und Dokumente aus Datenverarbeitungen von Sicherheits-, Personenstands- und Staatsbürgerschaftsbehörden sowie aus Datenverarbeitungen nach den §§ 26 und 27 des BFA-Verfahrensgesetzes (BFA-VG), BGBl. I Nr. 87/2012, im Datenfernverkehr einzuholen. Kann die Identität des E-ID-Werbers bei den Behörden gemäß Abs. 1 und 2 nicht eindeutig festgestellt werden, obliegt das weitere Verfahren zur eindeutigen Feststellung der Identität der Landespolizeidirektion.“

## ÖGV.AT – Single Sign On Bindungsprozess



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

### Welche „Dritte“ Dienstleister, Behörden und Institutionen bekommen Zugriff?

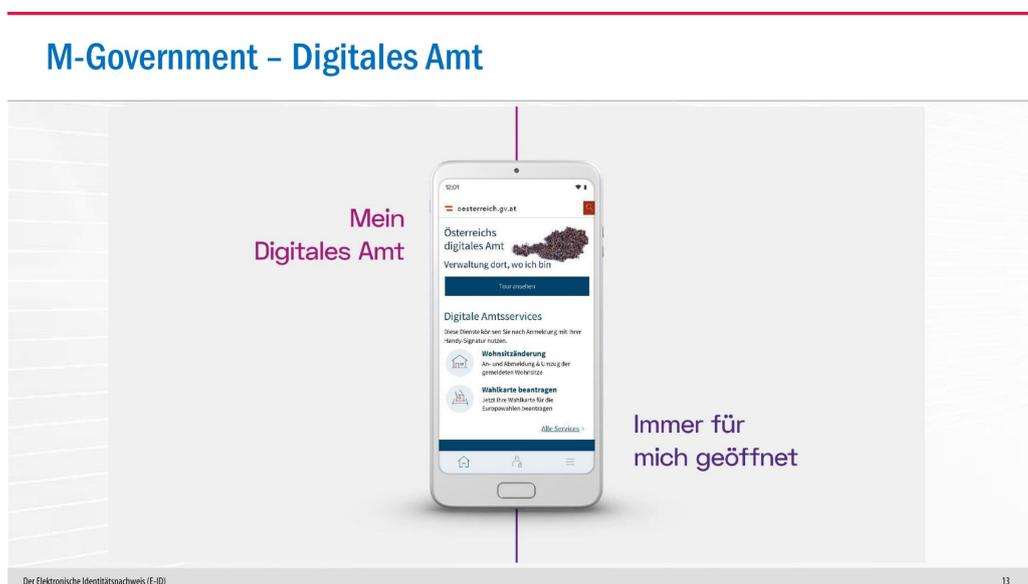
Der Bundesminister für Inneres ist ermächtigt, Dritten nach Abs. 1 Z 2 die Nutzung des E-ID- Systems zu eröffnen. Dritte gemäß Abs. 1 Z 2 haben sich hierfür beim Bundesminister für Inneres zu registrieren. Die Nutzung ist nicht zu eröffnen oder zu unterbinden, wenn Anhaltspunkte dafür bestehen, dass Dritte die ihnen zur Verfügung gestellten personenbezogenen Daten nicht gemäß dem Grundsatz nach Treu und Glauben und auf rechtmäßige Weise verarbeitet haben. Dritte haben dem Bundesminister für Inneres jeden Umstand bekanntzugeben, der dem entgegensteht. Auf Anfrage des Bundesministers für Inneres ist die Datenschutzbehörde ermächtigt, ihm mitzuteilen, ob und über welche Anhaltspunkte sie verfügt, dass der Dritte in den letzten fünf Jahren personenbezogene Daten nicht auf diese Weise verarbeitet hat. Dies gilt nur für jene Anhaltspunkte, die der Datenschutzbehörde in einem rechtskräftig abgeschlossenen Verfahren bekannt geworden sind. Die Nutzung des E-ID-Systems darf im konkreten Fall nur für die glaubhaft gemachten eigenen Zwecke in Anspruch genommen werden; die bloße Weitergabe von im Wege der Nutzung des E-ID ermittelten personenbezogenen Daten an Dritte ist kein eigener Zweck im Sinne dieser Bestimmung.

### Welche Ausnahmen wird es geben – Datenzugriff für Unternehmensserviceportale mit Verordnung BMI und Digitalisierungsministerium?

Der Bundesminister für Inneres ist im Einvernehmen mit dem Bundesminister für Digitalisierung und Wirtschaftsstandort ermächtigt, nähere Bestimmungen über die Vorgangsweise gemäß Abs. 1 und 2 durch Verordnung festzulegen, insbesondere welche Informationen außer dem für die Nutzung des E-ID glaubhaft gemachten Zweck im Zuge der Antragstellung anzugeben sind und inwieweit neben Teilnehmern des Unternehmensserviceportals gemäß § 5 des Unternehmensserviceportalgesetzes (USPG), BGBl. I Nr. 52/2009, auch andere Dritte registriert werden können

### Derzeit noch keine gesetzlichen Voraussetzungen für Echtbetrieb

Mit der Novelle des E-Government-Gesetzes (BGBl. I Nr. 121/2017) Rahmenbedingungen für die Weiterentwicklung des Konzepts Bürgerkarte hin zum E-ID (Elektronischen Identitätsnachweis) kundgemacht. Die Anwendbarkeit dieser Bestimmungen beginnt jedoch gemäß § 24 Abs. 6 E-GovG, idF BGBl. I Nr. 121/2017 erst mit Vorliegen der technischen und organisatorischen Voraussetzungen für den Echtbetrieb des E-ID.



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

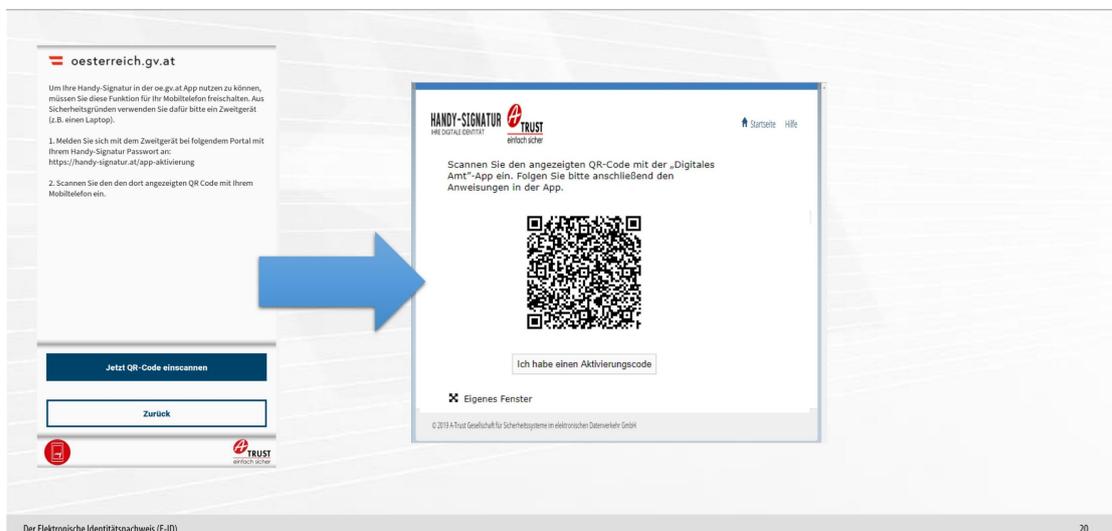
Dieser Zeitpunkt ist vom Bundesminister für Inneres im Bundesgesetzblatt kundzumachen. Dies ist bis dato nicht erfolgt, da die **Voraussetzungen für den Echtbetrieb des E-ID noch nicht vorliegen**. Die Vorarbeiten und Begleitmaßnahmen für den Pilotbetrieb des E-ID gemäß § 25 Abs. 2 E-GovG sowie die Weiterentwicklung der damit verbundenen Technologie bedingen im Vorfeld des Echtbetriebs noch kleinere Adaptierungen und Ergänzungen des rechtlichen Rahmens. So muss beispielsweise für die smartphone-basierte Verwendung des E-ID zusätzlich eine sicherheitstechnisch gleichwertige Umsetzung ausdrücklich ermöglicht werden, um die Nutzung durch den User insbesondere bei Apps zu vereinfachen. Weiters sollen zur Erweiterung der Nutzungsmöglichkeiten des E-ID künftig auch Attribute aus Registern von Verantwortlichen des privaten Bereichs über das System des E-ID (freiwillig und ausschließlich bei Einwilligung des Betroffenen) Dritten zur Verfügung gestellt werden können. Vorerst steht jedoch die Nutzung von Attributen aus Registern von Verantwortlichen des öffentlichen Bereichs weiterhin im Fokus, sodass Register von Verantwortlichen des privaten Bereichs erst in einem nächsten Schritt technisch angebunden werden sollen. Nichtsdestotrotz ist es vor allem aus

verwaltungsökonomischen Gründen ratsam, die **Rechtsgrundlage bereits in dieser Novelle vorzusehen**. Weiters sollen im Zuge der Registrierung des E-ID und bei Änderungen der Eintragsdaten im Ergänzungsregister für natürliche Personen (ERnP) zur Steigerung der Datenqualität auch Anpassungen vorgenommen werden. Schließlich sollen die im Zuge des **Pilotbetriebs** ausgestellten E-ID auch über den Zeitraum des Pilotbetriebs hinaus weiterverwendet und die zugehörigen Registrierungsdaten weiterhin verarbeitet werden dürfen. Schon die bisherige Regelung sah vor, dass es im Rahmen der Nutzung des E-ID dem E-ID-Inhaber möglich sein soll, neben den Kernidentitätsdaten (Vorname, Familienname, Geburtsdatum) weitere Merkmale aus für die Stammzahlenregisterbehörde zugänglichen elektronischen Registern eines Verantwortlichen des öffentlichen Bereichs Dritten (Serviceanbietern) zu Verfügung zu stellen. Zugänglich für die Stammzahlenregisterbehörde bedeutet das faktische Vorhandensein der technischen

### **Bekommen auch Serviceanbieter BigData Zugriff?**

Diese Möglichkeit soll nun auf für die Stammzahlenregisterbehörde zugängliche Register eines Verantwortlichen des privaten Bereichs erweitert werden, um die **Nutzungsmöglichkeiten des E-ID zu erweitern** und den Nutzen für E-ID-Inhaber sowie **Serviceanbieter** noch weiter zu erhöhen. Zugänglich ist ein solches Register für die Stammzahlenregisterbehörde nur, wenn eine geeignete technische Anbindung vorhanden ist und eine entsprechende gesonderte Rechtmäßigkeit der Verarbeitung gemäß Art. 6 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz – Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) – z. B. Einwilligung – für die Weitergabe der Merkmale aus diesem Register im Wege des E-ID besteht. So könnten beispielsweise **Versicherungsnachweise** oder Bestätigungen über **Mitgliedschaften** unter Nutzung der Funktion E-ID unter Kontrolle des E-ID-Inhabers berechtigten Serviceanbietern übermittelt werden. Wie bereits im allgemeinen Teil ausgeführt, soll die Möglichkeit der Nachweise von Merkmalen aus Registern von Verantwortlichen des privaten Bereichs erst in einem nächsten Schritt technisch umgesetzt werden. Dazu ist die aktuelle laufende **Digitalisierung** des österreichischen **Vereinsregisters** äußerst interessant.

## E-ID Aktivierung: Gerätepairing



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

Das Bundesministerium für Inneres verfolgt seit jeher das Ziel, die bestmögliche Datenqualität in den von ihm (in der Rolle des Verantwortlichen oder des Auftragsverarbeiters) geführten Registern zu gewährleisten. Erfahrungen aus der Verwaltungspraxis haben gezeigt, dass die Herausforderungen im Hinblick auf die Richtigkeit und die Aktualität der Daten im Ergänzungsregister für natürliche Personen (ERnP) vor allem durch Eintragungen von Sicherheits- und Personenstandsbehörden bewältigt werden können. Sofern diese Behörden beispielsweise durch ein laufendes Verwaltungsverfahren von geänderten Eintragsdaten Kenntnis erlangen, werden diese die Änderung in der Regel zuerst in ihrer eigenen Fachapplikation eintragen und sollen diese dem **Ergänzungsregister für natürliche Personen (ERnP)** in einem nächsten Schritt über eine technische Schnittstelle – den sogenannten Änderungszugriff – übermitteln. Erlangt ein sonstiger Verantwortlicher des öffentlichen Bereichs etwa durch ein laufendes Verwaltungsverfahren Kenntnis von geänderten Eintragsdaten des ERnP, hat er dies nach Maßgabe der technischen Möglichkeiten dem Auftragsverarbeiter zu melden. Letzterer verständigt in weiterer Folge die ursprünglich eintragende Stelle, sofern es sich hierbei um eine Sicherheits- oder Personenstandsbehörde handelt, die in weiterer Folge nach Abs. 4a erster Satz vorzugehen hat. Ansonsten hat der Auftragsverarbeiter die Änderung der Eintragsdaten im ERnP selbst vorzunehmen.

### Das Stammzahlenregister wanderte von der Datenschutzbehörde in das Digitalisierungsministerium

Das Stammzahlenregister wird von der Stammzahlenregisterbehörde betrieben und kann unter Zuhilfenahme der verschlüsselten Stammzahl bereichsspezifische Personenkennzeichen, sowohl in unverschlüsselter als auch in verschlüsselter Form, für eine Anwendung bereitstellen. Hierfür stellt das Stammzahlenregisters eine Schnittstelle zum Attribute Handler des Online Personenbindungs-Services bereit.

### Was ist das Identitätsdokumentenregister (IDR)

Das Identitätsdokumentenregister beinhaltet Daten zur Person, welche zur sicheren Identifikation (z.B. Reisepässe, Personalausweise, E-ID) benötigt werden. Bei der Aktivierung des E-ID wird das IDR vom VDA zur Abfrage von Personendaten im Zuge der Registrierung des E-ID benötigt. Ebenso verwendet das SZR das IDR zur Prüfung ob ein E-ID aktiviert und gültig ist.

### **Wer sind Vertrauensdiensteanbieter (VDA)**

Der Vertrauensdiensteanbieter (VDA) stellt die Infrastruktur für die Authentifizierung von Benutzern mittels qualifizierten elektronischen Signaturen (QSIG) bereit. Im Falle der oben angeführten E-ID Architektur, ist das der VDA A-Trust. Die Erstellung der QSIG durch den Benutzer stellt zugleich die Authentifizierung des Benutzers als auch die Einverständniserklärung zur Freigabe der Attribute durch den Benutzer dar.

### **Was ist das Mandate Issuing Service (MIS) das neue Onlinevollmachtsservice**

Das MIS (Mandate Issuing Service) ist Teil des Online Vollmachten Services und wird zur Abfrage von elektronischen Vollmachten durch den Identity Provider und zur Auswahl der Vollmacht durch den Benutzer benötigt.

### **Wofür wird die eIDAS Node die europäische Schnittstelle gebraucht?**

Der eIDAS Knoten bildet die Schnittstelle in das europäische eIDAS Netzwerk und wird für die Identifikation und Authentifizierung von ausländischen Personen verwendet.

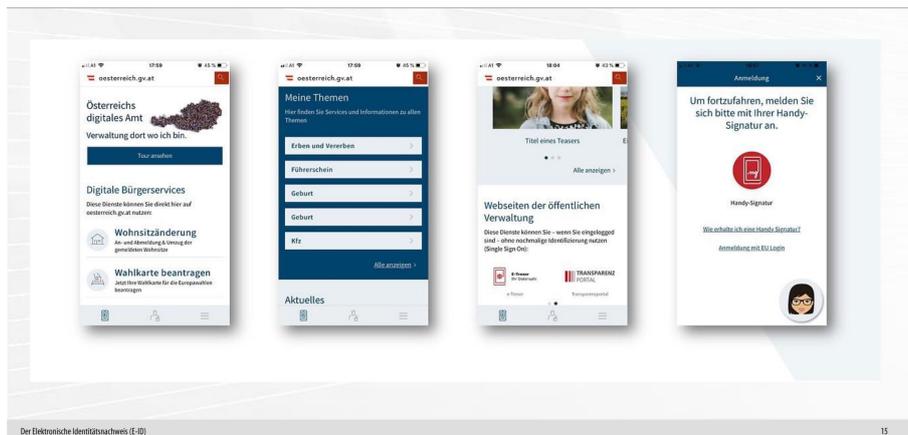
### **Wozu brauchen wir die Application AP**

Diese Komponente repräsentiert die Online Anwendung des Service Providers, die eine Identifikation und Authentifizierung mittels E-ID für eine Autorisierung an der Online-Anwendung benötigt.

### **Client – unser Handy, Computer, PDA und User – wir Bürger**

Der Client stellt das Gerät (Smartphone/Tablet/PC/Laptop) dar, mit dem der Benutzer auf eine Online Anwendung oder Service zugreifen möchte. Der Bürger bzw. die Bürgerin, die eine Online Anwendung oder eine elektronisches Service nutzt.

## Integrierte Services



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

### Wird das politische Ziel „Schneller zur Normalität“ mit dem Restart.ID-Konzept für die digitale Immunitätskarte gelingen?

Was findet man zum **Restart.ID-Konzept** auf der Internetseite der Staatsdruckerei?  
 Quelle: <https://www.staatsdruckerei.at/news/schneller-zur-normalitaet-restart-id-konzept-fuer-digitale-immunitaetskarte/>

**Die Staatsdruckerei zum Restart.ID-Konzept:** Da bei Immunitäts-Tests in absehbarer Zeit mit zuverlässigeren Produkten und einer breiten Ausrollung zu rechnen ist, haben die Experten der digitalen Staatsdruckerei-Tochter younix Identity AG die „Restart.ID“ konzipiert. Das Restart.ID-System unterstützt Wirtschaft und Gesellschaft beim Hochfahren und verbindet die Hochsicherheits-Expertise der Staatsdruckerei mit dem digitalen Know-how der younix Identity AG. Das Konzept sieht vor, einen offiziellen Identitätsnachweis des Users auf Basis des Reisepasses mit dem Nachweis einer bestehenden Immunität zu verbinden. Zukünftige Nutzer könnten auf Anfrage, z.B. einer Behörde, rasch und sicher via Smartphone gleichzeitig Identität und Immunität nachweisen.

### Konzept setzt auf Freiwilligkeit und Datenschutz

„Restart.ID“ kann Behörden sowie Bürgerinnen und Bürger beim schwierigen Weg zurück in den Alltag unterstützen. Dafür setzt das Konzept auf Dezentralisierung, Freiwilligkeit und Datenschutz. „Die persönlichen Daten sind immer dezentral und damit ausschließlich auf dem eigenen Smartphone verschlüsselt gespeichert. Es gibt keine zentrale Datenbank“, unterstreicht Staatsdruckerei-Geschäftsführer Praml.

### Open Source für volle Transparenz im In- und Ausland – zukünftig Weltweit?

Im Anlassfall, z.B. bei einem Grenzübertritt, bedarf es der expliziten Zustimmung des Nutzers für das Teilen der eigenen Daten mit einer anfragenden Partei, etwa einem Grenzbeamten. Schon zuvor sieht der Nutzer, welche Daten angefragt werden und kann entscheiden, ob er der Teilung zustimmt. Entscheidet sich der Nutzer dafür, so erfolgt der Austausch direkt mit dem Gerät des Beamten. Der Nutzer behält so immer die volle Souveränität über seine persönlichen Daten. Um Transparenz zu garantieren, soll Restart.ID auch als Open Source Projekt umgesetzt werden. Dafür ist die younix

Identity AG bei datenschutzrelevanten und ethischen Fragen bereits in fachlicher Abstimmung mit Univ.-Prof. Dr. Barbara Prainsack und Univ.-Prof. Dr. Nikolaus Forgó der Universität Wien.

### **Klares und hochsicheres Konzept**

Das Konzept setzt auf eine aktive Einbindung der öffentlichen Akteure – Behörden, Exekutive, Medizin. Eine echte Unterstützung kann Restart.ID aber nur mit Hilfe von Bürgerinnen und Bürgern entfalten. Daher soll die App besonders zugänglich sein und eine Verwendung ohne technisches Vorwissen problemlos ermöglichen:

- Nach dem App-Download und der Zustimmung des Nutzers wird das eigene Smartphone auf den persönlichen Reisepass gelegt.
- Mit dem OK des Nutzers kann „Restart.ID“ die im Reisepass-Chip enthaltenen Informationen (Portraitbild, Name, Geburtsdatum) anzeigen.
- Diese persönlichen Daten werden nicht weitergeleitet, sondern verbleiben ausschließlich verschlüsselt auf dem eigenen Gerät.
- Danach können Testergebnisse bereits absolvierter COVID19-Tests z.B. per QR-Code eingelesen werden.
- Im Bedarfsfall kann nach eigener Zustimmung jederzeit per Smartphone die eigene Identität und Immunität nachgewiesen werden.

### **Kein Zwang, sondern nur freiwillige Erweiterung**

„Restart.ID“ soll ausschließlich auf eine freiwillige Verwendung setzen. „Wir wollen eine freiwillige Unterstützung für alle anbieten. „Restart.ID“ soll jedenfalls nicht exklusiv oder verpflichtend zum Einsatz kommen“, stellt Praml klar. Personen ohne Smartphone oder Nutzungsabsicht sollen keinerlei Nachteil haben. „Es ist selbstverständlich, dass es parallel Möglichkeiten geben muss, sich analog auszuweisen“.

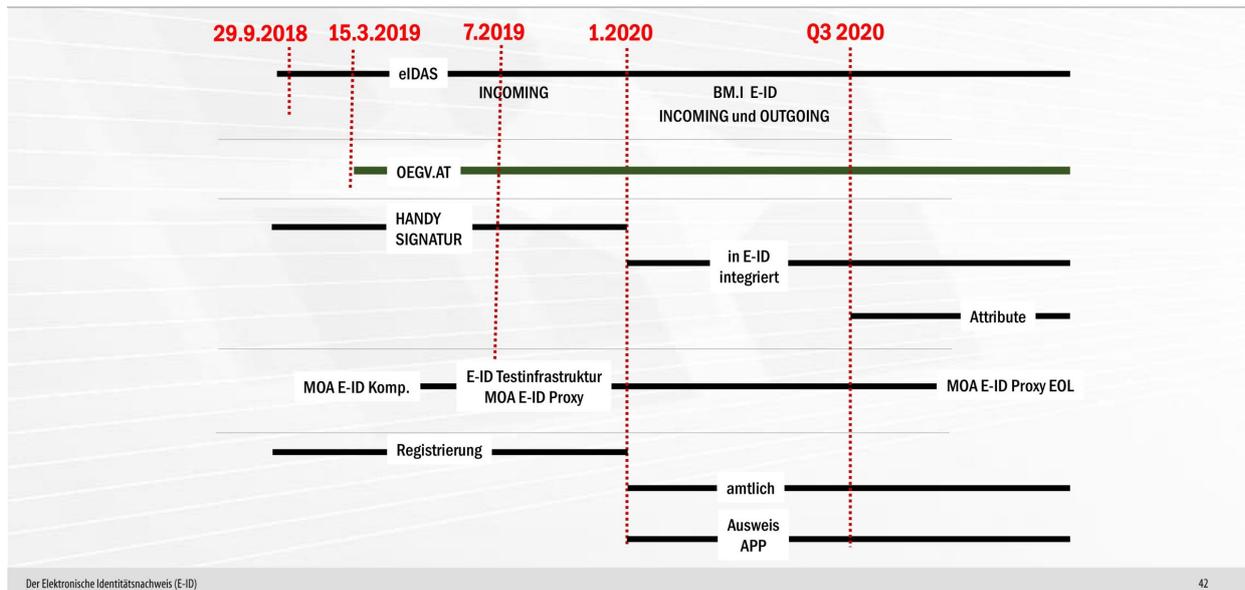
### **Wichtige Unterstützung für Reisen und Gesundheitswesen**

Das „Restart.ID“-Konzept soll zukünftig Staaten und Bürger gleichermaßen bei einer rascheren Rückkehr zur gewohnten Reisefreiheit unterstützen, indem Grenzübertritte unkompliziert, sicher und digital erfolgen könnten. Auch im Gesundheitswesen könnte Restart.ID für Vorteile sorgen. „Wenn sich kritisches Fachpersonal oder Patienten unkompliziert als immun ausweisen können, spart das Schutzausrüstung.“, skizziert Praml.

### **Grenzüberschreitender Einsatz als Ziel**

Die Österreichische Staatsdruckerei verfügt über das Know-how, um Restart.ID rasch zu realisieren. „Wir sind überzeugt, dass Restart.ID Staaten, Unternehmen und privaten Personen massiv bei der schwierigen Rückkehr in die Normalität unterstützen kann. Diese Hilfe kann aber nur Sinn machen, wenn wir gemeinsam mit starken Partnern auf staatlicher Ebene und mit der Unterstützung des Gesundheitssektors an der Umsetzung arbeiten. Gemeinsam können wir auf diese Weise innerhalb von wenigen Wochen einen entscheidenden Beitrag zum Schritt zurück zur Normalität schaffen“, schließt Praml.

## E-ID Roadmap



Screenshot – <https://eid.egiz.gv.at/> öffentliche pdf Präsentationen

Das gefällt Ihnen alles als Bürger nicht, was Sie da jetzt in meinem Artikel gelesen haben? Dann schreiben Sie zum Begutachtungsverfahren ihre persönliche Stellungnahme an das Parlament.

Wo? Hier:

[https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME\\_00056/index.shtml#tab-Stellungnahmen](https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00056/index.shtml#tab-Stellungnahmen)

Quellenangaben zu den Recherchen und zum Artikel:

[https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME\\_00056/index.shtml#tab-Stellungnahmen](https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00056/index.shtml#tab-Stellungnahmen)

[https://www.oesterreich.gv.at/themen/dokumente\\_und\\_recht/reisepass/Seite.020100.html](https://www.oesterreich.gv.at/themen/dokumente_und_recht/reisepass/Seite.020100.html)

<https://www.staatsdruckerei.at/sicherheit-qualitaet/high-security-solutions/total-security/>

<https://www.a-trust.at/de/handy-signatur/e-id/>

<https://eid.egiz.gv.at/>

[https://eid.egiz.gv.at/?page\\_id=1392](https://eid.egiz.gv.at/?page_id=1392)

[https://www.oesterreich.gv.at/themen/dokumente\\_und\\_recht/handy\\_signatur\\_und\\_kar tenbasierte\\_buergerkarte/1/Seite.2821106.html](https://www.oesterreich.gv.at/themen/dokumente_und_recht/handy_signatur_und_kar tenbasierte_buergerkarte/1/Seite.2821106.html)

<https://www.digitaustria.gv.at/initiativen/wirtschaft/projekte-wirtschaft/e-id.html>

<https://www.digitalaustria.gv.at/aktionsplan.html>

<https://www.jusline.at/gesetz/e-govg/paragraf/4>

[https://www.meinbezirk.at/eisenstadt/c-politik/kommt-der-digitale-impfpass-verknuempt-mit-elga-e-id-reisepass-und-restartid-app\\_a4071708](https://www.meinbezirk.at/eisenstadt/c-politik/kommt-der-digitale-impfpass-verknuempt-mit-elga-e-id-reisepass-und-restartid-app_a4071708)

Eine Stellungnahme von FPÖ GR Herbert Unger – zertifizierter Datenschutzbeauftragter  
Für alle Firmen, Personen, Institutionen und politischen Parteien gilt die  
Unschuldsumutung!

Vertrauliche Kommunikation mit dem Autor -hu-:

Threema ID hcclnname: WUU3ZJJV

hccl\_name@protonmail.com

**Wachsamkeitsschlagwörter:**

Überwachungsstaat, iD2020, I-ED, digitale Signatur, Handysignatur, BRZ, Blockchaintechnologie, ELGA, RFID-Chip, Restart.ID App, StoppCoronaApp, eIDAS-VO, Identitätsfeststellung, Vertrauensdienstegesetz, Smart Contracts, Netz- und Informationssystemssicherheitsgesetz, Datenschutz, EU DSGVO, Melderegister, Stammzahl, Stammzahlenregisterbehörde, Volksregisterzählung, E-Government, Digitalisierung, Datenschutzbehörde, Datenschutzrat, Aktionsplan zur Digitalisierung, Digital Austria, Gesichtserkennung, Security Accreditation Authority, Security Accreditation Board, Bundeskanzleramt, DP3T, PEPP-PT, eID-App, MICK (My Identity Check), Chainlock-Card, YOUNIQX Identity AG, Pan-European Privacy-Preserving Proximity Tracing, SpaceX, Future Operations Clearing Board, Think Austria, Computing-Zentrum IDRIS, Agentur für Hochleistungsrechnen GENCI, PRACE, PRACE COVID-19 Fast Track, Gesichtsfeldererkennung, SIS II, AFIS, Integrierte Fremdenadministration, IFA, COI-CMS System, Staatendokumentation, eCard, Zentrale Fremdenregister, IZR, AWS Cloud, Cyber-Physikalische-Systeme, Smart Factory, Smart Grid, Smart Logistics, Smart Health, Internet der Dinge, Daten und Dienste, Digital Industry 4.0, Digital Roadmap, digitaler Impfpass, elektronischer Impfpass, Immunitätsnachweis, New IP, New Internet Protocol, Holo-Sense Teleportation, ferSwarm, Providentia, Kiras, Weißbuch KI, SAA, Security Accreditation Authority, NCSA, National Communication Security Authority, NIS Behörde, BVT, Computer Emergency Response Teams, CERTs, National Security Authority, NSA, Büro der Informationssicherheitskommission, ISB, ISK, Security Clearances, PSC, Personnel Security Clearance, FSC, Facility Security Clearance, Epidemiologischen Meldesystem, EMS, Ge-sundheit Österreich GmbH, GÖG, AGES, Experience Management (XM), OPTIMOS 2, Nextthink, Computergestützte telefonische Erhebungen (CATI), KI-Textgenerator, Breitbandausbau, Glasfaserausbau, SoCs, virtuelle Perso, E-Perso, E2E-Verschlüsselung, E2EE, EARN IT Act, EC3, IETF, De-Cix-Knoten, IT-SiG2, NCAZ, Bluetooth-IDs, Exposure Notification API, BIAS, Bluetooth Impersonation Attacks, Siri, Alexa, Cortana, Bixby, Known Traveller Programm, Social-Scoring, cyberphysische Systeme, Sozialbonitätssysteme, Vollmachtenregister, eIDASProxy-Service, Identitätsprovider (IdP), MOA E-ID Proxy, VDA Authentifizierung, eIDAS Integration, PVP 2 S-Profil (SAML2), Handy-Signatur 2.0 (Security-Layer 2.0), E-ID Backend, bPK(s) / verschlüsselte bPK(s), OpenID Connect, PVP2 S-Profil, MOA Version 3.4.2, hobex, VIA bargeldlos zahlen, GAIA-X, IDEMIA, Sopra Steria, Shared Biometric Matching System, sBMS, eu-LISA, Ramjet, Scramjet, HAWC, Hypersonic Air-breathing Weapon Concept, ARRW, Air-Launched Rapid Response Weapon, BriefCam, Concardis, NetsGrout, NemID, BankID, Vermi, MRTD, Machine

Readable Travel Documents, Machine Readable Zone, MRZ, Nets App, further evolved Multimedia Broadcast Multicast Service, feMBMS, feMBMS-Signal, 5G-Antennenfernsehen, Thorium, eImpfpass, 5G New Radio (Dynamic Spectrum Sharing), Digital Services Act, fairdigitaleurope, Ressort-Chief Digital Officer, CDO-Task Force, Bundes-Chief Digital Officer, Kompetenzzentrum für Digitalisierung in der Bundesverwaltung, „Gesetz für digitale Dienste“, Secure Information Exchange Network Application (SIENA), Querying Europol Systems, EIS, Europol, QUEST Europol, Operational Real-Time Collaboration Solution, ORTICoS, Unified Search Engine (USE), Europol-Analysesystem (EAS), PERCI Europol, Terrorist Finance Tracking Programme (TFTP), Testing Context Based Approach for Targeted Decryption, Joint Cyber Unit, Satellite Imagery Related Datasets“ (SIRD), ATLAS Unterstützungsbüro, European Financial and Economic Crime Centre“ (EFECC)