WIEN / 18. Februar 2022

Stammzahlenregisterbehördenverordnung 2022

Geschäftszahl: 2022-0.032.809

Für epicenter.works
Mag.ª Tanja Fachathaler, MA, E.MA
Thomas Lohninger, BA

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Mit 20.01.2022 wurde der Entwurf der Verordnung der Bundesministerin für Digitalisierung und Wirtschaftsstandort über die Stammzahlenregisterbehörde (Stammzahlenregisterbehördenverordnung 2022, StZRegBehV 2022) zur Begutachtung vorgelegt.[1]

Diese soll die 2009 erlassene Verordnung ersetzen und stellt eine Anpassung an die aktuell noch im Gesetzgebungsverfahren befindlichen Novelle des E-Government-Gesetzes (E-GovG) dar.[2] Mit dieser Novelle werden die gesetzlichen Rahmenbedingungen für die Weiterentwicklung des Konzepts „Bürgerkarte" hin zum Elektronischen Identitätsnachweis (E-ID) geschaffen. Bereits im Vorfeld hat sich epicenter.works während des Begutachtungsverfahrens mit Stellungnahmen zu dieser gesetzlichen Neuerung geäußert.[3]

Der nunmehrige Verordnungsentwurf sieht seinen Erläuterungen zufolge aber genau diese problematische Errechnung der bereichsspezifischen Personenkennzeichen (bPK)[4] bei der Verwendung des E-ID an einer zentralen Stelle und die Einfügung in die Personenbindung unter der Hoheit der Stammzahlenregisterbehörde vor. Auch sollen damit die Bestimmungen des E-GovG zur Registrierung und Verwendung der E-ID konkretisiert werden. Die Voraussetzungen für einen Echtbetrieb würden allerdings noch nicht vorliegen. Dennoch soll die Verordnung bereits ab Inkrafttreten anwendbar sein, um den im E-GovG vorgesehenen Pilotbetrieb zu ermöglichen.

Durch diese Verordnung soll zum Wirkungsziel „Steigerung des Digitalisierungsgrades zum Nutzen für die Gesellschaft, Wirtschaft und Verwaltung" im Bundesvoranschlag beigetragen werden. Es ist jedoch unerlässlich, dass diese seitens der Bundesregierung angestrebten Optimierungsschritte Hand in Hand gehen mit datenschutzrechtlichen Garantien, um der Gesellschaft nicht nur den praktischen Nutzen, sondern auch die erforderliche Sicherheit ihrer Daten – und damit letztlich ihres Rechts auf Wahrung der Privatsphäre – zu gewährleisten.

In nachstehender Analyse werden die aus der Sicht von epicenter.works problematischsten Aspekte des Verordnungsentwurfs aus datenschutzrechtlicher Sicht dargelegt und Lösungsvorschläge unterbreitet.

1 RIS Dokument (bka.gv.at), https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_AFA956E2_7486_4FD9_B9CD_3E627AE6C488/BEGUT_AFA956E2_7486_4FD9_B9CD_3E627AE6C488.html

2 Zum aktuellen Status der Novelle: https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00161/index.shtml

3 https://epicenter.works/document/3799.

4 https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen.html

Inhaltsverzeichnis

ALLGEMEINE ANMERKUNGEN

Bestimmtheitsgebot

Eingangs ist zu bemerken, dass der vorgelegte Verordnungsentwurf in der aktuellen Formulierung vor dem Hintergrund der Komplexität des Regelungsgegenstandes bezüglich seiner Verständlichkeit auch für mit der Materie Vertraute mangelhaft ist. Bereits im Vorfeld war dieser Umstand im Zusammenhang mit dem E-GovG seitens des Datenschutzrates in seiner Stellungnahme dazu bemängelt und auf das Bestimmtheitsgebot in Art 18 B-VG verwiesen worden. Mit dem vorliegenden Verordnungsentwurf verhält es sich punkto Verständlichkeit nicht anders – sie kommt einer Denksportaufgabe gleich. Insofern schließt sich epicenter.works der Kritik des Datenschutzrates hierzu an. Eine Überarbeitung und klarer verständliche Formulierungen der einzelnen Bestimmungen ist jedenfalls vonnöten, um eine umfassende Bewertung der Konformität des Regelungswerks mit den Anforderungen der DSGVO zu ermöglichen. Insbesondere auch sind dabei die Ausführungen zu Verarbeitungsprozessen, Anforderungen und Verantwortlichkeiten ausreichend bestimmt zu determinieren, um dem Ziel einer Konkretisierung der Vorgaben aus dem E-GovG gerecht zu werden. Ebenso sind die Erläuterungen entsprechend nachvollziehbar zu formulieren.

Datenschutzfolgenabschätzung

Vor diesem Hintergrund ist es unerlässlich, dass eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO durchgeführt wird. Der aktuelle Entwurf sieht eine solche weder vor, noch wird erörtert, weshalb davon abgesehen werden könne. In Hinblick auf die Frage der Vertrauenswürdigkeit und Sicherheit der einzuführenden elektronischen Identitätsnachweise ist eine wirkungsorientierte Folgenabschätzung jedenfalls vonnöten.

Protokollierung

Insgesamt sieht der Entwurf der Verordnung an mehreren Stellen Protokollierungspflichten vor – so etwa in §§ 5, 6, und 7, auf die in weiterer Folge noch gesondert eingegangen wird. Dies ist zwar begrüßenswert, jedoch ist diese Sicherheitsmaßnahme alleine nicht ausreichend. Um auch tatsächlich wirksamen Schutz gegen etwaige auffällige Datenabfragen zu gewährleisten, bedarf es zusätzlich der Kontrolle dieser Protokolle durch die Stammzahlenregisterbehörde oder eine von dieser bevollmächtigte Stelle. Kontrollen der Protokolle sind im Verordnungsentwurf nicht vorgesehen, jedoch unabdinglich, um missbräuchliche Datenabfragen zu vermeiden. Weiters sind regelmäßige Audits vonnöten, um die Kompatibilität der Abfragen mit den Bestimmungen der DSGVO sicherzustellen und damit insbesondere abzuklären, ob die Abfragen auch dem Zweck der Datenverarbeitung entsprechen.

KONKRETE BESTIMMUNGEN

§ 5: bPK aus einem Bereich, in dem der Verantwortliche des öffentlichen Bereichs zur Vollziehung berufen ist

Die Bestimmung sieht in Abs. 2 vor, dass in Fällen, in welchen die von einem Verantwortlichen der Stammzahlenregisterbehörde bekanntgegebenen Daten nicht ausreichend seien, um eine Person eindeutig zuordnen zu können, die Stammzahlenregisterbehörde dem Verantwortlichen eine Liste von bestehenden Eintragungen aus dem ZMR oder ERnP – zu höchstens fünf Personen übermitteln kann. Auf diese Art soll eine eindeutige Zuordnung einer Person zu einem bestehenden Eintrag im ZMR oder dem Ergänzungsregister vorgenommen werden können.

Die Erläuterungen sprechen in diesem Zusammenhang von einer „bewährte[n] Vorgangsweise, die nicht nur „aus datenqualitätssichernden Gründen" notwendig sei, sondern „auch eine geeignete und unbedingt erforderliche Maßnahme" darstelle, um Mehrfacheintragungen ein- und derselben Person zu vermeiden. Dabei liege „die eindeutige und korrekte Zuordnung zu einem bestehenden Datensatz" im öffentlichen Interesse, seien doch aufgrund der fortschreitenden Digitalisierung und vermehrt auftretenden elektronischen Verwaltungsverfahren diese Eintragungen „die wichtigsten Anknüpfungspunkte innerhalb der österreichischen Verwaltung". Auch sei die Einschränkung der Liste auf fünf Datensätze das gelindeste Mittel und daher verhältnismäßig; eine Zuordnung einer Person zu einem bestehenden Datensatz könne auf anderem Weg nicht erreicht werden. Die höchstens fünf Datensätze würden „lediglich zum Zwecke der eindeutigen Zuordnung zu einem bestehenden Eintrag in das ZMR oder ERnP übermittelt und seien nach Erreichen des Zwecks zu löschen – sowohl im Falle einer Zuordnung, also auch dann, wenn dies nicht erfolgen konnte und ein neuer Eintrag zu erstellen ist.

Die Erläuterungen berufen sich in der beschriebenen Interessenabwägung unter anderem auch auf die Grundsätze der Datenminimierung und der Datenrichtigkeit. Außer Acht gelassen wird bei der dargelegten Vorgehensweise jedoch, dass schlimmstenfalls vier der fünf übermittelten Datensätze - im Falle des Nicht-Zutreffens gar alle fünf – „zu viel" und ohne Grund eingesehen wurden. Weshalb just die Anzahl von fünf Datensätzen als geeignet, erforderlich und gelindestes Mittel anzusehen ist, und nicht etwa weniger Datensätze (wenn überhaupt nötig) zu einem ähnlichen Ergebnis führen könnten, wird in den Erläuterungen nicht ausgeführt und ist die Verhältnismäßigkeitsprüfung allein schon aus diesem Grund mangelhaft.

Im Übrigen mangelt es der Bestimmung auch an Bestimmtheit insofern, als sie keine Ausführung darüber enthält, wo das Clearing stattfindet. Der vorletzte Satz der Bestimmung sieht vor, dass „die Stammzahlenregisterbehörde dem Verantwortlichen eine Liste von bestehenden Eintragungen aus dem ZMR oder dem ERnP [übermitteln kann], auf die die übermittelten Daten zutreffen". Dies lässt darauf schließen, dass der Abgleich nicht bei der Stammzahlenregisterbehörde stattfindet, sondern beim Verantwortlichen eines öffentlichen Bereichs.
Die sauberere Lösung wäre in diesem Fall, in dem ja zumindest vier nicht zutreffende Datensätze eingesehen werden, jedenfalls ein Clearing direkt bei der Stammzahlenregisterbehörde.

Den Erläuterungen ist zudem zu Abs. 3 der Bestimmung der Hinweis zu entnehmen, dass zum Zwecke der korrekten Zuordnung weitere Merkmale zu bestehenden Eintragungen übermittelt werden dürfen. Unter Verweis auf § 16 Abs. 1 MeldeG werden als Beispiele insbesondere das bPK im privaten Bereich, das Geburtsdatum, der Geburtsort oder der bisherige Wohnsitz genannt.
Dem Text des Verordnungsentwurfs mangelt es zur Gänze an einer Bezugnahme hierauf; ebenso wenig wird eine Verhältnismäßigkeitsprüfung vorgenommen.

So eine solche Prüfung der Erforderlichkeit und Verhältnismäßigkeit dennoch zugunsten der Aufnahme weiterer Merkmale ausschlagen sollte, wäre unser Lösungsvorschlag wie folgt:
Die erweiterte Ermächtigung zu einem Abgleich mit weiteren Merkmalen soll in den Text der Verordnung selbst Eingang finden und überdies sind die in Frage kommenden Merkmale – entgegen der aktuellen, demonstrativen Formulierung in den Erläuterungen - abschließend aufzuzählen.

§ 6: bPK aus einem Bereich, in dem der Verantwortliche des öffentlichen Bereichs nicht zur Vollziehung berufen ist

In den Erläuterungen wird zu dieser Bestimmung auf die Ausführungen zu § 5 verwiesen, der ja Situationen regelt, in denen der Verantwortliche des öffentlichen Bereichs zur Vollziehung berufen ist. Im Unterschied dazu jedoch ist dies in § 6 genau nicht der Fall: der Verantwortliche ist nicht zur Vollziehung berufen. Dennoch beschränken sich die Erläuterungen darauf, auf die „wesentliche Bedeutung" der korrekten Zuordnung zu verweisen, sowie, dass bei ähnlichen Personendatensätzen zu diesem Zwecke auch weitere Merkmale übermittelt werden dürfen.

Gänzlich unerwähnt jedoch bleiben Ausführungen zu den Rechtsgründen und Umständen, weshalb ein Verantwortlicher bPKs aus einem Bereich anfordern kann, in dem er nicht zur Vollziehung berufen ist. Dies erweckt den Eindruck, als ob der zu bewahrende Mehrwert des bPKs als 2004 bewusst eingezogene Firewall zwischen den Datenverarbeitungen der verschiedenen Teile unseres Staates von jener Institution, die mit der Einhaltung dieses Trennungssystems beauftragt ist, selbst nicht mehr in Erinnerung ist. Eine Abkehr vom System des bPK wäre ein gravierender Rückschritt und mutwilliger Abbau von Datenschutz durch die öffentliche Hand. Die fehlende Begründung und notwendige Ausführung der Umstände der Anwendung dieser Bestimmung stellen eine Mangelhaftigkeit dar, die dringend korrigiert werden muss.

Da auch in dieser Bestimmung die Übermittlung einer Liste von bis zu fünf ähnlichen Datensätzen zum Zwecke der eindeutigen Zuordnung vorgesehen ist, wird auf die Ausführungen zu § 5 verwiesen. Unter Einbezug der unmittelbar vorstehenden Bedenken erscheint die Verhältnismäßigkeitsprüfung in den Erläuterungen zu § 5 umso bedenklicher und wird auch dieser Aspekt im gegebenen Kontext, in dem ein Verantwortlicher Daten aus einem Bereich nutzen möchte, für den er unzuständig ist, gesondert zu beurteilen sein.

§ 7: bPK für die Verwendung im privaten Bereich

Diese Bestimmung sieht vor, dass ein Verantwortlicher des privaten Bereichs, also ein Unternehmen, die Stammzahlenregisterbehörde um die Errechnung von bPK ersuchen kann, wenn es aufgrund von

gesetzlichen Vorschriften die Identität seiner Kund*innen festzuhalten hat oder es seinen KundInnen eine technische Umgebung für die Datenübermittlung zur Verfügung stellt.

Die rechtlichen Voraussetzungen dafür, dass bei Vorliegen einer Einwilligung der Nutzer*innen Daten des E-ID auch privatwirtschaftlichen Anbietern zur Verfügung gestellt werden können, wurden mit dem E-GovG 2020 geschaffen. Den Erläuterungen zufolge ist dabei an Fälle wie etwa bei kommunalen Verkehrsverbünden, Banken, Versicherungen, Autofahrerclubs, etc. zu denken.

Es bedarf im Anwendungsbereich dieser Bestimmung jedenfalls einer intensiven Debatte darüber und insbesondere einer Einzelfallprüfung, ob die Anforderungen erfüllt sind, dass der/die Verantwortliche des privaten Bereichs aufgrund gesetzlicher Vorschriften die Identität seiner/ihrer Kund*innen festzuhalten hat. Es müssen ausreichend starke Schutzmaßnahmen bestehen, die vor nicht nötiger Identitätsfeststellung, Abfragen zusätzlicher Merkmale oder der Zusammenführung mit anderen Registern sowie der Weitergabe der Daten an Dritte schützen. Epicenter.works wird die weiteren Entwicklungen in der praktischen Umsetzung dieses Bereichs jedenfalls sehr genau mitverfolgen und verweist auf die gegenüber dem BMDW und BMI im Rahmen der eID-Arbeitsgruppe 2020 geäußerten Bedenken der Öffnung von staatlichen Identitätsdaten für die Wirtschaft.[5] Durch unsere zentrale Rolle in den Verhandlungen rund um die Reform der eIDAS-Verordnung auf EU-Ebene verweisenwir auch auf unsere Position zu diesem Rechtsakt, welche ähnliche Probleme diskutiert.[6]

Im Übrigen sieht die Bestimmung in Abs. 5 vor, dass das „Regelungsregime von § 6 vollinhaltlich anzuwenden“ sei. Dies würde auch eine Einbeziehung der Möglichkeit miteinbeziehen, im Falle der trotz bekanntgegebenen Daten nicht möglichen Zuordnung zu einer Person, „eine Liste von bestehenden Eintragungen aus dem ZMR oder dem Ergänzungsregister, auf die die übermittelten Daten zutreffen, [zu] übermitteln“. Dies soll nur zulässig sein, „wenn die vom Verantwortlichen übermittelten Daten auf höchstens fünf Personen zutreffen“. Diesbezüglich sei auf unsere vorstehend dargelegten Bedenken zu § 5 und § 6 verwiesen. Diese sind umso gravierender, als sich die gegenständliche Bestimmung auf den privaten Geschäftsverkehr bezieht und die normierte Vorgehensweise jedenfalls unverhältnismäßig ist.

5 https://epicenter.works/content/unsere-position-zur-elektronischen-identitaet
6 https://epicenter.works/document/3865 und https://epicenter.works/document/3880