IIIIII KANTON solothurn

# *Regierungsratsbeschluss*

vom 25. August 2020

Nr. 2020/1197

**Verordnung über das Behördenportal (BehöPV)**

---

## 1. Ausgangslage

Am 6. Mai 2020 hat der Kantonsrat das Gesetz über das Behördenportal (BehöPG) beschlossen (KRB Nr. RG 0238/2019). Das Gesetz regelt die Organisation, den Betrieb und die Nutzung des elektronischen Behördenportals des Kantons Solothurn sowie die Grundsätze von weiteren kantonalen E-Government-Lösungen. Einzelne Gesetzesbestimmungen bedürfen der Konkretisierung auf Verordnungsstufe.

## 2. Erwägungen

2.1 Erläuterungen zu den einzelnen Verordnungsbestimmungen

**Kapitel 1, Allgemeine Bestimmungen**

### § 1, Zweck des Behördenportals

Im Behördenportal (im Folgenden Portal) wird den Bürgerinnen und Bürgern, der Wirtschaft und der öffentlichen Hand (Bund, andere Kantone, Gemeinden) ein vielfältiges Angebot an elektronischen Dienstleistungen zur Verfügung gestellt. Privatpersonen und Unternehmen können die wichtigsten Amtsgeschäfte auf elektronischem Weg abwickeln und die Kommunikationsprozesse zwischen Privatpersonen oder Unternehmen einerseits und Behörden andererseits werden optimiert (§ 7 BehöPG). Die Schwerpunkte für die elektronische Geschäftsabwicklung sind in der E-Government-Strategie 2018 festgelegt worden (siehe Kapitel 5.2 der E-Government-Strategie 2018).

§ 1 führt die wichtigsten Tätigkeiten auf, die auf elektronischem Weg über das Portal ausgeführt werden können. Die Übermittlung elektronischer Eingaben an die Behörden und der Erhalt behördlicher Korrespondenz in elektronischer Form sind über das Portal möglich (Buchstaben a und b). Privatpersonen und Unternehmen können amtliche Dokumente über das Portal bestellen und beziehen (Buchstabe c) und auf elektronischem Weg Meldepflichten erfüllen (Buchstabe d). Die Auflistung ist nicht abschliessend.

Wichtige Beispiele für die elektronische Geschäftsabwicklung sind (siehe Kapitel 5.2 der E-Government-Strategie 2018 sowie Botschaft und Entwurf des Regierungsrates vom 17. Dezember 2019, RRB Nr. 2019/2035, Seite 16/17):

- Bewilligungsverfahren (Aufenthalts- und Niederlassungsbewilligungen, Arbeitsbewilligungen, Bewilligungen für Gewerbebetriebe, Anlassbewilligungen);

- Erfüllen von Meldepflichten (Mutationsmeldungen an das Handelsregister, An- und Abmeldung von Fahrzeugen);

– Erfüllen von Deklarationspflichten (Einreichung der Steuererklärung [Selbstdeklaration von Einkünften und Vermögen]);

– Bestellung und Bezug von amtlichen Dokumenten (Beglaubigungen, Kopien öffentlicher Urkunden).

## § 2, Aufbau des Behördenportals

Damit das Portal funktionsfähig ist, müssen gewisse technische und infrastruktur-bezogene Komponenten vorhanden sein. In § 2 werden die erforderlichen Komponenten des Portals definiert. Mit diesen Komponenten wird sichergestellt, dass die elektronische Geschäftsabwicklung über ein E-Konto erfolgt, dass die Nutzerinnen und Nutzer authentifiziert werden, dass nur autorisierte Nutzerinnen und Nutzer und nur autorisierte Mitarbeitende der Behörden auf das Portal Zugriff haben, dass die Fachanwendungen für die Bearbeitung der Geschäftsfälle in das Portal integriert werden und dass eine ausreichende technische Sicherheitsinfrastruktur sichergestellt wird.

– Zum E-Konto (Buchstabe a): Wer das Portal nutzen will, muss über ein E-Konto verfügen. Dieses E-Konto dient den Nutzerinnen und Nutzern zur Abwicklung der Geschäfte.

– Zum Authentisierungsdienst (Buchstabe b): Unter Authentifizierung wird der Nachweis der Identität mittels eines technischen Verfahrens verstanden. Durch den Authentisierungsdienst wird sichergestellt, dass die Nutzerinnen und Nutzer für jeden Geschäftsgang authentifiziert werden. Abhängig vom Schutzbedarf der Daten, welche bei den einzelnen Geschäftsarten bearbeitet werden, sind unterschiedliche Vertrauensstufen definiert (siehe auch Ausführungen zu § 6).

– Zum Autorisierungsdienst (Buchstabe c): Unter Autorisierung wird die Zuweisung und Überprüfung von Zugriffsrechten auf Fachanwendungen und Dienstleistungen für eine bestimmte Identität verstanden. Der Autorisierungsdienst sorgt einerseits dafür, dass die Nutzerinnen und Nutzer des Portals ausschliesslich auf ihre eigenen Daten zugreifen können. Andererseits wird durch den Autorisierungsdienst sichergestellt, dass nur autorisierte Mitarbeitende der kantonalen Verwaltung Zugriff auf die an das Portal angeschlossenen Dienste haben.

– Zum Dienst für die Integration von Fachanwendungen (Buchstabe d): Das Erfassen, Aufzeichnen, Verändern, Archivieren und Vernichten der Daten erfolgt nicht im Portal, sondern in den jeweiligen Fachanwendungen (beispielsweise Axioma, Kompass, CARI, eTax). Damit die ausgefertigten Unterlagen zur Abholung über das Portal bereitgestellt werden können, müssen die Fachanwendungen in das Portal integriert werden.

– Zur technischen Infrastruktur (Buchstabe e): Eine ausreichende technische Sicherheitsinfrastruktur umfasst sowohl die technischen Mittel zum Betrieb des Portals als auch die technischen Massnahmen zum Schutz der Daten und zur Gewährleistung einer verschlüsselten Kommunikation.

## Kapitel 2, E-Konto

### § 3, Daten im persönlichen E-Konto

Zu Absatz 1:

Für die Eröffnung eines persönlichen E-Kontos müssen die Nutzerinnen und Nutzer über eine SwissID oder eine andere vom Regierungsrat anerkannte elektronische Identität verfügen. Die SwissID ist eine von der Swiss Sign Group AG (im Folgenden SwissSign) herausgegebene digitale Identität. Diese ermöglicht den SwissID-Inhaberinnen und -Inhabern einen einfachen und sicheren Zugang zu verschiedenen Onlinedienstleistungen. Die SwissID ist persönlich und nicht übertragbar.

Die SwissID wird für verschiedene Sicherheitsniveaus angelegt. Es wird unterschieden zwischen «selbstdeklariert» und «verifiziert». Die vier Sicherheitsstufen (Level of Trust, LoT) präsentieren sich wie folgt:

- LoT 0: selbstdeklariert; Bei der Selbstdeklaration ist die SwissID-Inhaberin bzw. der SwissID-Inhaber für die Richtigkeit der von ihm angegebenen Daten verantwortlich.

- LoT 1: geprüfte Identität «niedrig»; Die Prüfung erfolgt mittels eines Smartphones mit der SwissID-App.

- LoT 2: geprüfte Identität «substantiell»; Die Prüfung erfolgt durch persönliche Vorsprache bei der Gemeinde- oder Stadtverwaltung.

- LoT 3: geprüfte Identität «hoch»; Diese Identität wird zurzeit noch nicht angeboten (siehe dazu auch die Ausführungen zu § 6).

Das Anlegen eines SwissID-Kontos erfolgt kostenlos. Nach erfolgreicher Eröffnung des SwissID-Kontos können die SwissID-Inhaberinnen und SwissID-Inhaber die digitale Identität grundsätzlich kostenlos nutzen. Die SwissID-Inhaberinnen und SwissID-Inhaber haben jedoch diejenigen Kosten zu tragen, die für die Datenverbindung anfallen, wie beispielsweise die Kosten des Mobilfunkanbieters, die Kosten für die Hard- und Software oder die Kosten für den Internetzugang[1]).

Die Herausgeberin der SwissID, die SwissSign, ist ein Joint Venture aus staatsnahen Betrieben, Finanzunternehmen, Versicherungsgesellschaften und Krankenkassen (SBB, Schweizerische Post, Swisscom, Banque Cantonale de Genève, Credit Suisse, Entris Banking, Luzerner Kantonalbank, Raiffeisen, Six Group, UBS, Zürcher Kantonalbank, Axa, Bâloise, CSS, Helvetia, Mobiliar, SWICA, Swiss Life, Vaudoise und Zürich)[2]).

Zurzeit der Inbetriebnahme des Portals steht die SwissID als elektronische Identität im Vordergrund. Sobald weitere anerkannte Identitäten zur Verfügung stehen – insbesondere zu denken ist an die nach den Vorschriften des neuen Bundesgesetzes über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID) vom 27. September 2019 anerkannten elektronischen Identitäten – können diese ebenfalls zugelassen werden. Der Entscheid darüber, welche elektronischen Identitäten für die Eröffnung des E-Kontos verwendet werden dürfen, obliegt dem Regierungsrat.

---

[1]) Siehe zum Ganzen die Allgemeinen Geschäftsbedingungen (AGB) SwissID, https://www.swissid.ch/de/agb, abgerufen am 28. Juli 2020.

[2]) https://www.swisssign-group.com/, abgerufen am 28. Juli 2020.

Zu Absatz 2:

Im persönlichen E-Konto können weitere Daten erfasst werden, um die Geschäftsabwicklung zu erleichtern. Nützlich sind insbesondere eine Postadresse für den Versand von Unterlagen in Papierform und zusätzliche Telefonnummern für telefonische Rückfragen. Zu den freiwillig zu erfassenden Daten gehört auch die Versichertennummer gemäss Artikel 50c Absatz 1 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) vom 20. Dezember 1946 (SR 831.10). Zudem können Vertretungsverhältnisse und Namen von bevollmächtigten Personen im persönlichen E-Konto erfasst werden.

**§ 4, Daten im nicht-persönlichen E-Konto**

Für die Erstellung eines nicht-persönlichen E-Kontos müssen die natürlichen Personen die identifizierenden Daten der juristischen Person, Personengesellschaft oder Einzelunternehmung erfassen (§ 16 Abs. 3 Bst. a BehöPG). Diese Daten müssen auf Verordnungsstufe konkretisiert werden. In § 4 BehöPV wird geregelt, welche identifizierenden Daten einer juristischen Person, Personengesellschaft oder Einzelunternehmung zwingend erfasst werden müssen.

Zu Absatz 1:

Gemäss Artikel 927 Absatz 1 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht; OR) vom 30. März 1911 (SR 220) wird in jedem Kanton ein Handelsregister geführt. Die Handelsregisterverordnung (HRegV) vom 17. Oktober 2007 (SR 221.411) regelt den Inhalt der Eintragungen (Art. 929 Abs. 1 OR). Zu den Daten der **juristischen Personen und Personengesellschaften des Privatrechts** gehören insbesondere die Firma, die Unternehmens-Identifikationsnummer (UID), der Sitz oder das Rechtsdomizil, die Rechtsform sowie der Zeitpunkt der Statuten, der Gründung oder des Beginns einer Gesellschaft (siehe 3. Titel HRegV). Bei den juristischen Personen und Personengesellschaften des Privatrechts genügen die Firma oder der Name, die Rechtsform und der Sitz zur Identifikation. Diese Daten müssen im nicht-persönlichen E-Konto erfasst werden.

Bei den **juristischen Personen des öffentlichen Rechts** sind je nach Organisationsform unterschiedliche Angaben zur Identifikation erforderlich. Bei einem Grossteil der öffentlich-rechtlichen Körperschaften, nämlich bei den Einwohnergemeinden, den anderen Kantonen und den Bundesbehörden, muss nur der Name im nicht-persönlichen E-Konto erfasst werden. Bei den Zweckverbänden, den öffentlich-rechtlichen Unternehmen und Anstalten mit eigener Rechtspersönlichkeit und den öffentlich-rechtlichen Stiftungen muss zusätzlich die Rechtsform erfasst werden.

Bei den **Einzelunternehmen** müssen Firma oder Name, Rechtsform und Sitz im nicht-persönlichen E-Konto erfasst werden. Diese Angaben werden auch im Handelsregister geführt (siehe 3. Titel HRegV).

Zu Absatz 2, 3 und 4:

Damit die Behörden überprüfen können, ob eine natürliche Person berechtigt ist, für eine juristische Person, Personengesellschaft oder Einzelunternehmung zu handeln, muss die natürliche Person ihre Vertretungsberechtigung nachweisen und einen Identitätsnachweis erbringen (Abs. 2).

Die Vertretungsberechtigung muss im Zeitpunkt der Kontoeröffnung bestehen. Die Vertretungsberechtigung kann sich aus einer Funktion oder aus einer ausdrücklichen schriftlichen Vollmacht ergeben. Bei den juristischen Personen und Personengesellschaften des Privatrechts sind die Funktion und die Zeichnungsart der vertretungsberechtigten Personen im Handelsregis-

ter eingetragen. Im nicht-persönlichen E-Konto genügt somit der Vermerk «Handelsregister» als Nachweis der Vertretungsberechtigung. Bei den Einzelunternehmen sind die Firmeninhaberinnen und Firmeninhaber als alleinige Eigentümer zur Vertretung berechtigt. Im nicht-persönlichen E-Konto genügt somit der Vermerk «Firmeninhaberin oder Firmeninhaber» als Nachweis der Vertretungsberechtigung. Bei den juristischen Personen des öffentlichen Rechts ergibt sich die Vertretungsberechtigung in der Regel aus der amtlichen Funktion, weshalb diese im E-Konto angegeben werden kann. Im Falle einer ausdrücklichen schriftlichen Vollmacht muss die Vollmacht eingereicht werden. Im nicht-persönlichen E-Konto wird der Vermerk «Vollmacht» angebracht.

Der Identitätsnachweis der vertretungsberechtigten Person wird in elektronischer Form durch die SwissID oder eine andere vom Regierungsrat anerkannte elektronische Identität erbracht (Abs. 4). Der Nachweis der Identität kann nicht mit Papierdokumenten wie einer Kopie des Reisepasses, der Identitätskarte oder des Führerausweises erbracht werden.

Zu Absatz 5:

Im nicht-persönlichen E-Konto können freiwillig weitere Daten erfasst werden, um die Geschäftsabwicklung zu erleichtern. Dazu gehören die Postadresse für den Versand von Unterlagen in Papierform oder zusätzliche Telefonnummern für telefonische Rückfragen. Damit weitere natürliche Personen auf das nicht-persönliche E-Konto zugreifen können, können entsprechende Zugriffsberechtigungen erteilt und die Namen der bevollmächtigten Personen im nicht-persönlichen E-Konto erfasst werden.

**§ 5, Benutzer-Identität (Benutzer-ID)**

Wie bereits ausgeführt, erfolgen das Erfassen, Aufzeichnen, Verändern, Archivieren und Vernichten der Daten nicht im Portal, sondern in den jeweiligen Fachanwendungen (beispielsweise Axioma, Kompass, CARI, eTax). Damit die ausgefertigten Unterlagen zur Abholung über das Portal bereitgestellt werden können, werden die Fachanwendungen in das Portal integriert.

Zu Absatz 1 und 2:

Die Kopplung zwischen der eindeutigen und unveränderlichen Benutzer-Identität (Benutzer-ID) im E-Konto und der entsprechenden Benutzer-Identität in den angebundenen Fachanwendungen wird über die separate Identity-Mapping-Anwendung (ID-Mapping-Anwendung) des Portals gelöst. Dass die Kopplungsinformation weder im Portal noch in den jeweiligen Fachanwendungen, sondern in einer getrennten ID-Mapping-Anwendung gespeichert ist, sorgt für eine höchstmögliche Datensicherheit.

Zu Absatz 3:

Für die Erstellung einer Kopplung in der ID-Mapping-Anwendung sind einerseits identifizierende Daten der Nutzerin oder des Nutzers im E-Konto und andererseits dieselben Daten in der Fachanwendung erforderlich. Stimmen die identifizierenden Daten im E-Konto mit denselben Daten in der Fachanwendung überein, wird die Kopplung hergestellt. Abhängig von der Fachanwendung können bei Bedarf weitere Daten der Nutzerin oder des Nutzers auf ihre Übereinstimmung überprüft werden. Es handelt sich um Angaben, die nur der Nutzerin oder dem Nutzer bekannt sind. Ein Beispiel dafür ist die Steuer-Personen-Nummer. Das nachfolgende Beispiel «Steuerkonto» soll den Prozess veranschaulichen:

> In der Steuerfachanwendung ist die Steuer-Personen-Nummer nur der steuerpflichtigen Person bekannt. Für die Kopplung mit dem eigenen Steuerkonto werden Name, Vorname und Geburtsdatum unveränderbar angezeigt. Die Nutzerin oder der Nutzer (steuerpflichtige Person) wird aufgefordert, die Steuer-Personen-Nummer einzugeben. Alle die-

se Parameter werden von der Fachanwendung auf Korrektheit und Eindeutigkeit geprüft. Ist die Prüfung erfolgreich – stimmen also alle Parameter überein – wird die Kopplung automatisch hergestellt und bleibt bis auf Widerruf für zukünftige Zugriffe auf das Steuerkonto bestehen.

Stimmen die Parameter nicht vollständig überein, wird keine Kopplung hergestellt. Eine Nichtübereinstimmung kann auf einen Schreibfehler beim Namen oder Vornamen oder auf unvollständige Angaben zurückzuführen sein. Deshalb besteht die Möglichkeit einer manuellen Prüfung, welche beispielsweise eine Rückfrage der Mitarbeiterinnen und Mitarbeiter der kantonalen Verwaltung, welche die Geschäfte in der Fachanwendung bearbeiten, bei der Nutzerin oder beim Nutzer beinhalten kann.

Die manuelle Prüfung, Freigabe oder Ablehnung wird durch autorisierte Mitarbeiterinnen und Mitarbeiter der kantonalen Verwaltung des entsprechenden Fachbereichs durchgeführt. Ergibt die manuelle Prüfung eine Übereinstimmung, wird die Kopplung zwischen E-Konto und Fachanwendung in der ID-Mapping-Anwendung erstellt.

Stimmen die ID-Mapping-Parameter der Nutzerin oder des Nutzers mit den Benutzerangaben in der Fachanwendung nicht überein bzw. können die Parameter nicht verifiziert werden, erfolgt keine Freigabe. Der Geschäftsgang wird unterbrochen. Die Nutzerin oder der Nutzer wird darüber informiert, dass das Geschäft nicht in elektronischer Form abgewickelt werden kann.

Für Fachanwendungen, bei welchen das automatische Koppeln generell nicht möglich ist (es gibt keine eindeutigen Parameter, die Nutzerin oder der Nutzer kennt die Parameter nicht oder die automatische Kopplung ist aus Gründen des Datenschutzes nicht gestattet), darf die Kopplung ausschliesslich manuell vorgenommen werden. Die manuelle Kopplung wird analog zur nicht erfolgreichen automatischen Prüfung durch die autorisierte Mitarbeiterin oder den autorisierten Mitarbeiter der kantonalen Verwaltung geprüft und entsprechend freigegeben oder abgelehnt.

**§ 6, Authentisierung**

Die Nutzerinnen und Nutzer haben sich für jeden Geschäftsgang zu authentisieren (§ 18 Abs. 1 BehöPG). Abhängig vom Schutzbedarf der Daten, welche bei den einzelnen Geschäftsarten bearbeitet werden, müssen unterschiedliche Vertrauensstufen definiert werden (§ 18 Abs. 2 BehöPG).

Zu Absatz 1:

Die Authentisierung der Nutzerinnen und Nutzer erfolgt über die SwissID nach den von der SwissSign definierten Prozessen oder über eine andere vom Regierungsrat anerkannte elektronische Identität.

Zurzeit der Inbetriebnahme des Portals steht die SwissID als Authentisierungsmittel im Vordergrund. Sobald weitere anerkannte Authentisierungsmittel zur Verfügung stehen – insbesondere zu denken ist an die nach den Vorschriften des E-ID-Gesetzes anerkannten elektronischen Identitäten – können weitere Authentisierungsmittel zugelassen werden. Der Entscheid darüber, welche elektronischen Identitäten für die Authentisierung verwendet werden dürfen, obliegt dem Regierungsrat.

Zu Absatz 2:

Im Zusammenhang mit Authentifizierungsfragen wird auf die Standards des Vereins eCH abgestellt. Der Verein eCH fördert E-Government in der Schweiz, indem er verschiedene Leistungen erbringt. eCH erleichtert die elektronische Zusammenarbeit zwischen Behörden und von Behör-

den mit Privaten, Unternehmen, Organisationen sowie Lehr- und Forschungsanstalten, indem er entsprechende Standards verabschiedet und koordiniert. eCH fördert zudem die Umsetzung internationaler Standards (siehe Art. 2 und 3 der Statuten vom 10. April 2014[1])). Massgebend für die Vertrauensstufen ist das Qualitätsmodell zur Authentifizierung von Subjekten (Standard eCH-0170; aktuelle Version 2.0 vom 13. September 2017[2]).

Zu Absatz 3:

In Anwendung des Qualitätsmodells zur Authentifizierung von Subjekten (Standard eCH-0170) gelten die folgenden vier Vertrauensstufen:

- Stufe 1: kein oder minimales Vertrauen;
- Stufe 2: geringes Vertrauen;
- Stufe 3: beträchtliches Vertrauen;
- Stufe 4: hohes Vertrauen.

Die Vertrauensstufen 1 bis 4 zeichnen sich im Wesentlichen durch folgende Charakteristika aus (siehe eCH-0170, Kapitel 4.1[3])):

Vertrauensstufe 1:

- Alle vorhandenen Informationen zur Identität wurden von den Nutzerinnen und Nutzern selbst deklariert und bei der Registrierung nicht überprüft.
- Die Authentifizierung erfordert nur einen Authentifizierungsfaktor, mit dem mit geringer Gewissheit sichergestellt werden kann, dass den Nutzerinnen und Nutzern beim wiederholten Zugriff dieselbe Identität zugeordnet werden kann.

Vertrauensstufe 2:

- Bei der Registrierung wurden die Angaben der Nutzerinnen und Nutzer mit Hilfe von Beweismitteln überprüft. Die Nutzerinnen und Nutzer müssen dazu mindestens online anwesend sein.
- Die Nutzerinnen und Nutzer müssen sich mit mindestens zwei verschiedenen Single-Factor Authenticators oder mit einem Multi-Factor Authenticator anmelden, damit die Gewissheit erhöht wird, dass den Nutzerinnen und Nutzern beim wiederholten Zugriff dieselbe Identität zugeordnet werden kann.

Vertrauensstufe 3:

- Bei der Registrierung wurden die Angaben der Nutzerinnen und Nutzer mit Hilfe von Beweismitteln stark validiert und die Kopie eines Beweismittels mit körperlichen Merkmalen erstellt. Die Nutzerinnen und Nutzer müssen mindestens online anwesend sein.

---

[1]) https://www.ech.ch/de/der-verein, abgerufen am 28. Juli 2020.
[2]) https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=2.0, abgerufen am 28. Juli 2020.
[3]) https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=2.0, abgerufen am 28. Juli 2020.

- Die Nutzerinnen und Nutzer müssen sich mit einem hardware-basierten Multi-Factor Authenticator anmelden.

Vertrauensstufe 4:

- Bei der Registrierung müssen die Nutzerinnen und Nutzer physisch oder Virtual-In-Person anwesend sein. Diese Präsenz wird dokumentiert. Die Beweismittel müssen staatlich anerkannt sein und biometrische Merkmale enthalten, die überprüft werden müssen.

- Bei der Authentifizierung müssen sich die Nutzerinnen und Nutzer mit einem hardware-basierten Multi-Factor Authenticator, welcher zertifiziert sein muss, anmelden.

- Als höchste Stufe bietet die Vertrauensstufe 4 ein sehr hohes Mass an Vertrauen in die beanspruchte Identität der Nutzerinnen und Nutzer.

Weil die Authentisierung mit der SwissID zurzeit im Vordergrund steht, wird in der Verordnung festgehalten, mit welchen Sicherheitsstufen der Swiss ID (Level of Trust; LoT) die Vertrauensstufen gemäss eCH-0170 erreicht werden können. Die Vertrauensstufen gemäss eCH-0170 entsprechen den vier Sicherheitsstufen (LoT) der Swiss ID:

- LoT 0: selbstdeklariert; Bei der Selbstdeklaration ist die SwissID-Inhaberin bzw. der SwissID-Inhaber für die Richtigkeit der von ihm angegebenen Daten verantwortlich.

- LoT 1: geprüfte Identität «niedrig»; Die Prüfung erfolgt mittels eines Smartphones mit der SwissID-App.

- LoT 2: geprüfte Identität «substantiell»; Die Prüfung erfolgt durch persönliche Vorsprache bei der Gemeinde- oder Stadtverwaltung.

- LoT 3: geprüfte Identität «hoch»; Diese Identität wird noch nicht angeboten.

Der Zusammenhang zwischen den Vertrauensstufen gemäss eCH-0170 und den Sicherheitsstufen der Swiss ID präsentiert sich wie folgt:

| **Vertrauensstufen Standard eCH-0170** | **Sicherheitsstufen SwissID** |
|---|---|
| Stufe 1:<br>kein oder minimales Vertrauen | LoT 0:<br>selbstdeklariert |
| Stufe 2:<br>geringes Vertrauen | LoT 1:<br>geprüfte Identität «niedrig» |
| Stufe 3:<br>beträchtliches Vertrauen | LoT 2:<br>geprüfte Identität «substantiell» |
| Stufe 4:<br>hohes Vertrauen | LoT 3:<br>geprüfte Identität «hoch» |

Sobald andere elektronische Identitäten verfügbar sind, muss definiert werden, inwiefern die Sicherheitsstufen der anderen elektronischen Identitäten den Vertrauensstufen gemäss eCH-0170 entsprechen.

Zu Absatz 4:

Abhängig vom Schutzbedarf der Daten, welche bei den einzelnen Geschäftsarten bearbeitet werden, haben die angeschlossenen Stellen zu definieren, welche Vertrauensstufe für die einzelnen Geschäftsarten erforderlich ist. Der Entscheid über die erforderliche Vertrauensstufe muss spätestens in jenem Zeitpunkt gefällt werden, in welchem eine Geschäftsart über das Portal zur Verfügung gestellt wird. Bei den kantonalen Verwaltungsbehörden entscheidet die jeweilige Dienststelle (Departement, Amt), welche Vertrauensstufe erforderlich ist. Bei den Gemeinden, den Zweckverbänden und den übrigen der Zusammenarbeit der Gemeinden dienenden öffentlich-rechtlichen Organisationen sowie bei den privatrechtlichen Organisationen und Privatpersonen, die öffentliche Aufgaben erfüllen, entscheidet die zuständige Stelle über die erforderliche Vertrauensstufe.

Erfüllt die elektronische Identität einer Nutzerin oder eines Nutzers die Anforderungen an die erforderliche Vertrauensstufe nicht, wird die Nutzerin oder der Nutzer im Portal darauf aufmerksam gemacht, dass die nötigen Schritte zur Erlangung einer höheren Vertrauensstufe in die Wege geleitet werden müssen.

## § 7, Protokollierung

Zu Absatz 1:

Alle Zugriffe der Nutzerinnen und Nutzer auf das E-Konto werden protokolliert (siehe auch § 19 Absatz 1 BehöPG). Die Zugriffs-Protokollierungen (sogenannte Logs) haben den Zweck, die Nachvollziehbarkeit der Handlungen in den persönlichen und nicht-persönlichen E-Konti zu gewährleisten. Protokolliert wird, welche Nutzerin oder welcher Nutzer den Zugriff ausgeführt hat und zu welchem Zeitpunkt der Zugriff erfolgt ist (Abs. 1). In Anlehnung an § 10 Absatz 4 der Verordnung zum Gesetz über die Einwohnerregister- und die Stimmregisterplattform (VESP) vom 10. November 2015 (BGS 114.4) werden die Protokolle nach 12 Monaten gelöscht (Abs. 2).

## § 8, Verlauf von Transaktionen

Das E-Konto dient den Nutzerinnen und Nutzern zur Abwicklung der Geschäfte (§ 14 Abs. 2 Bst. a BehöPG). Im Modul «Geschäftsmonitor» erhalten die Nutzerinnen und Nutzer einen Überblick über den Verlauf der im E-Konto getätigten Transaktionen.

## § 9, Auflösung des E-Kontos

Die Nutzerinnen und Nutzer haben jederzeit die Möglichkeit, ihr persönliches E-Konto auflösen zu lassen (§ 20 Abs. 1 BehöPG). Verlangt eine Nutzerin oder ein Nutzer die Auflösung des E-Kontos, wird dieses nach maximal 11 Tagen gelöscht (Abs. 1). Um die Auflösung des E-Kontos zu veranlassen, steht den Nutzerinnen und Nutzern im Portal die Funktion «E-Konto auflösen» zur Verfügung. Mit dem Anklicken dieser Funktion («Auflösen-Knopf») können die Nutzerinnen und Nutzer die Auflösung ihres E-Kontos direkt im Portal beantragen.

Mit der Auflösung werden auch alle im E-Konto gespeicherten Daten vollständig gelöscht (Abs. 2). Auch allfällige abonnierte Dienste wie Newsletter-Zustellungen werden eingestellt.

Will eine Nutzerin oder ein Nutzer erneut über das Portal Geschäfte tätigen, muss sie oder er ein neues E-Konto eröffnen. Eine Reaktivierung des alten E-Kontos ist ausgeschlossen. Eine Wiederanmeldung im Portal ist erst nach der Eröffnung eines neuen E-Kontos möglich (Abs. 3 und 4).

## § 10, Nutzungsbedingungen

Zu Absatz 1:

Die wichtigsten Rechte und Pflichten der Nutzerinnen und Nutzer – das kostenlose Nutzungsrecht, die Pflicht zur Eröffnung eines E-Kontos, die Pflicht zur Erfassung bestimmter Daten im E-Konto und das Recht zur jederzeitigen Auflösung des E-Kontos – werden im Behördenportalgesetz geregelt (siehe § 11 Abs. 2 BehöPG, § 14 Abs. 1 BehöPG, § 15 Abs. 1 BehöPG und § 20 Abs. 1 BehöPG). In § 11 BehöPV werden zusätzliche Einzelheiten festgehalten. Dazu gehören:

- die Pflicht zur wahrheitsgemässen Datenerfassung und zur Aktualisierung der erfassten Daten (Buchstabe a);

- die Pflicht zur bestimmungsgemässen Nutzung des Portals (Buchstabe b). Eine missbräuchliche Nutzung kann mit einer behördlichen Auflösung des E-Kontos sanktioniert werden (siehe § 20 Abs. 3 BehöPG). Allfällige strafrechtliche Sanktionen nach dem Schweizerischen Strafgesetzbuch (StGB) vom 21. Dezember 1937 (SR 311.0) bleiben vorbehalten. In Frage kommen insbesondere unbefugte Datenbeschaffung gemäss Art. 143 StGB, unbefugtes Eindringen in ein Datenverarbeitungssystem gemäss Art. 143$^{bis}$ StGB, Datenbeschädigung gemäss Art. 144$^{bis}$ StGB und betrügerischer Missbrauch einer Datenverarbeitungsanlage gemäss Art. 147 StGB.

- die Pflicht, die notwendigen technischen Massnahmen zum Schutz der Informatiksysteme zu treffen. Die Nutzerinnen und Nutzer müssen einen aktuellen Endgeräteschutz installieren. Dazu gehören ein aktuelles Viren- und Spyware-Schutzprogramm zum Schutz vor Viren und Spyware sowie eine aktuelle Firewall zum Schutz vor unerwünschten Netzwerkzugriffen (Buchstabe c);

- die Pflicht zum sorgfältigen Umgang mit den Zugangsdaten, den elektronischen Identifikationsmitteln und der elektronischen Signatur (Buchstabe d). Ein sorgfältiger Umgang ist eine zwingende Vorsichtsmassnahme, damit keine unbefugten Drittpersonen auf das E-Konto zugreifen, im E-Konto Daten ändern oder ohne Wissen der Nutzerinnen und Nutzer Geschäfte über das E-Konto abwickeln.

- die Vorgaben über die Kennwortgestaltung (Buchstabe e).

Zu Absatz 2:

Die Nutzerinnen und Nutzer werden in geeigneter Form über die Nutzungsbedingungen und die Risiken der Nutzung informiert. Die Nutzung des Portals bzw. die Bearbeitung der Daten im E-Konto birgt insbesondere folgende Risiken:

- Durch das versehentliche Löschen eines E-Kontos können die Dokumente, welche im E-Konto zur Abholung bereitgestellt waren, nicht mehr heruntergeladen werden. In einem solchen Fall müssen die Dokumente neu beschafft werden.

- Durch eine fehlerhafte Verarbeitung von Angaben können Informationen oder Dokumente unbeabsichtigt einer falschen Nutzerin oder einem falschen Nutzer zugeordnet werden. Dies kann dazu führen, dass eine Drittperson unberechtigterweise Einsicht in einzelne Informationen oder Dokumente einer Nutzerin oder eines Nutzers erhält.

- Durch fehlerhaftes Einrichten einer Stellvertretung besteht das Risiko, dass einer Drittperson unbeabsichtigt Zugang zu einzelnen Informationen und Dokumenten gewährt wird.

– Durch mangelhafte Sicherheitsmassnahmen am eigenen Informatiksystem nehmen die Nutzerinnen und Nutzer in Kauf, dass ihr System kompromittiert wird und eine Drittperson unberechtigterweise Zugang zu Informationen und Dokumenten erhält.

Zu Absatz 3:

Einzelne Rechte und Pflichten der Nutzer und Nutzerinnen sind auf Gesetzes- und Verordnungsstufe geregelt. Diese Nutzungsbedingungen gelten aufgrund ihres generell-abstrakten Charakters für alle Nutzer und Nutzerinnen, ohne dass es dazu einer Zustimmung bedarf. Einzelne Nutzungsbedingungen werden zusätzlich formuliert. Diesen Nutzungsbedingungen muss zugestimmt werden, bevor das E-Konto eröffnet wird. Aus Gründen der Benutzerfreundlichkeit werden alle Nutzungsbedingungen in einer Übersicht zusammengestellt. Die Nutzer und Nutzerinnen werden aufgefordert, den gesamten Nutzungsbedingungen zuzustimmen, bevor das E-Konto eröffnet. Die Zustimmung erfolgt durch das Setzen des entsprechenden «Häkchens» direkt im Portal.

## Kapitel 3, Zuständigkeiten und Aufgaben der Behörden

### § 12, Departement

Informatik und Telekommunikation gehören gemäss § 9 und Anhang der Verordnung über die Organisation des Regierungsrates und der Verwaltung (RVOV) vom 11. April 2000 (BGS 122.112) zu den Aufgaben des Finanzdepartements.

Die technologische Verantwortung, d.h. die Wahrnehmung der professionellen Informatik-Technologieaufgaben, liegt grundsätzlich beim Amt für Informatik und Organisation (AIO). Das AIO ist die zentrale Anlaufstelle für alle Informatikbelange und ist verantwortlich für die Umsetzung, Beratung und Unterstützung der Departemente sowie den Unterhalt und den Betrieb der zentralen und übergreifenden Informatik- und Kommunikationssysteme (Basisdienstleistungen)[1]).

## Fremdänderungen

### Verordnung über die Organisation des Regierungsrates und der Verwaltung

Im Anhang der Verordnung über die Organisation des Regierungsrates und der Verwaltung (RVOV) vom 11. April 2000 (BGS 122.112) ist der Bereich E-Government beim Aufgabenkatalog der Staatskanzlei nicht aufgeführt. Der Aufgabenbereich der Staatskanzlei wird um den Bereich E-Government ergänzt.

### V-ElÜb

Zu §§ 1 und 2:

Gemäss § 1 Absatz 4 V-ElÜb ist die Verordnung auf die Verfahren vor einer Gemeindebehörde anwendbar, wenn die Gemeinde über einen anerkannten elektronischen Zugang verfügt. Verfügt die Gemeinde über einen solchen Zugang, sind elektronische Eingaben an die Gemeinde möglich (§ 2 Abs. 3 V-ElÜb). Für die Zweckverbände und die übrigen der Zusammenarbeit der Gemeinden dienenden öffentlich-rechtlichen Organisationen gilt dies sinngemäss (§ 1 Abs. 4 Satz 2 und § 2 Abs. 3 Satz 2 V-ElÜb).

---

[1]) https://www.so.ch/verwaltung/finanzdepartement/amt-fuer-informatik-und-organisation, abgerufen am 28. Juli 2020.

Weil beispielsweise die Übermittlung elektronischer Eingaben über die vom Bund anerkannte Zustellplattform IncaMail auch dann möglich ist, wenn die Empfängerin oder der Empfänger (also die Gemeindebehörde) nicht an IncaMail angeschlossen ist, können elektronische Eingaben ohne das Wissen bzw. das Einverständnis der Gemeinde über IncaMail getätigt werden. Da es den Gemeinden jedoch freigestellt ist, ob und in welchen kommunalen Verfahren sie den elektronischen Geschäftsverkehr zulassen, muss in der V-ElÜb präzisiert werden, dass die Verordnungsbestimmungen nur *auf die von der Gemeinde festgelegten Verfahren* anwendbar sind bzw. elektronische Eingaben nur *in den von der Gemeinde festgelegten Verfahren* zulässig sind.

Zusätzlich werden die Bestimmungen zu den anerkannten Zustellplattformen präzisiert.

Zu § $2^{bis}$:

§ 2 regelt in allgemeiner Weise, dass Eingaben in elektronischer Form möglich sind, wenn die Behörde an das Behördenportal des Kantons Solothurn oder eine andere anerkannte Zustellplattform angeschlossen ist.

Auch nach der Inbetriebnahme des Behördenportals ist es nicht möglich, alle Dienstleistungen gleichzeitig in elektronischer Form anzubieten. Es muss deshalb definiert werden, in welchen Verwaltungsverfahren elektronische Eingaben möglich sind – sei es ab Inbetriebnahme des Portals oder zu einem späteren Zeitpunkt.

Zu §§ 11 und 14:

Gemäss § 11 Absatz 1 V-ElÜb werden die behördlichen Dokumente mit einem geregelten elektronischen Siegel im Sinne von Artikel 2 Buchstabe d des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur; ZertES) vom 18. März 2016 (SR 943.03) versehen. Das geregelte elektronische Siegel ermöglicht es der Empfängerin oder dem Empfänger, nachzuvollziehen, dass die Dokumente von der (kantonalen oder kommunalen) Behörde ausgestellt worden sind und nicht mehr verändert wurden. Zudem ist der Erstellungszeitpunkt aus dem Dokument ersichtlich.

Seit Inkrafttreten der V-ElÜb am 1. Juli 2018 wurden weitere Verfahren entwickelt, welche die Authentizität eines Dokuments nachweisen können. Der Kanton Freiburg beispielsweise bietet ein eigenes, benutzerfreundliches Verfahren an. Auf dem behördlichen Dokument erscheint ein QR-Code, der gescannt werden kann. Beim Scannen wird angezeigt, wann und von welcher Behörde das Dokument ausgestellt worden ist. Ein solches Verfahren ist ebenfalls geeignet, die Authentizität eines behördlichen Dokuments nachzuweisen. Solche Verfahren sollen deshalb zusätzlich oder alternativ zum geregelten elektronischen Siegel zur Anwendung gelangen. Die V-ElÜb wird entsprechend angepasst.

Es ist nicht bei jedem behördlichen Dokument erforderlich, die Authentizität nachzuweisen. Beispielsweise kann bei einer Eingangsbestätigung, einem schlichten Antwortbrief und dergleichen auf den Nachweis der Authentizität verzichtet werden. Deshalb wird in der V-ElÜb das Anbringen eines Authentizitätsnachweises nicht mehr für alle behördlichen Dokumente vorgeschrieben. Es ist Sache der Dienststellen, zu entscheiden, welche Dokumente mit einem Nachweis der Authentizität versehen werden.

2.2 Inkrafttreten

Die Verordnung tritt am 1. November 2020 in Kraft, auf den gleichen Zeitpunkt wie das Behördenportalgesetz.

## 3. Beschluss

Der Verordnungstext wird beschlossen.

Andreas Eng
Staatsschreiber

**Beilage**

Verordnungstext

**Verteiler RRB**

Staatskanzlei (2; rol, wyl)
Volkswirtschaftsdepartement
Amt für Gemeinden (2; gro, bae)
Departement des Innern, Rechtsdienst (lw)
Amt für Informatik und Organisation (2; tbu, reg)
Departement für Bildung und Kultur (4; an, gk, dk, dt)
Parlamentsdienste
Staatskanzlei (4) eng, rol, ett, jol (Einspruchsverfahren)
Fraktionspräsidien (5)
GS, BGS

Veto Nr. 447 Ablauf der Einspruchsfrist: 26. Oktober 2020.

**Verteiler Verordnung**

Es ist kein Separatdruck geplant.