



Digitale Postbearbeitung

St.Gallen, 18. Mai 2021

Philipp Egger, Leiter Informatik und Infrastruktur
Marlène Schürch, Juristin Recht und Logistik

Agenda

- Ausgangslage und Ziele
- Prozessuale Umsetzung
- Juristische Umsetzung
- Live-Demo



Eingehende Post beim Kanton St.Gallen

- Täglich rund 3'000 eingehende Briefe beim Kanton St.Gallen (Verwaltung in der Stadt St.Gallen ohne Aussenstellen)
- Rund 2'000 Briefe sind direkt zugestellte Meldungen (Steueramt, Strassenverkehrs- und Schifffahrtsamt, Migrationsamt, Arbeitslosenkasse und RAV)
- Rund 1'000 Briefe unstrukturiert
 - Triage und Feinverteilung durch Postdienst der kantonalen Verwaltung



Ziele des Projekts

- Zentrale Digitalisierung der eingehenden Post
- Beschleunigte Zustellung
- Orts- und zeitunabhängiges Bearbeiten von Post
- Ineinandergreifen des physischen und des digitalen Prozesses
- Digitalisierung der eingehenden Post als Basis für die durchgängige elektronische Geschäftsverwaltung
- Nachverfolgbarkeit der internen Post (insb. Einschreiben)
- Abdeckung der «letzten Meile» durch direkte elektronische Weiterbearbeitung (bspw. GEVER, SAP)

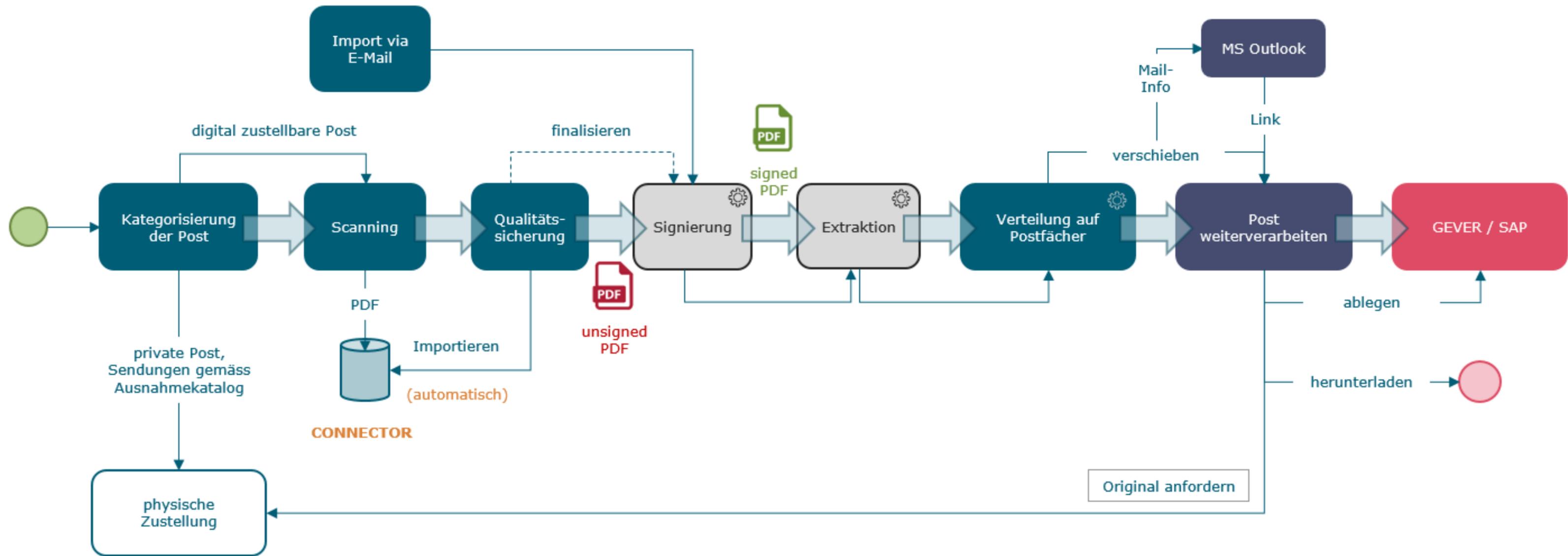


Inhaltliche Anforderungen

- Einfache Weiterleitung der Post
- E-Mail-Notifikation
- Zustellung von Kopien (Wahrung des Document-Ownerships)
- Anfordern des Originals bei Bedarf
- Nachverfolgbarkeit des Verlaufs
- Digitale Unveränderbarkeit der Dokumente
- Schnittstellen an Umsysteme
- Unterstützung durch Dokument-Extraktion



Prozessuale Umsetzung



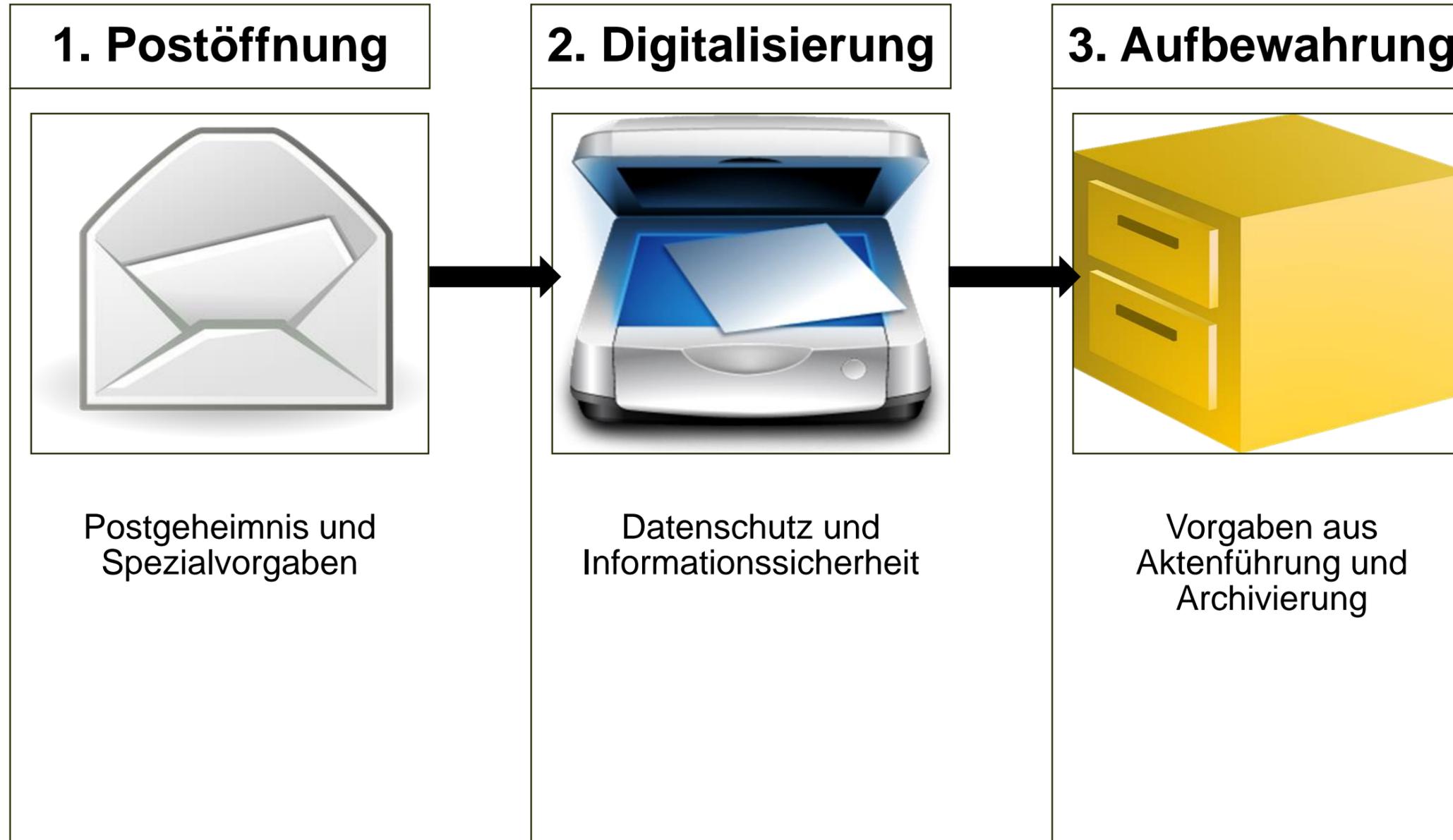
Ablauf Scanning und Zusammenspiel analog und digital

- Video zur digitalen Postbearbeitung
- https://e.video-cdn.net/video?video-id=BFRhVnBxghfFXCg4wwj9FJ&player-id=7M3vLiXUkBzmN5_zc1eA4m&channel-id=78573



Juristische Umsetzung

RECHTLICHE ABKLÄRUNGEN



1. Postöffnung

1.1 Verfassungsrechtlicher Schutz des Postgeheimnisses



- Art. 13 Abs. 1 der Bundesverfassung (SR 101):

Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

- BGE 140 I 353, Erw. 8.3:

Ein Grundrechtseingriff liegt auch vor, wenn Randdaten (Angaben über die Absenderin oder den Absender und die Adressatin oder den Adressaten sowie Art, Dauer und Häufigkeit von Kontakten) ausgeforscht werden.

→ Schutz gilt jedoch nur für **private** Post, geschäftliche Post darf zentral geöffnet werden

→ allerdings gibt es auch **geschäftliche Post mit sensitivem Inhalt** (persönlich / vertraulich)

Zur Wahrung des Postgeheimnisses und der Vertraulichkeit sind private Sendungen und geschäftliche Sendungen mit sensitivem Inhalt vor der Öffnung auszusortieren.



1. Postöffnung

1.2 Strafrechtlicher Schutz des Postgeheimnisses



Art. 321^{ter} des Schweizerischen
Strafgesetzbuchs (SR 311.0):

*Die Öffnung einer verschlossenen Sendung durch
einen Beamten, Angestellten oder einer
Hilfsperson einer Organisation, die Post- oder
Fernmeldedienste erbringt, ist verboten.*

Dies gilt jedoch bloss für Organisationen, die
gewerbsmässig Postdienste erbringen

-  **Art. 321^{ter}**¹ Verletzung des Post- und Fernmeldegeheimnisses

Verletzung des Post- und Fernmeldegeheimnisses

¹ Wer als Beamter, Angestellter oder Hilfsperson einer Organisation, die Post- oder Fernmeldedienste erbringt, einem Dritten Angaben über den Post-, Zahlungs- oder den Fernmeldeverkehr der Kundschaft macht, eine verschlossene Sendung öffnet oder ihrem Inhalt nachforscht, oder einem Dritten Gelegenheit gibt, eine solche Handlung zu begehen, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

² Ebenso wird bestraft, wer eine nach Absatz 1 zur Geheimhaltung verpflichtete Person durch Täuschung veranlasst, die Geheimhaltungspflicht zu verletzen.

³ Die Verletzung des Post- und Fernmeldegeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.

⁴ Die Verletzung des Post- und Fernmeldegeheimnisses ist nicht strafbar, soweit sie zur Ermittlung des Berechtigten oder zur Verhinderung von Schäden erforderlich ist.

⁵ Vorbehalten bleiben Artikel 179^{octies} sowie die eidgenössischen und kantonalen Bestimmungen über die Zeugnispflicht und über die Auskunftspflicht gegenüber einer Behörde.



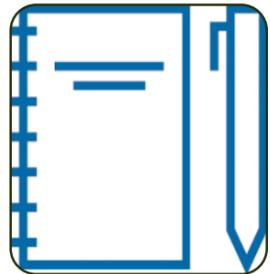
1. Postöffnung

1.3 Spezialrechtliche Öffnungsvorgaben



Art. 3 des Gesetzes über Wahlen und Abstimmungen (sGS 125.3)

→ *Wahrung des Stimmgeheimnisses bei Stimmabgaben*



Art. 30 der Verordnung über das öffentliche Beschaffungswesen (sGS 841.11)

→ *Öffnung von Angeboten bei öffentlichen Ausschreibungen*

→ Diese Sendungen können nicht zentral geöffnet werden und sind ebenfalls vor der Öffnung auszusortieren.

WICHTIG:

Ausnahmen, die vor der Öffnung aussortiert werden, müssen anhand der Adressierung oder des äusseren Erscheinungsbilds der Sendung erkennbar sein.



2. Digitalisierung

2.1 Datenschutz und Informationssicherheit: Rechtsgrundlagen



- **Datenschutzgesetz (sGS 142.1; abgekürzt DSG)**
 - hinreichende Rechtsgrundlage für die Bearbeitung von *Personendaten* (Art. 5 DSG)
 - Vorgaben bei der Bearbeitung durch Dritte (Art. 9 DSG) und evtl. cloud-spezifische Risiken
 - bei hohem Risiko für die Grundrechte: Vorabkonsultation bei der Fachstelle für Datenschutz (Art. 8a und 8b DSG)
- **Verordnung über die Informatiksicherheit (sGS 142.21; nachfolgend IS-Verordnung)**
 - Risikobeurteilung (Art. 6 ff. IS-Verordnung): hoher Schutzbedarf festgestellt
 - Datenklassifizierung (Art. 7 ff. IS-Verordnung)
 - Massnahmenkatalog (Art. 10 IS-Verordnung)
 - Zusammenarbeitsvertrag (Art 19 IS-Verordnung)



2. Digitalisierung

2.1 Datenschutz und Informationssicherheit: technische und organisatorische Massnahmen



- Ausnahme von Sendungen vor der Öffnung an gewisse Empfänger, bei denen erfahrungsgemäss erhöhter Schutzbedarf besteht: **Personaldienst / Fachstelle für Datenschutz**
- **Beschränkung der inhaltlichen Kenntnisnahme** von Sendungen durch die mit der digitalen Postbearbeitung betrauten Personen und Statuierung einer **Geheimhaltungspflicht**
- **Sichtschutz** und **Zutrittsbeschränkung zu Räumlichkeiten**
- Abschluss einer **umfassenden schriftlichen Vereinbarung mit ISDS-Regelungen** zusätzlich zur Rahmenvereinbarung (einschliesslich AGB SIK 2020), u.a. mit Regelungen zum Schlüsselmanagement, Löschung der Daten, Audits usw.



3. Aufbewahrung

Aufbewahrungspflicht von juristisch relevanten Originalen



- Grundsatz: elektronische Aktenführung (GEVER)
- BGer 9C_634/2014 Erw. 6.3.2:
«Eine Streitpartei trägt die Beweislast für die Echtheit der Unterschrift und setzt sich im Falle der Vernichtung der Originalunterschrift nach dem Einscannen dem Risiko aus, dass ihr der Echtheitsbeweis misslingt.»
- Die physischen Sendungen werden 30 Tage sicher aufbewahrt; für ein Jahr besteht eine digitale Sicherheitskopie

- Solange keine rechtssichere elektronische Unterschrift zur Verfügung steht, müssen **sämtliche Dokumente mit Urkundencharakter (juristisch relevante Originale)** als Beweismittel in Papierform aufbewahrt werden.
- Die zuständige Stelle muss für entsprechende Dokumente eine **Nachsendung** innert 30 Tagen seit Versand beantragen.



Rechtliche Regelung

- Dienstanweisungen bei den entsprechenden Dienststellen mit Verankerung gewisser Ausnahmen
 - vor der Öffnung: von aussen erkennbar
 - «persönlich-vertrauliche» Sendungen, darunter fallen
 - private Sendungen
 - geschäftliche Sendungen mit sensitivem Inhalt
 - spezialgesetzliche Ausnahmen (Stimmabgaben, Offerten bei öffentlichen Beschaffungen)
 - gewisse Empfänger: Personaldienst / Fachstelle für Datenschutz
 - nach der Öffnung: praktische Ausnahmen
 - Überformate
 - gebundene Unterlagen usw.
- Organisationsvorschriften GEVER
- schriftlicher Vertrag namentlich betreffend Datenhaltung zwischen Leistungserbringer und –bezüger
- An Stelle von Dienstanweisungen je Dienststelle wird eine übergeordnete Verwaltungsverordnung der Regierung angestrebt.



Live-Demo



E

Egger Philipp



Papierkorb

- https://e.video-cdn.net/video?video-id=BsC92YY_FnCfTUmSLqdKfz&player-id=FR2LXw9KF13cUyVa3MAiHk&channel-id=90361

