



Erfahrungen mit der Gesundheitskarte in
Österreich:
Die Bedeutung der **e-card** für die elektronische
Gesundheitsdatenverarbeitung in Österreich

Datenschutzfachtagung 9.Juli 2007
in Greifswald

Waltraut Kotschy
Österreichische Datenschutzkommission/
Stammzahlenregisterbehörde

Hintergrund

- **Evidenz basierte Medizin**

betont Bedeutung der
Information

gegenüber der

Intuition

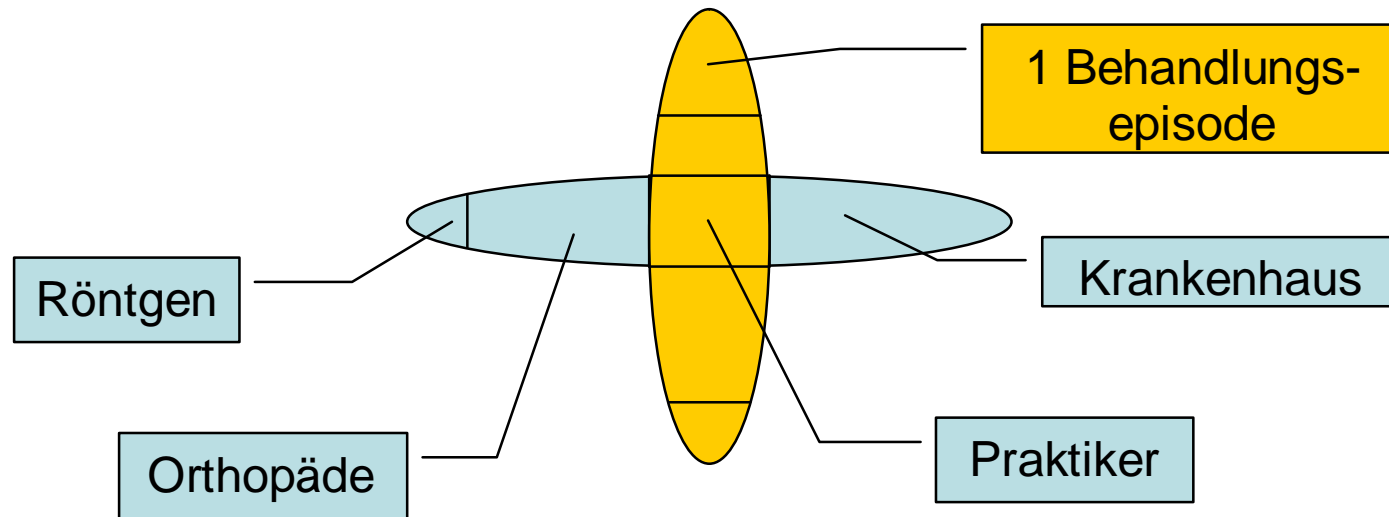
- Betont daher die Wichtigkeit von Datenermittlung und Dokumentation:
sammeln → aufbereiten → zugänglich machen



= **ELGA**

Dokumentation bisher

- Eine medizinische Episode, die durch den Behandlungsvertrag eingegrenzt ist. Kann auch mehrere Gesundheitsdienste umfassen.
- Mehrere Behandlungsepisoden beim selben Gesundheitsdienst werden ebenfalls gemeinsam dokumentiert.



Garantien der Vertraulichkeit

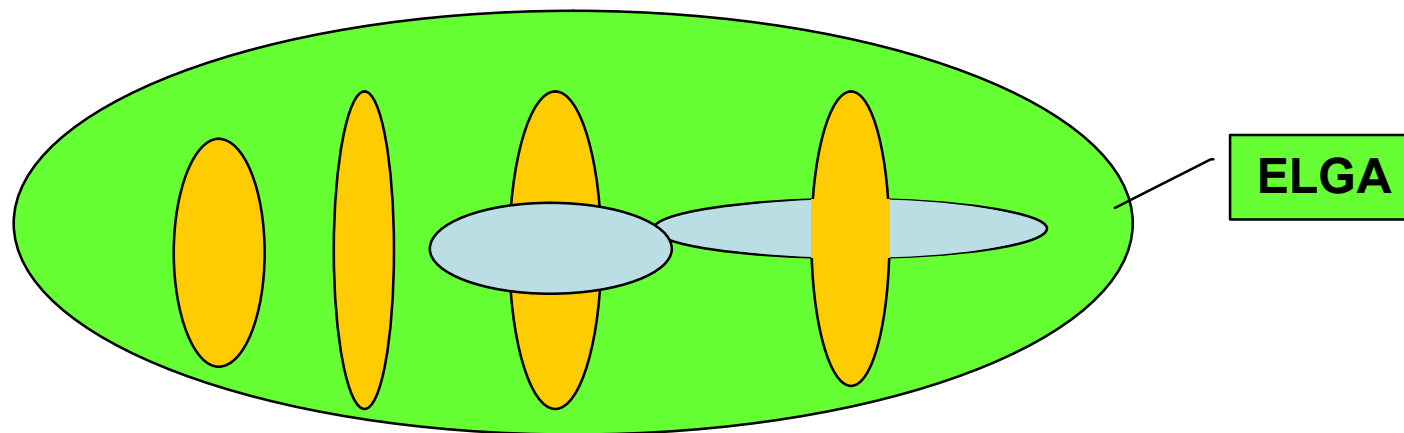
- Gemäß § 9 Z 12 DSG 2000: **nur**
 - die **ärztliche Verschwiegenheitspflicht**

und

 - „**entsprechende** Verschwiegenheitspflichten“

Dokumentation neu: ELGA

- Tendenziell: die umfassende Dokumentation aller Behandlungsfälle im Leben eines Menschen



Garantien der Vertraulichkeit ?

ELGA und Datenschutz

Problem aus datenschutzrechtlicher Sicht ?

- Die Kenntnis von Behandlungsdaten ist nicht mehr beschränkt auf den Arzt, der die Behandlung vorgenommen hat: die Behandlungsdaten stehen durch ELGA für künftige Verwendung zur Verfügung
- Das Ärztegeheimnis wird dadurch im Hinblick auf andere Gesundheitsdiensteanbieter gelockert und muss daher durch weitere „**geeignete Garantien**“ ergänzt werden, damit insgesamt kein Schutzdefizit gegenüber dem bisherigen Zustand eintritt

Wichtigste Forderung: Künftige Verwendung nur für Behandlungszwecke

„geeignete Garantien“

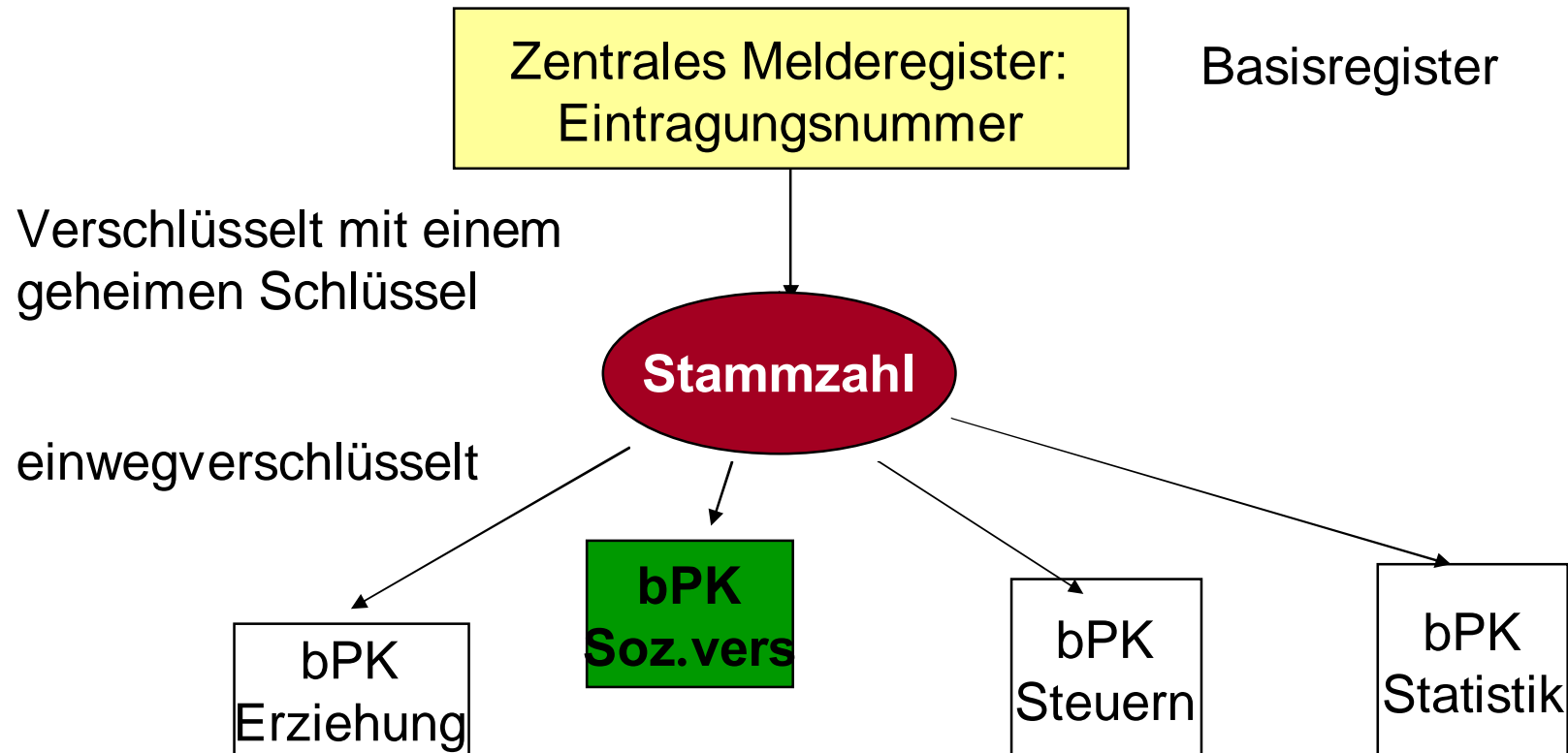
- Arbeitspapier der Art. 29 Gruppe zum elektronischen Gesundheitsakt : **WP 131**
- Enthält eingehende gemeinschaftsrechtliche Analyse der notwendigen Rechtsgrundlagen für elektronische Gesundheitsakten:
Gesetz gemäß Art. 8 Abs. 4 RL 95/46/EG
- Enthält ausführliche Auflistung der Themen, die im Rahmen der Schaffung eines Gesetzes als geeignete Garantien zu berücksichtigen wären

Sichere Identifikation und Authentifizierung als wichtige Garantieaspekte

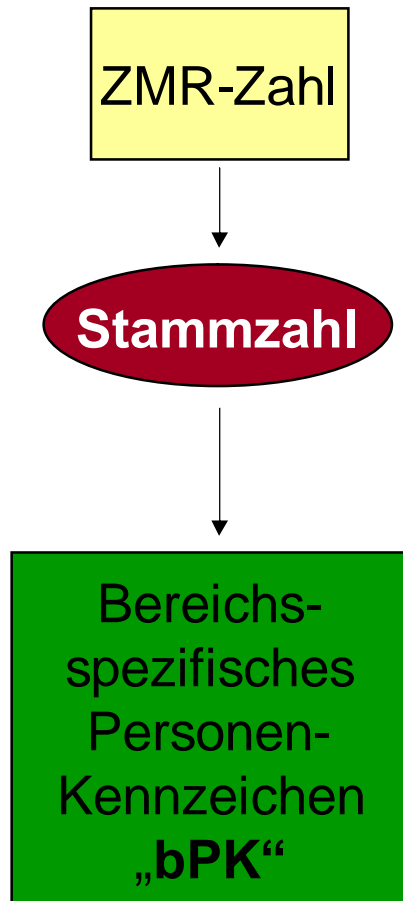
- Identifikation wesentlich hinsichtlich der Bezeichnung von Patienten, deren Daten über ELGA zugänglich gemacht werden
- Identifikation und Authentifizierung wesentlich hinsichtlich der Autorisierung von Personen, die auf ELGA-Daten zugreifen dürfen:
 - Gesundheitsdienstleister (GDAs), die den Betroffenen behandeln
 - der Betroffene selbst, der seine ELGA-Daten einsehen will

Identifizierung im österreichischen E-Government-System

- Elektronische Identität natürlicher Personen



Datenschutz



Das ZMR als Basisregister steuert die eindeutige Identifikation bei

Die Stammzahl repräsentiert die eindeutig identifizierte Person; sie ist eine „verborgene“ Zahl, die nur in der **Bürgerkarte gespeichert ist**, welche sich im Besitz des Betroffenen befindet

In den staatlichen Datenbanken schienen jeweils nur **das für den Bereich** der staatlichen Tätigkeit **passende „bPK“** zur Kennzeichnung einer bestimmten Person auf

Identifizierung der Patienten in ELGA

- Identifizierung soll **in e-Government-konformer Weise** geschehen, damit die Vorteile der e-Government Identifikations- und Authentifizierungsinstrumente genutzt werden können
- Ein gewisses Problem ergibt sich daraus, dass im ELGA-Kontext nicht nur staatliche Institutionen tätig werden – es wird daher eine spezielle Lösung erforderlich sein

Authentifizierung

- Diese wird im österreichischen E-Government-System mit Hilfe der sog. „**Personenbindung**“ bewirkt, das ist eine amtliche Bestätigung, dass ein bestimmter öffentlicher Signaturschlüssel zu einer bestimmten Stammzahl gehört:

[<Name + Stammzahl + Öff. Sig.Schlüssel>]

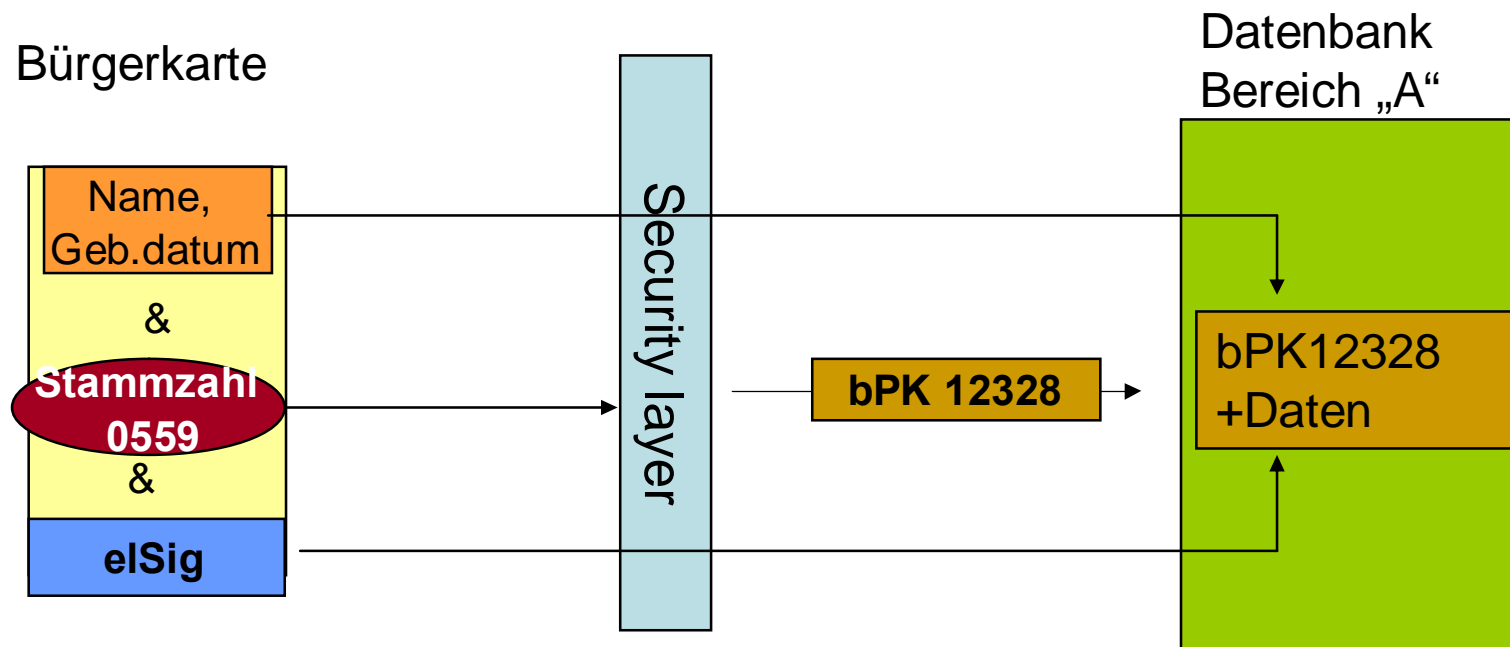
Zusammengehörigkeit
bestätigt durch elektronische
Signatur der StZRegBeh

Bürgerkarte

- Im österr. E-Government-System Mittel zur elektronischen Identifikation und Authentifizierung
- Enthält eine elektronische Signatur und die „Personenbindung“, d.h. eine **elektronische Signatur verbunden mit** einer **eindeutigen, amtlich bestätigten Identität**
- Ist auf unterschiedlichen technischen Infrastrukturen verwendbar (Chip-Karte, Mobiltelefon, USB-Stick, etc.)

Wie funktioniert das?

- Verwendung der Bürgerkarte zur Authentifizierung:



- In der Realität ist die Stammzahl 24-stellig und das bPK 28-stellig

e-card - die österreichische Gesundheitskarte

- Durch § 31 a ASVG wurde die sogenannte “e-card” geschaffen mit folgenden Eigenschaften:
 - **Identifikation**: Name, Geb.datum. Geschlecht, SVNr
 - **Authentifizierung**: Elektronische Signaturdaten
 - **Bürgerkarte**, wenn der Betroffene dies will
 - **Notfallsdaten** nur, wenn der Betroffene dies wünscht (wird praktisch nicht benützt)
 - Rückseite: Europäische Krankenversicherungskarte

Inhalte der e-card

SICHTBAR:

Name

Sozialversicherungsnummer (= 4-stell. Nummer +
Geburtsdatum)

NUR ELEKTRONISCH und nur AUF WUNSCH des
Betroffenen :

elektronische Signatur aktiviert

Stammzahl in der "Personenbindung" der Bürgerkarte
[allenfalls Notfallsdaten]

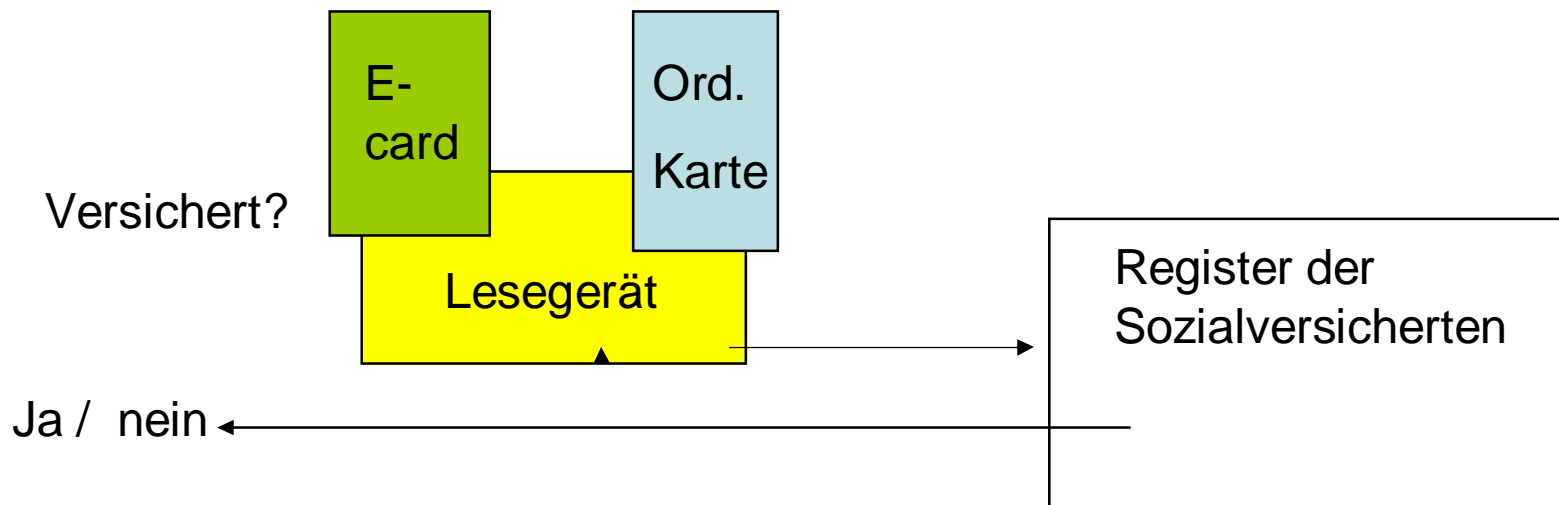
e-card als Schutzinstrument

- Sichere Identifikation und Authentifizierung
 - der **Patienten** ebenso wie
 - der **Behandler**ist Voraussetzung für Datensicherheit in ELGA-Systemen
- **e-card** ist das vorgesehene Hilfsmittel zur elektronischen Identifizierung und Authentifizierung der **Patienten** im österr. ELGA-System
- **Behandler** werden eigene Signatortoken („**GDAToken**“) haben, die auch ihre Rolle (Arzt welchen Fachs, etc.) ausweist

Funktionen der e-card (1)

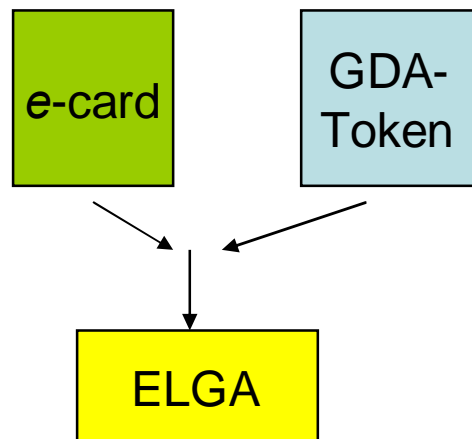
- **Derzeit: Nachweis des Sozialversicherungsstatus:**

In der Arztpraxis wird über ein spezielles Lesegerät die Identität des Karteninhabers ermittelt und mit dem Register der Sozialversicherten beim Hauptverband der Sozialversicherungsträger verglichen



Funktionen der e-card (2)

- Könnte zur Autorisierung des Zugangs von ELGA verwendet werden:
 - GDAs: Vieraugenprinzip: **e-card** + GDA-Token



-- Patienten: **e-card** als Bürgerkarte

ELGA: Projektstand

- Nach Vorliegen der Machbarkeitsstudie (Nov. 2006) wurde Projektplanung in Auftrag gegeben
- Rahmenbedingungen sind noch nicht festgelegt
- Zunächst sollen verwirklicht werden:
 - Infrastruktur:
 - System, über das das Dokument in ELGA angeboten wird
 - System, über das die Anfrage an ELGA gestellt werden kann
 - Register mit den Identitäten von Patienten und GDAs
 - Berechtigungssystem
 - ELGA-Module:
 - Arztbrief
 - Medikation
 - Röntgenbefunde
 - Laborbefunde

Organisationsstruktur von ELGA (1)

- Auch der **organisatorische Aufbau von ELGA** ist datenschutzrechtlich bedeutsam:
 - Entscheidung für dezentrale Lösung scheint bereits getroffen
 - **Wer wird verantwortlich für das Funktionieren von ELGA sein ?** ELGA-Betreiber mit bes. gesetzlichen Verantwortlichkeiten ?
 - Wer wird verantwortlich für den Inhalt von ELGA sein ?
 - Zunächst sicher der Dokumentationsersteller
 - Für Löschung von irrelevant gewordenen Daten?
 - Welchen Einfluss werden Patienten auf den Inhalt ihres ELGA haben? Inwieweit sollen sie einen solchen überhaupt haben?

Organisationsstruktur von ELGA (2)

- **Modularer Aufbau** zur Ermöglichung differenzierter Zugriffsregelungen auf ELGA-Daten

Scheint als Prinzip bereits akzeptiert: Projekt sieht Schaffung von 4 Modulen im Erstausbau stadium vor

(Medikation
Röntgenbefunde
Laborbefunde
Arztbrief)

Ausblick

- Die Artikel 29 Gruppe lädt die Vertreter der Gesundheitsberufe ein, die im Arbeitspapier Nr. 131 dargestellten datenschutzrechtlichen Erwägungen aus ihrer Sicht zu kommentieren
- Einlangende Kommentare werden ausgewertet und, soweit notwendig, bei einer Revision des Papiers berücksichtigt