Karlsruher Institut für Technologie

Ansätze für datenschutzkonformes Retina-Scanning

Friederike Schellhas-Mende, Ass. iur. – Forschungsgruppe Compliance, ZAR

Institut für Informations- und Wirtschaftsrecht (IIWR)
Zentrum für Angewandte Rechtswissenschaft (ZAR)

Einführung

- Vorstellung
- Warum Authentifizierung mittels biometrischer Verfahren?
- MARS-Projekt: öffentlich gefördert durch BMBF

Agenda

1. Einführung
2. Rechtliche Grundlagen: Datenschutzrecht
3. Biometrische Authentifizierung
4. Anwendungsbeispiel
5. Zusammenfassende Bewertung Retina-Scan

Rechtliche Grundlagen

- Volkszählungsurteil, BVerfGE 65,1
- (Grund-)Recht auf Informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 2 Grundgesetz (GG)
- Was ist ein personenbezogenes Datum?
- 7 Datenschutzprinzipien

Personenbezogene Daten (Legaldefinition)

§ 3 Abs. 1 BDSG:

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“

Rechtliche Grundlagen

- Volkszählungsurteil, BVerfGE 65,1
- (Grund-)Recht auf Informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 2 Grundgesetz (GG)
- Was ist ein personenbezogenes Datum?
- 7 Datenschutzprinzipien

Datenschutzprinzipien

- Rechtmäßigkeit: Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Erforderlichkeit / Verhältnismäßigkeit: Interessenabwägung
- Datensparsamkeit
- Transparenz: informierte Einwilligung
- Datensicherheit
- Nutzerrechte und Kontrolle

Verbot mit Erlaubnisvorbehalt

§ 4 Abs. 1 BDSG:

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

Datenschutzprinzipien

- Rechtmäßigkeit: Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Erforderlichkeit / Verhältnismäßigkeit: Interessenabwägung
- Datensparsamkeit
- Transparenz: informierte Einwilligung
- Datensicherheit
- Nutzerrechte und Kontrolle

Datensparsamkeit

§ 3a BDSG:

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.“

Datenschutzprinzipien

- Rechtmäßigkeit: Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Erforderlichkeit / Verhältnismäßigkeit: Interessenabwägung
- Datensparsamkeit
- Transparenz: informierte Einwilligung
- Datensicherheit
- Nutzerrechte und Kontrolle

Datensicherheit

§ 9 BDSG:

„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Datenschutzprinzipien

- Rechtmäßigkeit: Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Erforderlichkeit / Verhältnismäßigkeit: Interessenabwägung
- Datensparsamkeit
- Transparenz: informierte Einwilligung
- Datensicherheit
- Nutzerrechte und Kontrolle

Agenda

1. Einführung
2. Rechtliche Grundlagen: Datenschutzrecht
3. Biometrische Authentifizierung
4. Anwendungsbeispiel
5. Zusammenfassende Bewertung Retina-Scan

Biometrische Authentifizierung

- Was gibt es für Methoden?
- Fingerabdruck (biometrischer Reisepass, Notebook; Bezahlfunktion bspw. Scheck-in-Center)
- Gesichtserkennung (biometrischer Reisepass)
- Iriserkennung
- Stimmanalyse
- Verhalten: Gangbild, Tippverhalten etc.
- **UND: Retina-Scan**

Agenda

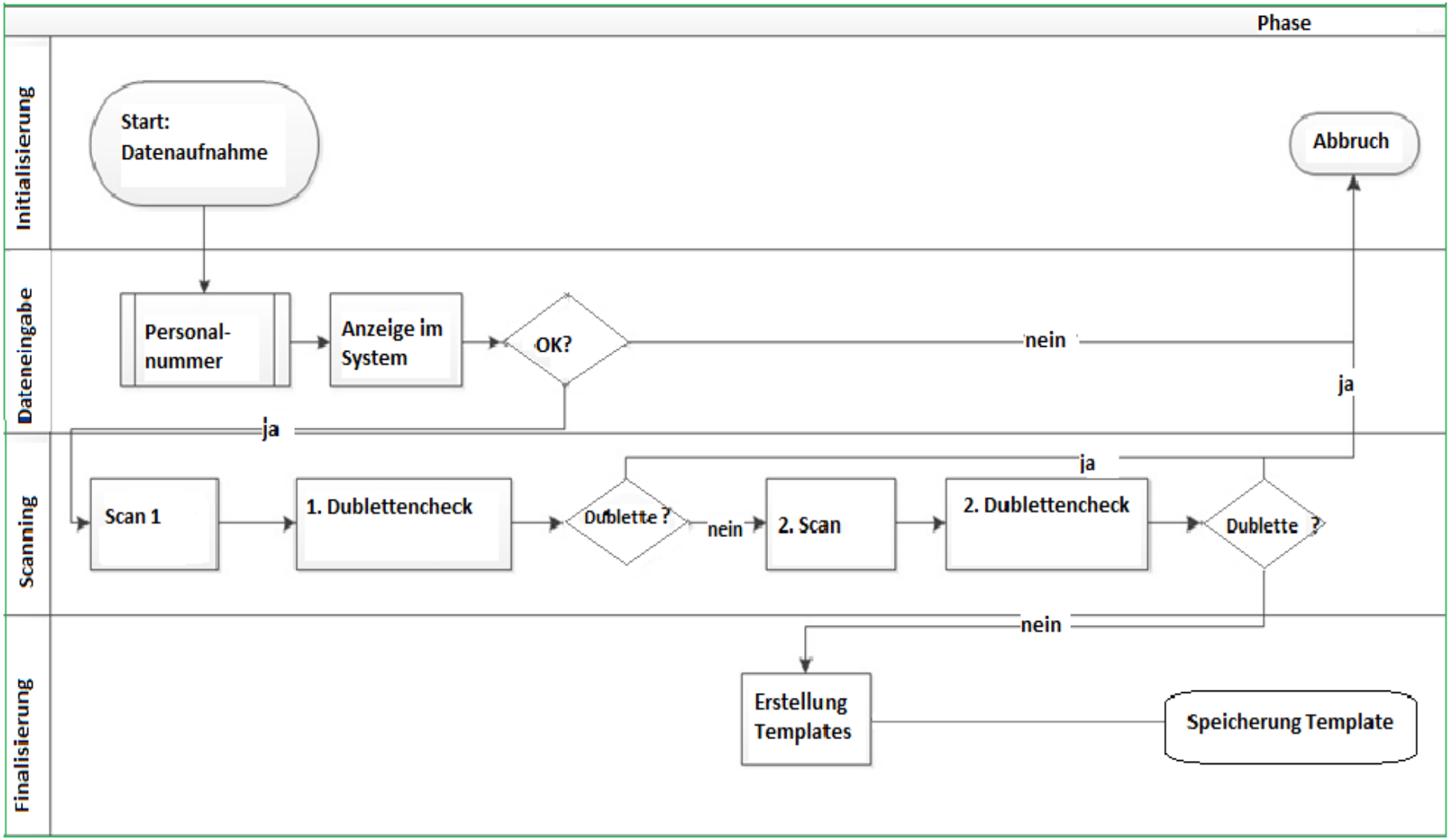
1. Einführung
2. Rechtliche Grundlagen: Datenschutzrecht
3. Biometrische Authentifizierung
4. Anwendungsbeispiel
5. Zusammenfassende Bewertung Retina-Scan

Anwendungsbeispiel

Filesave AG stellt Software für Berufsgruppen her die einer **Geheimhaltungspflicht** unterliegen und bietet diesen auch Cloud-Dienste an, so können sie dort ihre **Akten elektronisch sicher verwahren**. Um den Kunden aber auch innerhalb des Unternehmens selbst größtmögliche Sicherheit zu gewährleisten will Filesave AG Retina-Scans als **Authentifizierungsverfahren** sowohl **für** die **Kunden** als auch für die **eigenen Mitarbeiter** einführen. Welche **Voraussetzungen** gibt es aus **datenschutzrechtlicher** Sicht für die **Einführung** eines solchen **Systems**?

Anwendungsbeispiel:
Verwendung Retina-Scan bei Filesave AG

Prozess: Enrolment / Template-Erstellung



Rechtmäßigkeit – Retina-Scan

- Beim Kunden: § 28 BDSG
- gegenüber Arbeitnehmern: § 32 BDSG
- Einwilligungen:
  - Einfache personenbezogene Daten
  - Besondere Arten personenbezogener Daten
- Retina-Daten: können gesundheitsbezogene Informationen enthalten

  ⇒ Sensible Daten
- Problem: Freiwilligkeit Einwilligung im Arbeitsverhältnis
- **Folgedatenverwendung bei Überschussdaten**

Exkurs

- Exkurs: Arbeitnehmerdatenschutz-Recht
  - Erlaubnis durch Betriebsvereinbarung
  - Mitbestimmung Betriebsrat

- Exkurs: EU-Datenschutz-Grundverordnung Entwurf

(http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF)

  - keine stillschweigende Einwilligung
  - Biometrische Daten  gesundheitsbezogene Daten
  - Beweislastregelung

Zweckbindung – Retina-Scan

- Zweckänderung: nur in Ausnahmefällen
- „Einfache“ Personenbezogene Daten: § 28 Abs. 2 BDSG
- Folgedatenverwendung = Zweckänderung

neue Einwilligung erforderlich

Verhältnismäßigkeit – Retina-Scan

- Relativ mildestes Mittel?
  - Höhere Fälschungssicherheit
- Interessenabwägung
  - Gerechtfertigt bei besonders sensiblen Bereichen
  - Nicht nur allgemeine Zugangskontrolle / Zeiterfassung
- Weniger Gewicht bei rechtsgeschäftlicher Vereinbarung

Datensparsamkeit – Retina-Scan

- Möglichst wenig personenbezogene Daten
- Arbeit mit templatebasierten Verfahren, keine Rohdaten
- Zentrale Speicherung vs. Dezentrale Speicherung
- Direkte Kommunikation

Transparenz – Retina-Scan

- Geringere Missbrauchsgefahr
- Keine heimliche Datenerfassung
- Folge eines Missbrauchs/ Kompromittierung
- Chance: Einblendungen möglich: Display-Funktion

Datensicherheit – Retina-Scan

- Retina Daten = Sensible Daten
- Höheres Schutzbedürfnis
- Technische Lösungen:
  - Frühe Templatebildung
  - „Entbesonderung“ (Forschungsgruppe Compliance)
  - Löschung von Rohdaten
  - Templates ohne inhaltliche Aussagekraft

Nutzerrechte / Kontrolle – Retina-Scan

- Berichtigungsanspruch:
  - Betrifft nur die Verknüpfung
  - Retina-Scan-Daten / Template = immer richtig

Agenda

1. Einführung
2. Rechtliche Grundlagen: Datenschutzrecht
3. Biometrische Authentifizierung
4. Anwendungsbeispiel
5. Zusammenfassende Bewertung Retina-Scan

Zusammenfassende Bewertung Retina-Scan

- Retina-Daten sind besondere personenbezogene Daten
- Rechtmäßigkeit immer von widerruflicher Einwilligung abhängig
- Lösung: „Entbesonderung“ durch technische Lösung
- Rechtsgeschäftliche Vereinbarung erleichtert die Verwendung: Selbstbestimmung / Wahlrecht
- Kritisch: Authentifizierung mittels Retina Scan im Bereich von Arbeitsverhältnissen für einfache Zwecke
- Empfehlung: Vereinbarung von Betriebsvereinbarungen zur Einführung
- Vorteil Retina-Scan: Transparenz des Verfahrens bei Datenerhebung

Karlsruher Institut für Technologie

Danke für Ihre Aufmerksamkeit!