Das BGEID – auf dem Prüfstand des Datenschutzrechts

Am 7. März 2021 stimmt das Schweizer Volk über die staatlich anerkannte Elektronische Identität (E ID) ab. Es geht um das Bundesgesetz über Elektronische Identifizierungsdienste (BGEID), gegen welches das Referendum ergriffen wurde. Das Referendumskomitee sagt «Datenschutz ungenügend». Was ist dran an dieser Kritik?

Bei digitalen Vorgängen stehen Daten im Zentrum, was selbstredend auch für die E-ID gilt. Der Datenschutz ist deshalb für die E-ID zentral. Der nüchterne Blick auf die Fakten zeigt, dass das BGEID den Datenschutz deutlich verbessert – der Datenschutz wird mit dem BGEID sogar besser umgesetzt als mit dem Wunschszenario des Referendumskomitees, was dieser Beitrag beleuchtet.

Weshalb eine E-ID?

Wer eine E-ID hat, hat ein Login. Mit dem Login kann die Nutzerin nachweisen, wer sie ist, wenn dies z.B. bei der Online-Bestellung eines Kinobilletts, einer Online-Buchbestellung, beim Online-Behördengang (z.B. Strafregisterauszug bestellen) von ihr verlangt oder in ihr Belieben gestellt wird. Die Kinokasse, der Onlineshop oder die Behörde können unter Rückgriff auf die E-ID die Identität der Nutzerin feststellen.

Was verändert sich mit der E-ID?

Ein Online-Login funktioniert auch ohne E-ID. Wer sich im Internet bewegt, weiss, worum es beim Online-Login geht: Entweder schlägt z.B. die Kinokasse vor, dass die Nutzerin ein E-Mail und ein Passwort definiert, mit dem sie sich registriert, oder die Kinokasse erlaubt die Anmeldung über einen Drittdienst. Das BGEID ermöglicht, dass Drittdienste neuerdings ein Online-Login mit einem Gütesiegel des Staats anbieten können. Diese Möglichkeit gab es bislang nicht.

Die E-ID als neue Alternative

Dem Verständnis der E-ID dient die folgende Gegenüberstellung. Man kann drei Modelle unterscheiden, das dritte Modell beschreibt die E-ID (*siehe Abb. 1 - 3*)

Im Modell #1 wird die Interaktion der Nutzerin mit der Kinokasse gezeigt. Dem stehen die beiden Modelle unter Verwendung eines Drittdiensts gegenüber. Anbieter gemäss Modell #2 sind z.B. Twitter, Google oder Facebook. Im Modell #3 (mit E-ID) kann IdP (Anbieter des Drittdiensts) sein, wer die Anerkennungsvoraussetzungen erfüllt (Art. 13 Abs. 2 BGEID: Datenhaltung Schweiz, Gewähr für den Datenschutz).

Um welche Daten geht es?

Die Kinokasse definiert die Angaben, die sie zur Identifikation der Nutzerin benötigt (sog. Personenidentifizierungsdaten). Damit weiss sie, wer (die Nutzerin) wann und mit wem (Kinokasse) interagiert hat (man spricht von Nutzungsdaten). Auch um welchen Film es ging (Titel und Spielzeit der gebuchten Filmvorführung), ist bei der Kinokasse gespeichert (man spricht von Inhaltsdaten). Wenn die Nutzerin mehr als einmal in wiedererkennbarer Weise ein Ticket kauft, gruppiert die Kinokasse diese Angaben (also Inhaltsdaten) sowie die Bestellhistorie (also Nutzungsdaten) zu einem sog. Nutzungsprofil. Was die Kinokasse im Modell #1 und im Modell #2 nicht so genau weiss: Ob die Personenidentifizierungsdaten auch real sind bzw. tatsächlich einer existierenden Person zugeordnet werden können.

Die Rolle von Drittdiensten ohne E-ID

Wenn die Kinokasse einen Drittdienst (im Beispiel: Facebook) für den Login-Service benutzt, fallen bei diesem Nutzungsdaten an. Facebook weiss also, wer (die Nutzerin) mit wem (der Kinokasse) wann einen Vertrag abgewickelt hat. Diese Nutzungsdaten gehen somit in die USA. Der Staat verbietet dies nicht, nicht einmal mit dem geltenden oder dem revidierten Datenschutzgesetz (DSG). Inhaltsdaten gehen über, wenn die Kinokasse zusätzlich noch Weiteres übermittelt. Facebook kann bereits aus den überstellten Nutzungsdaten viele Rückschlüsse ziehen – gänzlich ausserhalb der Einflusssphäre der Schweiz.

Was ist bei der E-ID anders?

Mit der E-ID steht der Nutzerin eine Alternative offen. Der IdP übernimmt dabei zunächst dieselbe Rolle wie Facebook. Auch beim IdP fallen Nutzungsdaten an. Und doch gibt es wichtige Unterschiede, und um diese geht es beim BGEID:

- der IdP ist reguliert, untersteht der Aufsicht der E-ID-Kommission (EIDCOM) und muss die Vorgaben des BGEID einhalten

- er sorgt für getrennte Datenhaltung von Personenidentifikations- und Nutzungsdaten, gewährt Einsicht und löscht die Daten entsprechend den gesetzlichen Vorgaben

- der IdP darf die Personenidentifikationsdaten einerseits und Nutzungsdaten anderseits nicht für eigene Zwecke oder sachfremde Zwecke Dritter verwenden (die vom Referendumskomitee behauptete Kommerzialisierung durch den IdP ist verboten und würde sanktioniert)

- die Kinokasse (Merchant) schliesst einen Anbindungsvertrag mit dem IdP; auch dieser sichert den Datenschutz ab

Mit diesen Massnahmen werden Online-Bewegungen der Nutzerin geschützt. Bei herkömmlichen Drittdiensten fehlt dieser Schutz. Er entsteht erst mit dem BGEID.

Die E-ID verbessert die datenschutzrechtliche Analyse

Aus Sicht des Datenschutzrechts geht es jeweils um Folgendes: Wo und zu welchen Zwecken werden Daten erhoben? Wer hat Zugriff auf Daten? Wer darf Daten verwenden und wer nicht?

Der vorstehende Abschnitt hat gezeigt: Das BGEID sieht sehr strikte Zugriffs- bzw. Weitergabeverbote vor, die es ohne BGEID in der Form nicht gäbe (auch nicht im DSG, das Weitergabeverbote a priori nur für besonders schützenswerte Personendaten vorsieht). Die Weitergabe von Nutzungsdaten wäre unter dem BGEID auch mit Zustimmung der Nutzerin nicht möglich, was den Schutz der Nutzerin klar verbessert (anders im DSG). Ebenso streng ist die Analyse in Bezug auf die Verwendungsverbote. IdP dürfen Personenidentifikations- und Nutzungsdaten nicht für eigene oder sonstige sachfremde Zwecke verwenden. Die Kommerzialisierung durch den IdP ist klar ausgeschlossen.

Die Zukunft würde sich im Vergleich zur heutigen Situation mit dem BGEID somit deutlich verbessern. Aus einer datenschutzrechtlichen Optik führt das Referendum aus Nutzersicht somit zu keiner Verbesserung. Die Datenschutzkritik des Referendumskomitees ist unbegründet.

Was ist am BGEID umstritten?

Der IdP verteilt Logins an Personen, die ein solches Login wollen und beim IdP beantragen (Nutzerinnen der E-ID). Wer ein solches Login hat, hat die E-ID erworben. Aus Sicht des Identitätsdienstleisters gilt Folgendes: Er hat der Nutzerin eine E-ID ausgestellt. Nur dieser Ausstellungsvorgang wird mit dem Referendum angefochten. Das Referendumskomitee will, dass der Staat Logins verteilen soll, und nicht ein privater IdP.

Wie sähe die Alternative aus?

Dass der Staat eine private Dienstleisterin (einen Outsourcer) einsetzen würde, wenn er selber die Logins ausgäbe, wäre die naheliegende Folge der vom Referendumskomitee verfolgten Vision (und wird auch vom Referendumskomitee nicht in Abrede gestellt). Der Outsourcer würde für den Staat handeln und die technische Infrastruktur für den Bund bereitstellen. Grafisch lässt sich der Unterschied wie in *Abb. 4 und 5* darstellen.

Der Vergleich zeigt, wie wenig die vom Referendumskomitee propagierte Alternative die Situation ändern würde:

- anstelle des IdP erhielte ein Outsourcer Zugriff auf die Identifikationsdaten

- auch dem Outsourcer wäre die Datennutzung verboten (allerdings nur noch aus Vertrag und nicht mehr kraft des Gesetzes)

- es gäbe nur noch einen Anbieter (Bund mit Outsourcer) und nicht mehrere, im Wettbewerb stehende Lösungen. Der Wettstreit der Ideen käme so nicht zum Tragen

- der Bund erhielte auch auf die Nutzungsdaten Zugriff (was gemäss BGEID so nicht stattfindet); dies würde den vom Referendumskomitee selber betonten Zielen (Datenvermeidung) widersprechen

Weiter ist zu hören, dass die zentrale Speicherung von Daten ein Datenschutzproblem darstelle. Es sei eine dezentrale Datenspeicherung vorzuziehen. Dies ist aus Datenschutzsicht ein grundsätzlich richtiger Gedanke (Risikominimierung). Es handelt sich allerdings um eine Frage der Softwarearchitektur. Und hierzu macht das BGEID bewusst keine Vorgaben. Gleich in Art. 1 Abs. 3 BGEID legt es den Grundsatz der Technologieneutralität fest. Das BGEID würde somit IdP-Lösungen mit dezentraler Datenstruktur zulassen. Wer die zentrale Datenhaltung kritisiert, sollte nicht das BGEID bekämpfen. Das BGEID ist vielmehr eine Einladung an Anbieter mit einem dezentralen Lösungsdesign, sich als IdP anerkennen zu lassen. Zudem: Wenn das fedpol selber die eigene Datenbank bei einem Outsourcer hosten lässt, wäre mit dem Referendum nichts gewonnen. Und dass eine redundante Datenhaltung mit dem Referendum vermieden werden kann, ist alles andere als gesichert.

Gibt es das beschworene Missbrauchspotential in der E-ID?

Das Referendumskomitee bringt vor, es bestehe bei der privatwirtschaftlichen Lösung ein Missbrauchspotential (gemeint ist: erst und gerade wegen des BGEID). Und zwar gehe es um Missbrauch durch den IdP. Dies liege an der zentralen Speicherung von Daten beim IdP. Diese Kritik lässt sich nicht ernsthaft aufrecht erhalten. Wie gesehen, ist die zentrale Speicherung vom BGEID nicht vorgeschrieben. Solange genügend Sicherheitsmassnahmen bestehen, kann ein Anbieter mit einer solchen Lösung noch immer als IdP anerkannt werden (Art. 13 Abs. 2 lit. g BGEID). Zudem: Da das BGEID Datenzugriffs- und Datenverwendungsverbote enthält, die weit schärfer sind als was das DSG fordert, ist der Missbrauchsvorwurf nicht naheliegend. Namentlich die vom Referendumskomitee heraufbeschworene Gefahr der Kommerzialisierung von Daten durch einen IdP ist im BGEID explizit ausgeschlossen.

Fazit

Nach alldem: Der mit Vehemenz vorgetragene Hauptpunkt des Referendumskomitees (E-ID als Staatsaufgabe!) ist nicht geeignet, die Daten der Bürgerinnen besser und effizienter zu schützen, als dies gemäss BGEID der Fall wäre. Im Gegenteil: Die Wunschlösung des Referendumskomitees führt sogar zu schlechteren Resultaten. Dass es zu einer Datenübermittlung auf Server eines oder mehrerer IdP kommt, kann jedenfalls mit Blick auf die Aufsicht durch die EIDCOM und die festgeschriebenen Nutzungs- und Weitergabeverbote nicht ausschlaggebend sein – insbesondere mit Blick darauf, dass eine langfristige Speicherung von besonders sensiblen Daten beim IdP ebenfalls ausgeschlossen ist. Ergänzend noch dies: Die Ablehnung des BGEID führt nicht automatisch zum Wunschzustand des Referendumskomitees. Vielmehr wird der Status Quo beibehalten – und den will niemand.

LAUX LAWYERS AG
ZURICH | BASEL

Zum Autor

Dr. Christian Laux, LL.M., ist Rechtsanwalt und Partner einer Kanzlei mit Büros in Zürich und Basel sowie Vizepräsident der Swiss Data Alliance (www.swissdataalliance.ch). Er gibt in diesem Beitrag seine persönliche Meinung wieder.

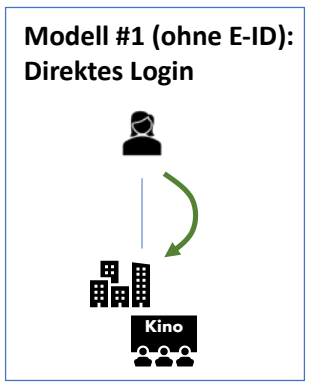

Abb. 1: Direktes Login

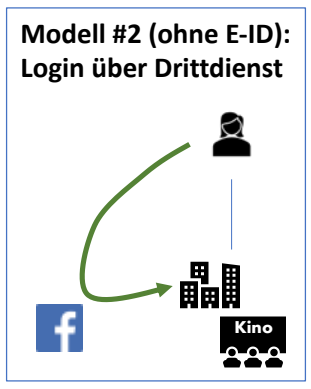

Abb. 2: Login mit Drittdienst

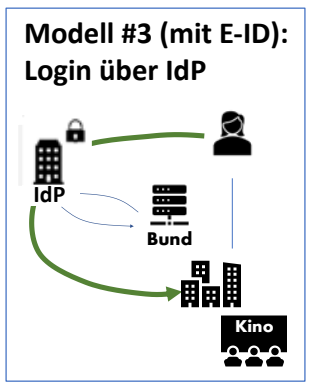

Abb. 3: Login mit IdP

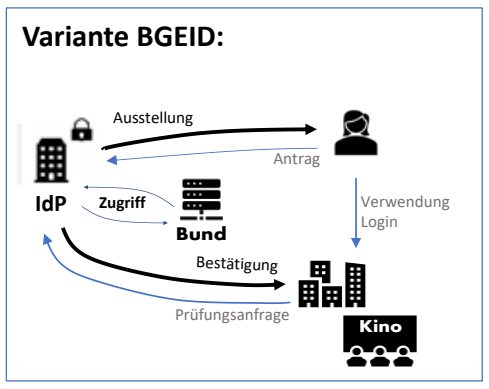

Abb. 4: Ausstellung durch den IdP

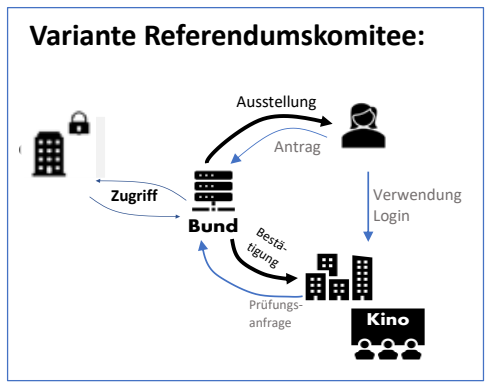

Abb. 5: Ausstellung durch den Bund