privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Merkblatt für Online-Portale der öffentlichen Verwaltung

1 Einleitung

Die heutigen Technologien bieten die Möglichkeit, Dienstleistungen rund um die Uhr anzubieten und zu nutzen. Wer von den Chancen der Digitalisierung nachhaltig profitieren will, muss die Risiken kontinuierlich bewerten und Sicherheitsvorkehrungen treffen. Dieses Merkblatt befasst sich spezifisch mit den juristischen und technischen Anforderungen an Online-Portale der öffentlichen Verwaltung. Das Dokument unterstützt öffentliche Organe bei der Planung und beim Betrieb von Online-Portalen, bietet Entwicklerinnen und Entwicklern eine entsprechende Orientierung und dient Datenschutzbeauftragten bei der Einschätzung und Beurteilung von Online-Portalen.

2 Begriffsdefinitionen

Identifizierung/Verifizierung/Authentifizierung/Autorisierung: Diese Begriffe werden in der Praxis oft verwechselt. Da für keinen der Begriffe eine verbindliche Definition vorliegt, sollen diese im Folgenden geklärt und voneinander abgegrenzt werden.

Nachfolgend werden die wichtigsten Begriffe definiert:

Begriff	Beschreibung
Amtliche Identifizierung	Bei einer amtlichen Identitätsprüfung wird eine Person durch den entsprechenden Prozess amtlich identifiziert und ihre Identität damit durch eine glaubwürdige Stelle rechtskräftig bestätigt. Solche Prozesse sind beispielsweise: • Persönliches Vorsprechen am Schalter • Identifizierung mittels Brief • Drittanbieter verifiziert mittels eines amtlichen Ausweises (z.B. Suisse ID oder Mobile ID) Prinzipiell sollte die Identität nur dort nachgewiesen werden müssen, wo dies für den Geschäftsvorgang notwendig ist.
Attributbezogene Verifizierung	Bei der attributbezogenen Verifizierung wird ein zur Benutzerin oder zum Benutzer gehörendes Element überprüft. Beispielsweise wird überprüft, ob ein Bestätigungscode (SMS) auf der angegebenen Handynummer empfangen wurde. Es sind dies beispielsweise: • Verifizierung einer E-Mail-Adresse • Bestätigung der Telefonnummer
Authentifizierung (Authentication = Prozess der Überprüfung)	Bei der Authentifizierung handelt es sich um die Überprüfung der korrekten Anmeldeinformationen der Benutzerin oder des Benutzers. Für diese Überprüfung werden die Anmeldeinformationen der Benutzerin oder des Benutzers (häufig Benutzername und Kennwort) mit den im System hinterlegten Daten abgeglichen.
Autorisierung (Authorization)	Bei der Autorisierung handelt es sich um die Einräumung von speziellen Rechten. War die Authentifizierung einer Benutzerin oder eines Benutzers erfolgreich, bedeutet dies nicht automatisch, dass diese Person bestimmte Dienste und Leistungen nutzen darf. Darüber entscheidet die Autorisierung. Die Autorisierung erfolgt nicht ohne eine vorherige erfolgreiche Authentifizie-

Begriff	Beschreibung
	rung.
Portal	Unter dem Begriff Portal wird ein im Internet verfügbarer Eintrittspunkt (Single Point of Access) für Benutzerinnen und Benutzer zu den digitalen Dienstleistungen und Geschäftsabwicklungen mit öffentlichen Organen (kommunalen, kantonalen und Bundesbehörden) verstanden.
Registrierung	Die Registrierung ist die erste einmalige Anmeldung einer Einwohnerin oder eines Einwohners für ein Einwohnerkonto oder eine Dienstleistung, die über ein Portal angeboten wird. Je nach Geschäftsfall reicht eine attributbezogene Verifizierung aus oder es ist eine amtliche Identifizierung nötig.

Tabelle 1: Begriffsdefinitionen

3 Portaltypen

Grundsätzlich kann als Portaltyp zwischen einem Durchgangsportal und einem Stammdatenportal unterschieden werden.

Ein Durchgangsportal dient der reinen Authentifizierung und Autorisierung der Benutzerin oder des Benutzers, bevor sie oder er auf eine Fachanwendung zugreifen kann. Ausser den Authentifizierungs- und Autorisierungsdaten für das Portal werden keine weiteren Daten gespeichert.

Im Durchgangsportal gespeicherte Authentifizierungs- und Autorisierungsdaten sind:
- Benutzername und Passwort
- n-Faktor-Informationen
  - Handynummer/Zertifikat nach ZertES
  - usw.
- Autorisierungs- und Berechtigungsinformationen
  - Zugriffsberechtigungen auf Fachapplikationen
  - Vollmachten und Berechtigungen
- Ob und wie die Benutzerin oder der Benutzer identifiziert wurde
- Statusmeldungen

Bei einem Stammdatenportal sind nebst der Authentifizierung und Autorisierung (vergleiche Daten Durchgangsportal) auch Stammdaten im Portal hinterlegt bzw. werden aus anderen Fachanwendungen importiert. Die Stammdaten können auch an einzelne Fachapplikationen weitergereicht werden.

Stammdaten sind dabei:
- Vorname, Name und Adresse
- Korrespondenzsprache
- Portal-Einstellungen
- usw.

In der Praxis kann es vorkommen, dass für einzelne spezifische Fachapplikationen in einem Stammdatenportal keine Stammdaten hinterlegt sind, sondern nur reine Authentifizierungs- und Autorisierungsdaten.

Je nach Geschäftsfall ist es möglich, dass im Portal zusätzlich temporär oder permanent Fachapplikationsdaten gespeichert werden. In diesem Fall gelten die gleichen Anforderungen für das Portal wie für die Fachapplikation.

4 Möglichkeiten zur Registrierung einer Benutzerin oder eines Benutzers

Die Anforderungen an die Registrierung und die damit verbundene allfällige Identifizierung ergeben sich aus dem jeweiligen Geschäftsfall, den zu bearbeitenden Daten und den Anforderungen der angebundenen Fachapplikation. Die konkreten Anforderungen sind im Einzelfall zu prüfen.

Im Falle einer Registrierung für einen SMS-Newsletter reicht unter Umständen eine attributbezogene Verifizierung der Telefonnummer, während für komplexe Geschäfte und für die Bearbeitung von sensitiven Daten gegebenenfalls eine amtliche Identifizierung notwendig ist.

Die folgende Tabelle enthält einige Anwendungsfälle für die Registrierung für die attributbezogene Verifizierung und die amtliche Identifizierung.

Verifizierung/Identifizierung	**Anwendungsfälle für Registrierung**
Attributbezogene Verifizierung	• Anmeldung für E-Mail-Newsletter • SMS-Erinnerung für den Abfallkalender • …
Amtliche Identifizierung	• Online-Steuererklärung • Beantragen von Stipendien • …

Tabelle 2: Anwendungsfälle Registrierung

5 Möglichkeiten zur Authentifizierung einer Benutzerin oder eines Benutzers

Die konkreten Anforderungen und Massnahmen an die Authentifizierung leiten sich aus dem jeweiligen Geschäftsprozess, den zu bearbeitenden Daten und den Anforderungen der jeweiligen Fachapplikationen ab. So bedeutet eine Authentifizierung nicht immer, dass für den Zugriff ein Benutzername und Passwort benötigt wird. Unter Umständen kann auch eine Plausibilisierung (Abgleich mit aktuellen Daten der kommunalen oder kantonalen Behörden) ausreichend sein. Sind Dienste mit unterschiedlichen Anforderungen an die Authentifizierung (einfach/stark) über das gleiche Portal zugänglich, so kann entweder von Anfang an stark authentifiziert werden oder erst beim Aufrufen (stufenweise) des entsprechenden Dienstes, der eine starke Authentifizierung benötigt.

Die nachfolgende Tabelle listet die Möglichkeiten zur Authentifizierung auf und klassifiziert sie.

Authentifizierung	**Beschreibung**
Einfach	• Anwendbar für Anwendungsfälle mit Personendaten • Benutzername und Passwort • Plausibilisierung von personenbezogenen Daten gegenüber aktuellen Daten (z.B. Stammnummer Fahrzeug, Meldeadresse oder Geburtsdatum)

Authentifizierung	Beschreibung
Stark:	Anwendbar für Anwendungsfälle mit besonderen Personendaten/sensitive Daten
2-Faktor	• Smartcard/Zertifikat • TAN/mTAN/One-time Password (OTP) • Drittanbieter verifiziert mit 2-Faktor-Login (z.B. Mobile ID) • App-Verifizierung/-Bestätigung • …
n-Faktor	• In gewissen Fällen (Bearbeitung sensitiver Daten) ist eine n-Faktor-Authentifizierung (3 oder mehr Faktoren) notwendig. Dies ist im Einzelfall zu prüfen.

Tabelle 3: Zusammenfassung Authentifizierung

Es ist grundsätzlich davon auszugehen, dass wenn eine amtliche Identifizierung nötig ist, auch eine starke Authentifizierung benötigt wird. Es ist daher empfehlenswert, die Prozesse für die Registrierung, Identifizierung und Authentifizierung in einer gemeinsamen Risikoanalyse und Massnahmendefinition zu betrachten.

6 Übersicht Anwendungsfälle

Grundsätzlich lassen sich die Dienstleistungen in fünf verschiedene Anwendungsfälle einteilen. Die jeweiligen Anforderungen an die Identifizierung und die Authentifizierung sowie die nötigen Massnahmen sind im Einzelfall zu prüfen.

Für jeden Anwendungsfall kann dabei unterschieden werden, ob er ohne Authentifizierung oder mit Authentifizierung zur Anwendung kommt. Unter die Authentifizierung fällt dabei auch die Verknüpfung von Personendaten, beispielsweise die Verknüpfung der Autonummer mit dem Namen.

Anwendungsfall	ohne Authentifizierung	mit Authentifizierung
1. Anwendungsfall «Informationen einmalig» Einmaliges Abrufen und Kommunizieren von Informationen in anonymer Form	• Publizieren von News und Veranstaltungen auf der Website • Aufrufen von Informationen in einfacher und anonymer Form beim öffentlichen Organ • Aufrufen von Informationen in anonymer Form, wie Gemeindenews, Abfallkalender (anonym), Veranstaltungen, Schulferien • Download von Formularen, Dokumente, Erlassen, Merk- und Infoblättern usw. • …	• n/a

Anwendungsfall	ohne Authentifizierung	mit Authentifizierung
2. Anwendungsfall «Informationen wiederkehrend» Wiederkehrendes Abrufen und Empfangen von Informationen in anonymer Form	• Abonnieren von Informationen, z.B. einem E-Mail-Newsletter • …	• n/a
3. Anwendungsfall «Informationen personalisiert» Kommunikation durch Behörde in personalisierter Form	• n/a	• Wiederkehrende (häufigere) Bestellung • Gemeindenews und Veranstaltungen personalisiert • Abonnieren von personalisierten Informationen und Events, bei Angabe von Interessen, Ort usw., wie Gemeindenews, Abfallkalender, Veranstaltungen, Schulferien • Stundenplan der Schule individuell pro Kind zusammengestellt • Download von vorausgefüllten Formularen • …
4. Anwendungsfall «Geschäft mit Behörde einfach» Einfache Geschäfte und Kommunikation mit Behörde, z.B. Anfragen, Bestellungen, Meldungen usw.	• Meldung über Zustand kommunale Infrastruktur (Strassenlaterne geht nicht) • Frage an ein Amt (Datenschutzfrage an DSB) • Bestellung Gemeindechronik • Bestellung Parkkarte • Bestellung SBB-Tageskarte • Anmeldung für Termin Fahrzeugprüfung • …	• Bestellung Parkkarte mit Übernahme der Daten aus der alten Bestellung/Auswahl des von mir eingelösten Fahrzeugs • Anmeldung für Termin Fahrzeugprüfung mit Übernahme der Daten aus der alten Prüfung/Auswahl des von mir eingelösten Fahrzeugs • Bestellung SBB-Tageskarte mit Übernahme der Adressdaten • eUmzug, Melden eines Wohnortwechsels • …
5. Anwendungsfall «Geschäft mit Behörde komplex» Austausch Daten im Rahmen eines Antragsverfahren Interaktion und Zusammenarbeit mit der Behörde	• n/a	• Wiederkehrende Interaktion zwischen Einwohnerin/Einwohner und Behörde: • Bewilligungsverfahren (z.B. Arbeitsbewilligung) • Eingabe und Verwaltung von Baugesuchen • Eingabe der Steuererklärung • Beantragen von Sozialhilfe, Stipendien • …

Tabelle 4. Übersicht Anwendungsfälle mit/ohne Authentifizierung

7 Rechtliche Aspekte

Ob und auf welcher Stufe die Schaffung einer Rechtsgrundlage für den Betrieb eines Online-Portals durch ein öffentliches Organ notwendig ist, hängt von zahlreichen Faktoren ab, wie etwa von den Voraussetzungen des jeweiligen kantonalen Datenschutzgesetzes. Es gilt in jedem Einzelfall die faktische und rechtliche Ausgangslage zu prüfen.

Dazu gehört insbesondere die Beantwortung folgender Fragen:

- Um welche Art von Portal handelt es sich? Welche und wie viele Fachapplikationen werden an das Portal angeschlossen?
- Werden Personendaten im Portal bis zur Abholung durch die Fachapplikation zwischengespeichert?
- Welche Daten (besondere oder normale Personendaten) werden zu welchem/n Zweck(en) von welchen Organen bearbeitet?
- Wie viele Personendaten werden im Portal bearbeitet (Möglichkeit der Bildung von Persönlichkeitsprofilen bei einer grossen Menge von Geschäftsfällen)?
- Aufgrund welcher gesetzlichen Grundlage bearbeitet das öffentliche Organ die Fachapplikationsdaten?

Aus den Antworten auf diese Fragen beziehungsweise aufgrund der Umstände des Einzelfalls ergeben sich Inhalt, Bestimmtheit und Normstufe einer allfälligen Rechtsgrundlage. Der Erlass der Rechtsgrundlage ist nach der Ausgestaltung des Portals zu richten.

Betreibt eine Amtsstelle alleine ein Portal, das nur die von dieser Amtsstelle bearbeiteten Daten enthält, ist dafür keine Rechtsgrundlage notwendig, wenn die Datenbearbeitung von den gesetzlich umschriebenen Aufgaben umfasst ist. Sobald das Online-Portal Daten von mehreren Amtsstellen enthält, verschiedene Amtsstellen auf die Daten im Portal zugreifen können oder eine stärkere Authentifizierung vorgesehen ist, muss dafür eine Rechtsgrundlage bestehen. Dabei ist insbesondere die Verantwortung zu regeln.

Soll durch die Portallösung ein Datenaustausch zwischen verschiedenen Amtsstellen stattfinden, der nicht durch die bereits bestehende gesetzliche Grundlage gedeckt ist, bedarf dies den Erlass einer neuen Rechtsgrundlage.

Der Erlass einer Rechtsgrundlage kann dem Ausbau des Portals entsprechend auch schrittweise erfolgen, indem zunächst eine interne Regelung, dann eine Verordnung und bei Ausbau des Portals schliesslich ein Gesetz im formellen Sinne erlassen wird. Es ist jedoch zu empfehlen, dass bei einem späteren, aber von Anfang an geplanten Ausbau des Portals zu Beginn ein Gesetz im formellen Sinn erlassen wird.

Im Zusammenhang mit Online-Portalen sind aus datenschutzrechtlicher Sicht unter anderem folgende Themen zu klären:

- Identifikator und dessen (verwaltungsinterne) Verwendung
- Im Portal bearbeitete Personendaten: Aus der Rechtsgrundlage muss hervorgehen, welche Personendaten im Online-Portal bearbeitet werden.
- Zuständigkeiten
- Verantwortung und Haftung
- Zugriffsrechte
- Informationsaustausch zwischen verschiedenen öffentlichen Organen über das Portal

- Zwischenspeicherung von Personendaten im Portal
- Löschung der Daten und des Kontos (Fälle (z.B. Tod), Modalitäten)

Diese Themen müssen je nach Ausgestaltung des Portals in einem Gesetz im formellen Sinne festgehalten werden. Es ist in jedem Fall sinnvoll und aus datenschutzrechtlicher Sicht angezeigt, verbindliche verwaltungsinterne Regelungen zu schaffen, die sich mit den wichtigsten Themen rund um das jeweilige Portal auseinandersetzen.

Ein Beispiel für ein Behördenportalgesetz findet sich unter folgendem Link: Gesetz über ein zentrales elektronisches Behördenportal des Kantons Basel-Stadt.

8 Organisatorische und technische Massnahmen

Um die Informationssicherheit eines Portals gewährleisten zu können, sind zahlreiche organisatorische und technische Anforderungen, zu erfüllen. Die grundlegenden Schutzziele (Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit und Integrität) sind mit geeigneten Schutzmassnahmen sicherzustellen. Die Massnahmen sind auf Basis einer regelmässigen Risikoanalyse, nach dem Stand der Technik und nach anerkannten Standards zu definieren. Die Verantwortlichkeiten für die Risikoanalyse, -bewertung und die Massnahmendefinitionen sind im Sinne einer fachlichen Gesamtverantwortung klar zu regeln. Die Grundsätze Privacy by Design und Privacy by Default sind konsequent umzusetzen.

Beim Aufbau und Betrieb eines Portals sind insbesondere die folgenden Punkte zu beachten:

- Die Prozesse und Abläufe für die Benutzerverwaltung und Authentifizierung sind gemäss den Anforderungen des Geschäftsprozesses zu wählen und umzusetzen.
- Die Übermittlung von Daten (data in transport) und ihre Aufbewahrung (data at rest), insbesondere von besonderen Personendaten/sensitiver Daten, sind mit geeigneten kryptografischen Verfahren abzusichern.
- Für die Entwicklung ist ein Entwicklungsprozess anzuwenden, der die Informationssicherheit unterstützt.
- Es sind Massnahmen zur Mitigation der Top-10-Sicherheitslücken[1] des Open Web Application Security Projects (OWASP) zu treffen.
- Die Benutzerinnen und die Benutzer sind über die Risiken der Nutzung des Portals aufzuklären.
- Die Zugriffsberechtigungen sind festzuhalten und periodisch zu überprüfen.
- Sicherheitskritische Ereignisse sind zu protokollieren und periodisch auszuwerten.

9 Benutzername als eindeutiger Identifikator

Durch die Einführung eines zentralen Portals müssen sich die Benutzerinnen und Benutzer nur noch mit einer Benutzerkennung/Benutzer-ID anmelden, um auf die einzelnen Fachapplikationen zugreifen zu können. Aus Sicht des Datenschutzes birgt dies ein gewisses Risiko, da die Benutzerkennung/Benutzer-ID pro System und pro Benutzerin/Benutzer eindeutig ist. Somit kann der Benutzername als eine eindeutige Identifizierung über die einzelnen Fachapplikationen verwendet werden (siehe auch Diskussion zur

1 OWASP Top Ten Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Verwendung der AHV-Nummer[2]). Technisch stehen heute Mittel zur Verfügung, die es erlauben, für die jeweilige Fachapplikation eine eigene pseudonymisierte Benutzerkennung/Benutzer-ID zu verwenden. Im Einzelfall ist zu prüfen und das Risiko abzuwägen, ob eine eigene pseudonymisierte Benutzerkennung/Benutzer-ID pro Applikation anzuwenden ist oder ob eine gemeinsame Benutzerkennung/Benutzer-ID verwendet werden kann.

10 Abgrenzungen

10.1 Abgrenzung zu eVoting

Das Thema eVoting (elektronische Stimmabgabe) wird in diesem Dokument ausgeklammert, da beim eVoting speziellere Anforderungen an die Identifizierung, die Authentifizierung, die Autorisierung, den Datenschutz, die Anonymisierung (Stimm- und Wahlgeheimnis) und die Informationssicherheit bestehen als bei einem Einwohnerportal für den Verkehr mit den Behörden. Die Beantwortung der vielen ungeklärten Fragen um eVoting würde den Rahmen des Dokuments sprengen. Für weitere Details sei auf Fachartikel und Diskussionen wie das Essay «Securing Elections»[3] von BRUCE SCHNEIER verwiesen.

10.2 Abgrenzung zu Informationsvermittler (Data Broker)

Im Zuge der fortschreitenden Digitalisierung dürfte auch der elektronische Austausch von amtlichen oder privaten Dokumenten zwischen Staat (kommunalen, kantonalen und Bundesbehörden), Privaten und Benutzerinnen und Benutzer sowohl für amtliche als auch private Geschäfte häufiger gefragt sein, beispielsweise für einen Hypothekarantrag (Steuerauszug) oder für die Steuererklärung (Bankbelege). Für diesen Austausch kommt ein Informationsvermittler zum Einsatz. Die rechtlichen, organisatorischen und technischen Anforderungen an einen Informationsvermittler sind so komplex, dass im Rahmen dieses Dokuments nicht darauf eingegangen wird. Es wird angeregt, das Thema separat zu behandeln.

---

2 privatim, Verwendung der AHV-Nummer mit hohen Risiken verbunden, 16. Oktober 2017, http://www.privatim.ch/de/verwendung-der-ahv-nummer-mit-hohen-risiken-verbunden/

3 BRUCE SCHNEIER, Securing Elections, 10. Mai 2017, https://www.schneier.com/blog/archives/2017/05/securing_electi.html

11 Übersicht eGovernment-Anwendungen CH

Die nachfolgende Tabelle enthält die Übersicht der aktuellen und bekannten eGovernment-Anwendungen auf kantonaler Ebene in der Schweiz. Diese Übersicht ist nicht abschliessend.

Öffentliches Organ	**Beschreibung**	**Identifizierung/ Authentifizierung**	**Anwendungsfall (1, 2, 3, 4, 5)**	**Status**
DSB-Website	Websites der DSB mit Informationen, Merkblättern und Kontaktformular	• Anonym	1	Online
Kanton Zug (Zuglogin)	Online-Zugang zu den Verwaltungsgeschäften und -daten	• Eindeutige Identifikationsnummer • mTAN • Suisse ID	3, 4, 5	Online, Steuern ab 2018
Stadt Zug	Bürger-ID auf Basis einer Blockchain	• Blockchain	Details sind noch nicht bekannt.	Online
Kanton Schaffhausen	Mit der Firma Procivis soll eine Bürger-ID auf Basis einer App («eID+») eingeführt werden.	• App, in der die ID gespeichert wird.	3, 4, 5	Online, seit Dezember 2017
Steuerportal ZH	Online-Steuerportal des Kantons Zürich	• Registration mittels Zugangscode • Suisse ID • PW + mTAN	5	Online
eUmzug	eUmzug – der elektronische Umzug	• Melden des Wohnungswechsels	4	Online
eRechnung LU	Elektronische Übermittlung vom und zum Kanton Luzern	• Rechnungsangaben	4	Online
eBAGE+ LU	Abwicklung Baurechtsgesuche	• Online-Formular	5	Online
Kantonale Steuerbehörde	Online-Steuerportal des Kantons Bern	• Registration mittels brieflich zugestellten Zugangsdaten und ID-Code	5	Online
Kanton Bern	BE-Login: elektronische Plattform des Kantons Bern für ausgewählte Dienste	• Registrierungsprozess mit E-Mail-Adresse, Passwort, fak. ID oder Pass • Sicherheitsmerkmal mTAN oder Codekarte für Dienste mit Sicherheitsstufe 2	4, 5	Online

Öffentliches Organ	**Beschreibung**	**Identifizierung/ Authentifizierung**	**Anwendungs-fall (1, 2, 3, 4, 5)**	**Status**
Dienstleistungen Abraxas (inkl. ehemals VRSG) (diverse Gemeinden ZH)	Diverse Online-Dienstleistungen: • FD Finanzen und Debitoren • FD eRechnung • VI Inkasso- und Verlustschein-bewirtschaftung • SN neue Steuern • ZP ZüriPrimo • Loganto Einwohner • WEG Wasser, Elektrizität und Gas	• Registration mittels AHV- oder Registernummer • Benutzername und Passwort • Suisse ID	3, 4, 5	Online

Tabelle 5: Übersicht und Klassifizierung eGOV-Anwendungen