

**E-Government-Forum
der öffentlichen Verwaltung
in Schleswig-Holstein**

E-Government und Datenschutz

Lukas Gundermann

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

LD2@datenschutzzentrum.de

Übersicht

- **Frontoffice: Information und Interaktion mit dem Bürger mittels Telekommunikation**
- **Backoffice: Verwaltungsinterne Aspekte, insbesondere Zusammenarbeit mehrerer Stellen, Archivierung**
- **Übergreifende Fragen**
- **Sonderproblem: Authentisierung in Frontoffice und Backoffice**



Frontoffice - Problemfelder

- **Risiken für die Datensicherheit durch Systemöffnung; Gefährdung der Verfügbarkeit des Systems und der Vertraulichkeit und Integrität der Daten**
- **Unzulässige Weitergabe von personenbezogenen Daten; Übermittlung an Unberechtigte bei Interaktionsvorgang**
⇒ **Notwendigkeit der Authentisierung**
- **Risiken der digitalen Datenübertragung: Zusatzinformationen entstehen, die für verschiedene Instanzen zugänglich sind (bug oder feature?)**



Frontoffice - Empfehlungen

- **Einwilligung einholen, wenn elektronisch verwaltet werden soll (Unklarheit im VwVfG)**
- **Herstellen von Transparenz - Bürger müssen wissen, wer was über sie weiß, aber auch auf technische Risiken hingewiesen werden**
- **Datensparsamkeit: Erhebung personenbezogener Daten vermeiden, z.B. bei Bestellung von Newslettern, Abruf von allg. zugänglichen Informationen; Zurückhaltende Protokollierung von Geschäftsvorfällen**
- **Zurückhaltung bei der Veröffentlichung der Daten der Mitarbeiter - nur mit Einwilligung zulässig**



Backoffice - Problemfelder

- **Problem digitaler Archivierung, Verfall und künftige Inkompatibilität der Speichermedien**
- **Zentralisierung der Datenbestände, Gefahr der Erosion der Zweckbindung**
- **Verantwortungsdiffusion aufgrund unklarer Regelungen der Zusammenarbeit mehrerer Stellen**



Backoffice - Empfehlungen

- **Insbes. bei Zusammenwirken mehrerer Stellen oder Weitergabe der e-Akte an andere Behörden: Beschränkung der Zugriffsmöglichkeiten auf die Daten auf das jeweils Erforderliche**
- **Protokollierung wichtiger Verfahrensschritte**
- **Automatisierung der Löschung**
- **Auswertungen außerhalb des eigentlichen Speicherzwecks nur anonymisiert oder pseudonymisiert**



Übergreifende Fragen

- **Verschlüsselung sensibler Daten bei der Übertragung und ggf. Speicherung**
- **Nichtbeherrschbarkeit der Daten, wenn technische Dienstleister eingeschaltet sind; sorgfältige Auswahl, vertragliche Absicherung**
- **Kein Umgehen von Rechtsvorschriften durch Automatisierung (z.B. Standardisierung der Prüfung des berechtigten Interesses)**
- **Keine gefährdende Technik verwenden; wenig aktive Inhalte; Vorsicht mit langlebigen Cookies**



Authentisierung 01

- **Zwickmühle: Ganz ohne Authentifizierung geht es oft nicht; schriftformersetzende qualifizierte elektronische Signatur aber zu kompliziert und gefährdend**
- **Elektronische Signatur kann eine härtere Authentisierung darstellen als herkömmliche Unterschrift, läßt aber andere Eigenschaften vermissen (z.B. Warnfunktion)**
- **Elektronischen Signatur nicht ohne Risiko für Heimanwender: Kein Hineintreiben der Bürger in diese Technik (negatives Beispiel: Beantragen von Anwohnerparkausweis mittels qualifizierter elektronischer Signatur)**



Authentisierung 02

- **Es gibt andere Mittel der Authentisierung: In vielen Fällen reicht Authentisierung durch erfolgte Zahlung**
- **oder durch Verwendung bekannter Meldeadressen oder durch Abfrage von Kontextinformation (Beisp. Wahlschein per E-Mail)**
- **Authentisierung im Backoffice: qualifizierte Signaturen i.d.R. nicht erforderlich; wichtig ist eher durchdachtes Verfahren (EGB SH im Unterschied zu MV)**

