ARTIKEL 29-DATENSCHUTZGRUPPE

00145/12/DE
WP 189

Arbeitspapier 01/2012 zu epSOS

Angenommen am 25. Januar 2012

1. Einleitung

Ziel dieses Arbeitspapiers der Artikel 29-Datenschutzgruppe ist es, eine Orientierungshilfe zu Datenschutzfragen im Zusammenhang mit dem Projekt epSOS (European Patients Smart Open Services) zu bieten. Keinesfalls sollen in diesem Papier alle spezifischen Aspekte des epSOS-Projekts umfassend behandelt werden. Es werden darin vielmehr die wichtigsten Grundsätze der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erläutert. Ferner befasst sich das Papier mit der Frage, wie die im Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten“ (WP 131) vorgenommene Analyse der Richtlinie im Fall des Projekts epSOS aussehen sollte.

Das Papier ändert jedoch nichts an der Verpflichtung aller am epSOS-Projekt beteiligten Organisationen, die nationalen Datenschutzbestimmungen, mit denen die Richtlinie 95/46/EG ungesetzt wurde, einzuhalten. Daher können die Datenschutzbehörden in den Mitgliedstaaten weitere Orientierungshilfen geben und Aufsichtsmaßnahmen übernehmen.

epSOS ist ein Pilotprojekt[1], das EU-Bürgern grenzüberschreitende elektronische Gesundheitsdienste anbietet. Im Mittelpunkt steht der Aufbau eines praxistauglichen eHealth-Rahmens sowie einer IKT-Infrastruktur (IKT – Informations- und Kommunikationstechnik), mit der ein Zugriff auf Patientendaten aus verschiedenen europäischen Gesundheitssystemen möglich ist. Damit soll die Gesundheitsversorgung für Bürger bei Reisen in ein anderes europäisches Land verbessert werden. epSOS wird in zwei Pilotphasen getestet. An diesen Pilotphasen nehmen verschiedene Mitgliedstaaten teil. Die erste Pilotphase von epSOS läuft demnächst an, und die technischen, rechtlichen und organisatorischen Grundlagen für die zweite Phase sind bereits in Arbeit.

epSOS wird für zweierlei Zwecke verwendet:

- für eine Patienten-Kurzakte mit medizinischen Daten, zu der Anbieter von Gesundheitsdienstleistungen bei der Patientenbehandlung Zugang haben, und
- für den grenzüberschreitenden Einsatz elektronischer Verschreibungen („ePrescription“- oder „eMedikation“-Systeme).

Da das epSOS-Projekt noch in der Entwicklung ist, stehen seine technischen, rechtlichen und organisatorischen Grundlagen noch nicht fest. Daher kann die Arbeitsgruppe derzeit noch keine abschließende Beurteilung abgeben.

Die Richtlinie 2011/24/EG über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung enthält Bestimmungen, mit denen in der Union sichere, hochwertige grenzüberschreitende Gesundheitsdienstleistungen angeboten, die Patientenmobilität gewährleistet und die Zusammenarbeit der Mitgliedstaaten in der Gesundheitsversorgung gefördert werden sollen. Sie findet Anwendung auf Patienten, die in einem anderen Mitgliedstaat als dem Versicherungsmitgliedstaat die Gesundheitsversorgung in Anspruch nehmen wollen. Sie wahrt die Zuständigkeiten der Mitgliedstaaten für die Organisation und Erbringung von Gesundheitsdienstleistungen und medizinischer Versorgung. Dasselbe gilt für dieses Papier: es lässt die Zuständigkeiten der Mitgliedstaaten

[1] Vorläufiges Projekt mit echten Daten.

für die Organisation und Erbringung von Gesundheitsdienstleistungen und medizinischer Versorgung unberührt und geht nicht auf die nationalen Gesundheits- oder eHealth-Systeme ein.

Die Arbeitsgruppe ist sich jedoch der höchst unterschiedlichen rechtlichen, technischen und organisatorischen Gegebenheiten in den Mitgliedstaaten sowie der Unterschiede im Stand und in der Planung des jeweiligen nationalen eHealth-Rahmens und der IKT-Infrastruktur bewusst. Sie weiß auch um die unterschiedliche Auslegung der Richtlinie 95/46/EG im Gesundheitssektor und um die Tatsache, dass diese Unterschiede bei der supranationalen Datenverarbeitung durchaus eine Rolle spielen können.

In Anbetracht dieser komplexen und unterschiedlichen Gegebenheiten und des vorläufigen Charakters des epSOS-Projekts ist es recht problematisch, Empfehlungen auszusprechen. Im Augenblick können nur allgemeine, aber keine spezifischen Empfehlungen formuliert werden.

Auch wenn in diesem Papier die Problematik nicht erschöpfend behandelt werden kann, sind die Fragen doch mit Blick auf die künftige Zusammenarbeit zwischen den Mitgliedstaaten zu verstehen und zu diskutieren. Die Arbeitsgruppe möchte einige der Kernprobleme und grundsätzlichen Datenschutzfragen herausarbeiten, die bei grenzüberschreitenden Projekten mit Patientendaten auftreten könnten und gelöst werden müssen. Die zukünftige Zusammenarbeit in diesem Bereich könnte gemeinsam von den zuständigen nationalen Datenschutzbehörden überwacht werden (nähere Einzelheiten weiter unten).

Das Papier befasst sich mit folgenden Aspekten:

- der Rechtsgrundlage für die Verarbeitung von Daten im Rahmen des Projekts einschließlich des Grundsatzes der Verhältnismäßigkeit und der Zweckbindung
- organisatorischen Fragen
- Transparenz und
- Datensicherheit.

Da sich dieses Dokument hauptsächlich mit der Datenverarbeitung in elektronischen Patientenakten befasst, sollte es als Ergänzung zum WP 131 „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ betrachtet werden.

2. Beschreibung des epSOS-Projekts

epSOS ist ein Pilotgroßprojekt, in dessen Mittelpunkt elektronische Speichersysteme für Patientendaten stehen, wobei in der Anfangsphase das Hauptaugenmerk zwei grenzüberschreitenden Diensten gilt, nämlich der Patienten-Kurzakte und elektronischen Verschreibungen (e-Rezept). Zunächst wird sich das epSOS-Projekt mit dem Entwurf, der Entwicklung, der Umsetzung und dem Betrieb dieser beiden grenzüberschreitenden interoperablen Pilotdienste befassen, die den Kern des Systems bilden. Mittelfristig wird sich epSOS auch mit den eventuellen Auswirkungen des Projekts auf eHealth in Europa beschäftigen und Empfehlungen für die Weiterentwicklung grenzüberschreitender elektronischer Gesundheitsdienste formulieren, darunter auch Empfehlungen für gesetzgeberische und Regulierungsmaßnahmen, die erforderlich werden könnten, um neue grenzüberschreitende elektronische Gesundheitsdienste und neue Länder einzubeziehen.

Das vorliegende Papier ist vor dem Hintergrund der Vorbereitung und Entwicklung der beiden Kerndienste (Patienten-Kurzakte und elektronische Verschreibungen) zu sehen.

Bei beiden Diensten kann ein Mitgliedstaat die Rolle von „Land A“ oder „Land B“ spielen. „Land A“ ist der Versicherungsmitgliedstaat, also das Land, in dem die personenbezogenen Daten eines epSOS-Patienten gespeichert sind und in dem er versichert ist. „Land B“ ist das Land, in dem die grenzüberschreitende Gesundheitsversorgung erfolgt, wenn der Patient im Ausland eine Behandlung vornehmen lässt oder sich ein Rezept besorgt. Hierbei handelt es sich um ein anderes Land, in dem Informationen über den Patienten zur Erbringung der Gesundheitsversorgung benötigt werden[2].

Als Land A und/oder Land B teilnehmende Mitgliedstaaten haben jeweils eine „nationale Kontaktstelle“ zu benennen. Dieser juristischen Person obliegen in einem Land alle rechtlichen Verpflichtungen, und sie ist vertraglich verpflichtet, bei allen das Land betreffenden Fragen den „epSOS trusted domain“(vertraulichen Bereich) zu schützen.[3]

Der Datenaustausch erfolgt direkt zwischen diesen nationalen Kontaktstellen. Das epSOS-Projekt verfügt allerdings nicht über eine zentrale Netzwerkschaltstelle. Die bei den nationalen Kontaktstellen ablaufenden Datenverarbeitungen unterliegen jedoch gemeinsamen Sicherheits- und Kommunikationsstandards und werden durch zentrale Dienste und Verzeichnisse unterstützt.

epSOS selbst beschreibt den allgemeinen Ablauf wie folgt:

- Ein Patient möchte sich von einer medizinischen Fachkraft in Land B behandeln lassen;
- Die medizinische Fachkraft stellt eine Patientenkennung aus und bestätigt die Einwilligung des Patienten in eine Abfrage von Daten für die Zwecke des betreffenden Behandlungstermins. Willigt der Patient ein, bestätigt die medizinische Fachkraft dies gegenüber der nationalen Kontaktstelle in Land B und übermittelt anschließend eine entsprechende Anfrage;
- die nationale Kontaktstelle in Land B leitet die Anfrage und die Bestätigung der Einwilligung des Patienten an die nationale Kontaktstelle im Land A zur weiteren Bearbeitung weiter;
- die nationale Kontaktstelle in Land A beantwortet die Anfrage unter Beachtung ihrer eigenen sowie der epSOS-Sicherheitsvorkehrungen;
- die nationale Kontaktstelle in Land B verarbeitet die erhaltenen Daten und leitet sie an die anfragende Fachkraft weiter;
- die Fachkraft in Land B meldet, dass sie die Leistung erbracht hat. Diese Information wird von der nationalen Kontaktstelle im Land B an die nationale Kontaktstelle in Land A weitergegeben.

---

[2] Siehe das folgende von epSOS veröffentlichte Dokument: “D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites”, p. 7 (Rechtliche und regulatorische Vorgaben für Mitgliedstaaten, die am Entwurf von epSOS teilnehmen. Standardvertragsbedingungen für die Mitgliedstaaten. Zusagen über die Pilotstandorte), S. 7 (http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf).

[3] Das Konzept des „trusted domain“ wird weiter unten in diesem Kapitel näher erläutert.

Zwischen den als Land A und/oder Land B teilnehmenden Mitgliedstaaten wird ein so genannter „epSOS trusted domain“ eingerichtet. Er ist folgendermaßen definiert:

„Der ‚epSOS trusted domain' umfasst die nationalen Kontaktstellen von epSOS und ihre nationalen Vertragspartner, die allesamt die technischen, rechtlichen und organisatorischen Anforderungen erfüllen, um sichere epSOS-Dienste erbringen und innerhalb des ‚epSOS trusted domain' im Einklang mit dieser Rahmenvereinbarung eine sichere und vertrauliche Datenübermittlung oder -speicherung im Zusammenhang mit einer Behandlung zu gewährleisten“.[4]

Der Beschreibung des „epSOS trusted domain“ ist zu entnehmen, dass das Pilotprojekt mit Hilfe von Verträgen beziehungsweise Verordnungen[5] durchgeführt werden soll. Dies gilt für das Verhältnis zwischen den teilnehmenden Mitgliedstaaten und dem epSOS-Projekt beziehungsweise zwischen den Mitgliedstaaten und deren nationalen Kontaktstellen sowie zwischen den nationalen Kontaktstellen und den Anbietern von Gesundheitsdienstleistungen. epSOS wird einen Mustervertrag ausarbeiten, der dann von den nationalen Kontaktstellen den jeweiligen Erfordernissen ihres Landes angepasst werden kann. Der endgültige Vertrag ist jedoch dem Lenkungsausschuss des epSOS-Projekts zur Billigung vorzulegen (damit soll gewährleistet werden, dass die Verträge in den einzelnen Mitgliedstaaten nicht zu stark voneinander abweichen und eine Reihe von Mindestanforderungen erfüllen).

Wichtig ist in diesem Zusammenhang, dass das epSOS-Projekt selbst darauf hinweist, dass dieses Vertragssystem nur während der Laufzeit des Pilotprojekts genutzt werden kann: *„Diese Regelung kann jedoch nach Beendigung des Projekts nicht beibehalten und muss in eine Dauerregelung überführt werden, wenn die Dienste in großem Maßstab eingeführt und routinemäßig angeboten werden“.*[6]

3. Rechtsgrundlage und Verhältnismäßigkeit

- **Allgemeine Anmerkungen zur Rechtsgrundlage**

Das Recht auf Datenschutz ist ein in Artikel 8 der Charta der Grundrechte der Europäischen Union verankertes Grundrecht. Nach dieser Bestimmung hat jeder Mensch das Recht auf Schutz seiner personenbezogenen Daten. Solche Daten müssen nach Treu und Glauben für einen bestimmten Zweck und entweder mit Einwilligung der betroffenen Person oder auf einer anderen im nationalen Recht niedergelegten legitimen Grundlage verarbeitet werden.

---

4 Siehe das folgende von epSOS veröffentlichte Dokument: “D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites”, S. 8. (http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf)

5 Mit Hilfe von Verordnungen könnten die Beziehungen zwischen Regierung/Staat und einer nationalen Kontaktstelle geregelt werden.

6 Siehe das folgende von epSOS veröffentlichte Dokument: *“D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites”, S. 19 (http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf*)

Jede Person hat das Recht, Auskunft über die über sie erhobenen Daten zu erhalten und diese, falls sie unrichtig sind, berichtigen zu lassen. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Behörde überwacht.

Unter bestimmten Voraussetzungen können Datenschutzrechte eingeschränkt werden. Eine derartige Einschränkung muss jedoch geregelt sein und nach dem Grundsatz der Verhältnismäßigkeit vorgenommen werden (siehe Kapitel 5).

Weitere Ausführungen zur allgemeinen Rechtsgrundlage der Verarbeitung von Gesundheitsdaten aus Patientenakten sowie zu elektronischen Verschreibungen lassen sich den detaillierten Kommentaren im WP 131 entnehmen, die näher auf die entsprechenden Bestimmungen der Richtlinie 95/46/EG eingehen.

Ferner sind die in Artikel 6 der Richtlinie festgelegten **allgemeinen Grundsätze** zu berücksichtigen. Dazu zählen insbesondere der Grundsatz der Zweckbindung, der Grundsatz der Verhältnismäßigkeit, der Grundsatz der Datenqualität und der Grundsatz, dem zufolge Daten nicht länger aufbewahrt werden dürfen, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, erforderlich ist. Darüber hinaus sind noch weitere grundsätzliche Aspekte wie Informationsanforderungen, das Recht der betroffenen Person auf Auskunft, Berichtigung und Löschung sowie Pflichten im Zusammenhang mit der Datensicherheit zu beachten.

Des Weiteren haben, wie es auch im WP 131 heißt, sämtliche in medizinischen Unterlagen, elektronischen Patientenakten und EPA-Systemen enthaltenen bzw. gespeicherten Daten als „**sensible personenbezogene Daten**“ zu gelten. Sie fallen daher nicht nur unter die allgemeinen Bestimmungen der Richtlinie über den Schutz personenbezogener Daten, sondern auch unter die besonderen Vorschriften für die Verarbeitung sensibler Daten in **Artikel 8** der Richtlinie.

- **Anwendbarkeit von Artikel 8 der Richtlinie**

Artikel 8

Nach Artikel 8 Absatz 1 der Datenschutzrichtlinie 95/46/EG ist die Verarbeitung von Gesundheitsdaten generell untersagt. Gemäß Artikel 6 des Übereinkommens Nr. 108 des Europarates dürfen solche Daten nur automatisch verarbeitet werden, „wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet“. In Anbetracht jedoch der Bedeutung, die der Nutzung von Informationen über einen Patienten zukommt, um ihm eine angemessene medizinische Behandlung zukommen lassen zu können, bestehen Ausnahmen vom allgemeinen Verbot der Verarbeitung medizinischer Daten. Die Richtlinie enthält in Artikel 8 Absatz 2 und 3 zwingende Ausnahmen sowie eine fakultative Ausnahme in Artikel 8 Absatz 4. Alle diese Ausnahmen sind eng gefasst und eng auszulegen.

Artikel 8 Absatz 3

Nach Artikel 8 Absatz 3 der Datenschutzrichtlinie 95/46/EG gilt das Verbot der Verarbeitung personenbezogener Gesundheitsdaten nicht, wenn die Verarbeitung dieser Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen

Recht, einschließlich der von den zuständigen einzelstaatlichen zuständigen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Im WP 131 wird Artikel 8 Absatz 3 folgendermaßen ausgelegt (S. 11):
*Diese Ausnahme gilt nur für die Verarbeitung personenbezogener Daten zu dem **speziellen Zweck** der Erbringung gesundheitsbezogener Dienstleistungen wie Vorsorge, Diagnostik, Therapie und Nachsorge sowie zu Verwaltungszwecken wie etwa Abrechnung, Buchführung oder Statistik.*

Nicht erfasst ist hingegen jegliche Art der Weiterverarbeitung, die zur Erbringung dieser Leistungen nicht unmittelbar erforderlich ist, wie medizinische Forschung, nachträgliche Kostenerstattung durch die Krankenversicherung oder die Durchsetzung von Geldforderungen. Nicht unter Artikel 8 Absatz 3 fallen ferner eine Reihe sonstiger Verarbeitungsvorgänge im Bereich des öffentlichen Gesundheitswesens und der sozialen Sicherheit, beispielsweise zur Sicherung der Qualität und Kosteneffizienz der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen; sie sind im Erwägungsgrund 34 der Richtlinie als Beispiele für die Anwendung von Artikel 8 Absatz 4 erwähnt.

Ausgehend von dieser Auslegung fällt die Verarbeitung im Fall von epSOS vermutlich nicht unter die besonderen Zwecke des Artikels 8 Absatz 3.

Es fehlen allgemeine Garantien, dass in Land B keine Weiterverarbeitung zu anderen Zwecken als der Erbringung und Verwaltung der Gesundheitsversorgung erfolgt. So bestehen beispielsweise in manchen Ländern Rechtsvorschriften, nach denen medizinisches Personal verpflichtet ist, Daten aus elektronischen Patientenakten ohne Einwilligung der Patienten an Forschungseinrichtungen weiterzugeben, und zwar unabhängig davon, ob die Daten von epSOS oder lediglich von einem nationalen Erbringer von Gesundheitsleistungen stammen.

Gleiches gilt für die nationalen Kontaktstellen; je nach innerstaatlichem Recht und der Rechtsgrundlage für die einzelnen nationalen Kontaktstellen ist nicht unbedingt sichergestellt, dass die nationalen Kontaktstellen weder in Land A noch in Land B die von ihnen verarbeiteten sensiblen Daten für andere Zwecke als epSOS weitergeben dürfen.

Darüber hinaus ist noch keine Lösung für das Problem gefunden worden, dass nur dem Berufsgeheimnis unterliegendes Personal Zugriff auf die epSOS-Daten erhalten soll.

In Anbetracht all dessen wäre in Zukunft eine Einschränkung und Spezifizierung der Zwecke und Einsatzbereiche von epSOS erforderlich, damit Artikel 8 Absatz 3 als Rechtsgrundlage für epSOS herangezogen werden kann. In seiner jetzigen Ausgestaltung erfüllt epSOS die darin genannten Anforderungen kaum.[7]

[7] Da die Zwecke des epSOS-Projekts bisher noch nicht so formuliert wurden, dass sie im Einklang mit Artikel 8 Absatz 3 stehen, dürfte zudem fraglich sein, ob die Verarbeitung gesundheitsbezogener Daten für die in Artikel 8 Absatz 3 erwähnten Zwecke wirklich „erforderlich“ ist.

Artikel 8 Absatz 4

Ein Verweis auf Ausnahmen im wichtigen öffentlichen Interesse, wie sie in Artikel 8 Absatz 4 der Richtlinie geregelt sind, könnte einigen Mitgliedstaaten eine ausdrückliche Rechtsgrundlage für die Übermittlung von Gesundheitsdaten an andere Anbieter medizinischer Leistungen innerhalb der EU bieten. Dies trifft jedoch nicht auf alle Mitgliedstaaten zu. Außerdem könnte eine solche innerstaatliche Rechtsgrundlage nur die Übermittlung von Gesundheitsdaten an andere Anbieter medizinischer Leistungen (in einem anderen Mitgliedstaat, Land B) regeln, nicht jedoch die Verwendung dieser Daten durch diese Anbieter medizinischer Leistungen im Land B.

Schlussfolgerungen

Die Arbeitsgruppe ist daher der Ansicht, dass die **ausdrückliche Einwilligung** [(Artikel 8 Absatz 2 Buchstabe a] und das **lebenswichtige Interesse der betroffenen Person** [(Artikel 8 Absatz 2 Buchstabe c] als angemessene Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen des epSOS-Projekts in seiner derzeitigen Ausgestaltung dienen können.

- **Ausdrückliche Einwilligung und Aufklärung**

Artikel 8 Absatz 2 Buchstabe a der Richtlinie lautet:
„Absatz 1 findet in folgenden Fällen keine Anwendung: a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvorschriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch eine Einwilligung der betroffenen Person nicht aufgehoben werden;“.

Die für eine Einwilligung erforderlichen Elemente sind in der Stellungnahme zur Definition der Einwilligung (WP 187) ausführlich behandelt worden. WP 131 befasst sich mit dem Sonderfall der Gesundheitsdaten. Beide WP enthalten folgende Elemente:

„Als Einwilligung ist gemäß Artikel 2 Buchstabe h der Richtlinie ’jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt’ zu betrachten.

‚Ohne Zwang’ bedeutet, dass sich eine Person aus freien Stücken und im Vollbesitz ihrer geistigen Kräfte ohne jeglichen sozialen, finanziellen, psychologischen oder sonstigen Druck von außen entscheiden kann. Erfolgt die Einwilligung nur, weil mit Nichtbehandlung oder einer schlechteren medizinischen Behandlung gedroht wird, kann von einer Einwilligung ‚aus freien Stücken’ nicht die Rede sein. Die Einwilligung einer Person, die nicht die Möglichkeit hat, eine echte Wahl zu treffen oder vor vollendete Tatsachen gestellt wurde, ist daher ungültig. Die betreffende Person kann tatsächlich frei entscheiden und muss anschließend die Einwilligung ohne irgendwelche Nachteile zurückziehen können.

Die Einwilligung ‚für den konkreten Fall’ muss sich auf eine genau umrissene konkrete Situation beziehen, in der die Verarbeitung der medizinischen Daten erfolgen soll. Eine ‚pauschale Zustimmung’ der betroffenen Person beispielsweise zur Erfassung ihrer medizinischen Daten in einer elektronischen Patientenakte und zur anschließenden Weitergabe früherer und aktueller Daten an in die Behandlung eingebundene medizinische Fachkräfte wäre keine Einwilligung im Sinne von Artikel 2 Buchstabe h der Richtlinie.

‚In Kenntnis der Sachlage' meint Einwilligung der betroffenen Person nach der bewussten Erfassung und Würdigung der Fakten und Auswirkungen einer Handlung. Sie muss in klarer und verständlicher Form genau und umfassend über alle relevanten Aspekte, insbesondere die in den Artikeln 10 und 11 genannten wie Art und Zweckbestimmung der verarbeiteten Daten, Personen, an die die Daten möglicherweise weitergegeben werden, und ihre Rechte, aufgeklärt werden. Hierzu gehört auch die Aufklärung über die möglichen Folgen einer Verweigerung der Einwilligung zu der jeweiligen Verarbeitung.

Bei sensiblen personenbezogenen Daten und damit auch bei für die elektronische Patientenakte bestimmten Daten muss die Einwilligung im Gegensatz zu den Bestimmungen in Artikel 7 der Richtlinie ***ausdrücklich*** *erfolgen. Opt-out-Lösungen, bei denen die Einwilligung vorausgesetzt wird, wenn keine ausdrückliche Ablehnung erfolgt, genügen nicht dem Erfordernis der ‚ausdrücklichen' Einwilligung. Gemäß der allgemeinen Definition, wonach die Einwilligung eine Willensbekundung voraussetzt, muss sich die Einwilligung ausdrücklich auf die* ***sensiblen Daten*** *beziehen. Die betroffene Person muss sich darüber im Klaren sein, dass sie auf den besonderen Schutz ihrer Daten verzichtet. Eine schriftliche Einwilligung ist allerdings nicht erforderlich.*

Anders als in Artikel 7 wird in Artikel 8 Absatz 2 Buchstab a dem Umstand Rechnung getragen, dass es Fälle geben kann, in denen das Verbot der Verarbeitung sensibler Daten ***selbst durch ausdrückliche Einwilligung nicht*** *aufgehoben werden kann. Die Mitgliedstaaten können selbst entscheiden, ob und wie sie diese Fälle im Einzelnen regeln."*

- **Einwilligung in zwei Stufen**

Die Arbeitsgruppe empfiehlt, eine **zweistufige Einwilligung** der betroffenen Person in die Übermittlung und Verarbeitung gesundheitsbezogener Daten ins Auge zu fassen. Zunächst sollte die betroffene Person ihrer Teilnahme am epSOS-Projekt oder Teilen davon ausdrücklich zustimmen (beispielsweise in Form modularer Zugriffsrechte für Anbieter von Gesundheitsdienstleistungen, siehe unten). Mit dieser ersten Einwilligung in Land A könnten Anbieter von Gesundheitsdienstleistungen bestimmte Daten zu dem Zweck aufbereiten, sie künftig anderen Anbietern von Gesundheitsdienstleistungen im Rahmen von epSOS zur Verfügung zu stellen. Die erste Einwilligung wäre nur einmal an der Stelle erforderlich, an der die Daten der betroffenen Person aufbereitet oder dem System zur Verfügung gestellt werden (d. h. davor). Daraus folgt, dass die erste Einwilligung zwangsläufig vor der zweiten Einwilligung erteilt werden muss. Sollten sich nach Erteilung der ersten Einwilligung wesentliche Änderungen bei der Verarbeitung der Daten innerhalb von epSOS ergeben, wird eine neue Einwilligung erforderlich.

Das Erfordernis einer ersten Einwilligung hätte unter Umständen auch den Nebeneffekt, dass die Anzahl der im System befindlichen betroffenen Personen auf das unbedingt erforderliche Mindestmaß beschränkt und damit auch der potenzielle Schaden bei einer unrechtmäßigen Verarbeitung dieser sensiblen Daten möglichst gering gehalten würde.

Damit betroffene Personen, die in Land B eine Behandlung benötigen, aber noch nicht ihre Einwilligung im Land A erteilt haben, die Vorteile von epSOS nutzen können, könnte das epSOS-Projekt die Möglichkeit prüfen, dass Patienten ihre erste Einwilligung beispielsweise auch über eine sichere Internetverbindung in Land B geben können.

Mit der zweiten Einwilligung wird der Verarbeitung der Gesundheitsdaten bei einer tatsächlichen Behandlung in Land B ausdrücklich zugestimmt.

Wie bereits erwähnt, ist eine der Vorbedingungen für die Gültigkeit einer Einwilligung, dass die betroffene Person (von dem für die Verarbeitung Verantwortlichen oder seinem Vertreter) gemäß den Anforderungen von Artikel 10 und 11 der Richtlinie **aufgeklärt** worden ist.

Bei der Aufklärung im Zusammenhang mit der **ersten Einwilligung** sollte eine umfassende, genaue und verständliche Beschreibung des epSOS-Projekts gegeben werden, wobei zumindest zu erwähnen wäre, welche Kategorien von Daten von welchem Anbieter von Gesundheitsdienstleistungen an andere Anbieter von Gesundheitsdienstleistungen und andere Einrichtungen übermittelt würden. Dazu gehören auch die Einrichtungen, die in Land B an der Weiterverarbeitung der Daten zu anderen Zwecken als der Erbringung und Verwaltung der Gesundheitsversorgung beteiligt sind. Zu informieren ist auch über den Zweck der Übermittlung und die Speicherfrist der Daten. Schließlich muss deutlich gemacht werden, dass die Möglichkeit besteht, die Einwilligung jederzeit zurückzuziehen. Die betroffene Person ist ferner über ihr Recht aufzuklären, Auskunft über sie betreffende Daten und deren Berichtigung verlangen zu können.

Bei der Aufklärung im Zusammenhang mit der **zweiten Einwilligung** ist zumindest anzugeben, welcher Anbieter von Gesundheitsdienstleistungen und welche andere Einrichtung welche Datenkategorien zu welchem Zweck verarbeiten wird.

Der Patient sollte ferner die Möglichkeit haben, seine Einwilligung zur Übermittlung und Verarbeitung nur bestimmter Kategorien von Gesundheitsdaten zu geben (**modulare** Zugriffsrechte für Anbieter von Gesundheitsdienstleistungen in einem anderen Land). Schließlich muss deutlich gemacht werden, dass die Möglichkeit besteht, die Einwilligung jederzeit zurückzuziehen. Die betroffene Person ist ferner über ihr Recht aufzuklären, Auskunft über sie betreffende Daten und deren Berichtigung verlangen zu können.

- **Lebenswichtige Interessen der betroffenen Person**

Gemäß Artikel 8 Absatz 2 Buchstabe c der Richtlinie 95/46/EG ist die Verarbeitung sensibler personenbezogener Daten zulässig, wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich ist, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben. Die Verarbeitung muss in einem Zusammenhang mit wesentlichen individuellen Interessen der betroffenen Person oder eines Dritten stehen und muss – im medizinischen Kontext – für eine lebensrettende Behandlung in einer Situation erforderlich sein, in der die betroffene Person nicht in der Lage ist, ihren Willen zu bekunden (Notfall). Diese Ausnahme würde folglich nur bei wenigen Behandlungsfällen und nur dann gelten, wenn die erste Einwilligung des Zwei-Stufen-Modells gegeben worden ist. Es ist äußerst wichtig, den Anwendungsbereich dieser Ausnahme eng zu definieren und genau festzulegen, wann und wie sie angewandt werden darf. Weiter sollte mit technischen Maßnahmen ein Missbrauch der Notfallsituation verhindert werden.

Über den Datenaustausch in derartigen Fällen innerhalb des epSOS-Projekts sollte die betroffene Person im Rahmen der allgemeinen Aufklärung über das epSOS-Projekt informiert werden.

In dieser Situation kommt es vor allem darauf an, dass der Patient Auskunft über die erfolgten Datenübermittlungen erhält (siehe Näheres im Kapitel ‚Transparenz').

- **Verhältnismäßigkeit und Zweckbindung**

Der „Grundsatz der Verhältnismäßigkeit" gehört zu den Kerngrundsätzen des EU-Rechts. Er besagt, dass jede Maßnahme, die die Rechte von Personen berührt, zu dem angestrebten Ziel in einem angemessenen Verhältnis stehen und nicht über das hinausgehen darf, was zum Erreichen dieses Ziels erforderlich ist. Artikel 6 der Richtlinie übernimmt diesen Grundsatz, denn er besagt, dass personenbezogene Daten den Zwecken entsprechen müssen, für die sie erhoben und/oder weiterverarbeitet werden, sowie dafür erheblich sein und nicht darüber hinausgehen dürfen. Ferner heißt es dort, dass personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Wie bereits erwähnt, haben sämtliche in medizinischen Unterlagen, elektronischen Patientenakten und anderweitig in EPA-Systemen enthaltenen Daten als „sensible personenbezogene Daten" zu gelten. Dies hat wie gesagt zur Folge, dass abgesehen von einigen Sonderfällen die Verarbeitung solcher Daten generell untersagt ist. Gleichzeitig ist jede Ausnahme von dieser allgemeinen Regel genau zu bedenken und eng auszulegen. Dies gilt für Daten in der elektronischen Patienten-Kurzakte und für elektronische Verschreibungen (ePrescription).

Wie bereits erläutert, könnte die ausdrückliche Einwilligung betroffener Personen oder auch eine Maßnahme zum Schutz ihrer lebenswichtigen Interessen als angemessene Rechtsgrundlage für die Verarbeitung personenbezogener Gesundheitsdaten im Rahmen des epSOS-Projekts dienen. Die Verarbeitung solcher Daten muss jedoch **streng auf das beschränkt bleiben, was für das Erreichen der Zwecke von epSOS unbedingt erforderlich** ist. In der Patienten-Kurzakte und in ePrescription sollten nur Daten gespeichert werden, die für die Zwecke von epSOS erheblich sind.

Des Weiteren dürfen die Daten in diesen Diensten nicht länger als erforderlich aufbewahrt werden, wie es Artikel 6 Absatz 1 Buchstabe e der Richtlinie vorschreibt.

Jede Abfrage von personenbezogenen Daten aus dem epSOS-System sollte auf einen tatsächlichen Bedarf an spezifischen Daten zu der zu erbringenden medizinischen Versorgungsleistung oder Behandlung oder zu dem zu verschreibenden oder abzugebenden Medikament zurückgehen.

Wie bereits im WP 131 gesagt, haben Zugang zu den medizinischen Aufzeichnungen und damit zur Patienten-Kurzakte und zu Verschreibungen im Rahmen von epSOS nur jene medizinischen Fachkräfte oder Mitarbeiter von Gesundheitseinrichtungen, die an der Behandlung des Patienten mitwirken. Aus dem Wortlaut der der Arbeitsgruppe vorgelegten Unterlagen geht nicht hervor, dass die nationalen Kontaktstellen für die Zwecke von epSOS medizinische Daten speichern müssen; eine Speicherung solcher Daten durch die nationalen Kontaktstellen sollte daher vermieden werden.

Falls jedoch personenbezogene Daten beispielsweise bei den nationalen Kontaktstellen gespeichert werden müssen, sollte das epSOS-Projekt eine Höchstspeicherfrist vorsehen

sowie ein gemeinsames Verfahren bestimmen, das regelt, was mit den Daten nach Ablauf der Speicherfrist geschehen soll.

Der Zugriff auf Daten über das epSOS-System zu anderen Zwecken als der medizinischen Betreuung und Behandlung von Patienten oder der Verschreibung und Abgabe von Medikamenten sollte untersagt werden.

Aufgrund seiner eindeutigen Verknüpfung mit dem Grundsatz der Zweckbindung darf der Grundsatz der Verhältnismäßigkeit allerdings nicht isoliert betrachtet werden. Um angemessen beurteilen zu können, wie diese Anforderungen in die Praxis umgesetzt werden sollten, ist es erforderlich, den/die rechtmäßige(n) Zweck/e genau zu bestimmen, für den/die das epSOS-Projekt die personenbezogenen Daten eigentlich verarbeiten soll. Wie es in der Richtlinie heißt, muss es sich um festgelegte eindeutige Zwecke handeln, die also genau und klar bestimmt sind; daher wäre ein allgemeiner Ansatz nicht ausreichend. Die „Bereitstellung von medizinischer Betreuung und Behandlung“ und „die Verschreibung und Abgabe von Medikamenten“ sind natürlich rechtmäßige Zwecke, doch stellt sich die Arbeitsgruppe die Frage, ob sie die Ziele und Tätigkeiten von epSOS hinreichend genau beschreiben. Des Weiteren sind vor jeglicher Verarbeitung alle ins Auge gefassten Zwecke zu bestimmen, um zu gewährleisten, dass nicht mehr personenbezogene Daten als erforderlich verarbeitet werden, und um somit den Anforderungen des Gemeinschaftsrechts Genüge zu tun.

- **Ein eigenes Rechtsinstrument als Grundlage des Systems**

Es wäre zu überlegen, ob nicht auf EU-Ebene ein Rechtsinstrument zur Regulierung des epSOS-Systems und der Datenschutzaufgaben der verschiedenen Akteure (Anbieter von Gesundheitsdienstleistungen, nationale Kontaktstellen usw.) ausgearbeitet werden sollte. Dazu müsste das epSOS-Projekt in ein „EU-Projekt“ überführt werden und es müsste geprüft werden, ob die Europäische Kommission einen entsprechenden Beschluss annehmen könnte.[8]

Außerdem ist bis zum 25. Oktober 2013 die EU-Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung umzusetzen. Es ist wohl davon auszugehen, dass im einzelstaatlichen Recht der Richtlinie entsprechende Bestimmungen erlassen werden. Gemäß Artikel 14 der Richtlinie 2011/24/EU ist das Netzwerk für elektronische Gesundheitsdienste für die Erörterung der Anforderungen an den Informationsaustausch zwischen Mitgliedstaaten zuständig.

4. Das epSOS-Projekt: Organisatorische Fragen

Gegenstand dieses Kapitel sind nur die supranationalen epSOS-Verarbeitungen, die zusätzlich zu den bestehenden nationalen Systemen elektronischer Gesundheitsdienste entwickelt werden. Es befasst sich nicht mit den einzelstaatlichen Systemen, da diese als solche vom epSOS-Projekt nicht berührt werden.

[8] Vergleichbar mit der Entscheidung der Kommission 2008/49/EG vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI).

- **Hintergrund**

Das epSOS-System ist ein System für die Kommunikation zwischen allen teilnehmenden nationalen Kontaktstellen ohne zentrale Netzwerkschaltstelle.

Der Ablauf sieht folgendermaßen aus: Eine medizinische Fachkraft (Land B) fordert Informationen über den Patienten X mit Wohnsitz in Land A an. Die nationale Kontaktstelle (Land B) fordert daraufhin Daten über den Patienten X bei der nationalen Kontaktstelle (Land A) an. Sind in Land A irgendwelche Informationen über den Patienten X vorhanden, werden sie von der nationalen Kontaktstelle (Land A) an die nationale Kontaktstelle (Land B) übermittelt. Die nationale Kontaktstelle (Land B) übermittelt die Informationen über den Patienten X an die medizinische Fachkraft (Land B).

Das epSOS-System besteht also im Wesentlichen aus einer Vielzahl von Verbindungen zwischen zwei Punkten, auch wenn diese gemeinsamen Sicherheits- und Kommunikationsstandards unterliegen und von zentralen Diensten und Verzeichnissen unterstützt werden:

„Die epSOS-Schnittstellen in den nationalen Kontaktstellen sind für Dienstleistungen gedacht, die von anderen nationalen Kontaktstellen der epSOS-Infrastruktur bereitgestellt und in Anspruch genommen werden. epSOS-Schnittstellen haben für eine nationale Kontaktstelle von epSOS „normativen" Charakter. Eine nationale Kontaktstelle ist dann und nur dann „Teilnehmer" von epSOS, wenn sie bezüglich Struktur, Verhalten und Sicherheitskonzept die normativen Schnittstellen von epSOS einhält. Im Wesentlichen betrifft dies den Datenaustausch zwischen den nationalen Kontaktstellen, doch lassen sich jetzt oder in Zukunft einige für alle gleiche Dienste zentralisieren."[9]

„Es gibt eine Reihe von Informationsquellen, die für alle nationalen Kontaktstellen relevant sind und für alle nationalen Kontaktstellen im selben Zustand sein müssen. Dazu gehören beispielsweise gemeinsame Taxonomien, Schemata und WSE-Adressen von nationalen Kontaktstellen. Diese gemeinsamen Daten werden zentral verwaltet, um Unstimmigkeiten und Konflikte zwischen Versionen bei einer Ausdehnung von epSOS zu vermeiden."[10]

- **Die Verarbeitung**

Land B fragt gemäß Artikel 2 Buchstabe b der Richtlinie 95/46/EG die von Land A (durch Übermittlung) weitergegebenen Patientendaten ab.

Der Austausch von Patientendaten zwischen Land A und Land B kann als *Vorgangsreihe* (bestehend aus diesen beiden Vorgängen) gelten.

- **Wer ist der für die Verarbeitung Verantwortliche?**

- *Die nationale Kontaktstelle*

[9] D3.3.2 Final epSOS System Technical Specification (Endgültige technische Spezifikationen für das epSOS-System), Version 1.4 (April 2010), S. 64.

[10] D3.3.2 Final epSOS System Technical Specification, Version 1.4 (April 2010), S. 71.

Artikel 2 Buchstabe d der Richtlinie lautet:

„'Für die Verarbeitung Verantwortlicher' [bezeichnet] die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften geregelt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden".

Eine weitere Definition findet sich in der Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter"[11].

Nachstehend wird auf einige zentrale Elemente der Definition des „für die Verarbeitung Verantwortlichen" näher eingegangen.

- „entscheidet"

1) „Man sollte die spezifischen Verarbeitungen betrachten und ermitteln, wer über diese entscheidet, indem man als erstes die folgenden Fragen stellt: „Warum wird diese Verarbeitung durchgeführt? Wer hat sie veranlasst?"." (S. 13 der Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter")

2) „Der Begriff ‚für die Verarbeitung Verantwortlicher' [...] sollte in erster Linie gemäß dem Datenschutzrecht der Gemeinschaft ausgelegt werden, und er ist funktionell, da er die Verantwortung entsprechend dem tatsächlichen Einfluss und damit auf der Grundlage einer faktischen anstelle einer formalen Analyse zuweist." (S. 12 der Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter")

- „Zwecke und Mittel"

3 „Der Begriff „Mittel" bezeichnet nicht nur die technischen Methoden für die Verarbeitung personenbezogener Daten, sondern auch das „Wie" der Verarbeitung; dazu gehören Fragen wie „Welche Daten werden verarbeitet?", „Welche Dritte haben Zugang zu diesen Daten?", „Wann werden Daten gelöscht?" usw." (S. 17 der Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter")

Das epSOS-Projektpapier besagt Folgendes:

„Ein „Land" wird bei epSOS vertreten durch eine einzige juristische Person, die alle rechtlichen Verpflichtungen übernimmt und vertraglich verpflichtet ist, bei allen das Land betreffenden Fragen den „epSOS trusted domain" zu schützen. Diese juristische Person wird als nationale Kontaktstelle bezeichnet. [...] Die nationale Kontaktstelle ist in jedem Land

[11] Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (WP 169).

dafür verantwortlich, dass mit den Patientenrechten im Einklang mit dem jeweiligen innerstaatlichen Recht angemessen umgegangen wird [...].“[12]

Diese Ansicht von epSOS stimmt mit der vorstehenden Analyse von Artikel 2 Buchstabe d der Richtlinie überein.

Ausgehend von der Begriffsbestimmung des „für die Verarbeitung Verantwortlichen“ im WP 169 einerseits und der Darstellung der Fakten durch das epSOS-Projekt selbst andererseits wird deutlich, dass die nationale Kontaktstelle in Land A der für die Verarbeitung Verantwortliche für die *Weitergabe* der Patientendaten und die nationale Kontaktstelle im Land B der für die Verarbeitung Verantwortlich für die *Abfrage* der Patientendaten ist.
Aus den Antworten auf den Fragebogen geht jedoch hervor, dass sich die Lage von Land zu Land unterschiedlich darstellt.[13]

Die EU-Ebene spielt aufgrund der Erbringung zentraler Dienstleistungen durch das epSOS-Projekt sowie der Sicherheits- und Kommunikationsstandards ebenfalls eine gewisse regulatorische Rolle, doch ist damit die EU nicht unmittelbar in die Datenverarbeitung eingebunden. Weitere Fragen sind die Aufnahme neuer Teilnehmer und die Aufklärung betroffener Personen (z. B. www.epsos.eu). Sollte dieses Pilotsystem zu einer ständigen Einrichtung werden, könnte es sinnvoll sein, ein eigenständiges Gremium einzusetzen, das allein oder zusammen mit den teilnehmenden nationalen Kontaktstellen als für die Verarbeitung Verantwortlicher fungiert.

- *Die Anbieter von Gesundheitsdienstleistungen*

Zunächst einmal sind Anbieter von Gesundheitsdienstleistungen für die Verarbeitung Verantwortliche in Bezug auf die *Erstellung* der medizinischen Aufzeichnungen, aus denen die epSOS-Datensätze abgeleitet und dann ins Ausland übermittelt werden.

In bestimmten EU-Mitgliedstaaten wird davon ausgegangen, dass alle teilnehmenden Anbieter von Gesundheitsdienstleistungen gemeinsam für die Verarbeitung durch die nationale Kontaktstelle verantwortlich sind, wobei die nationale Kontaktstelle als Auftragsverarbeiter auftritt.[14]

Der Begriff der *gemeinsamen Kontrolle* ist im WP 169 analysiert worden. Hintergrund ist die *Funktion* des Begriffs „für die Verarbeitung Verantwortlicher“:

"[D]ie Bestimmungen über die Rechte der betroffenen Person – das Recht auf Information, Auskunft, Berichtigung, Löschung und Sperrung sowie das Recht, Widerspruch gegen die Verarbeitung einzulegen (Artikel 10 bis 12 und Artikel 14), wurden so formuliert, dass sie dem für die Verarbeitung Verantwortlichen Pflichten auferlegen. Der für die Verarbeitung Verantwortliche spielt auch in den Bestimmungen über die Meldung und die Vorabkontrolle

---

[12] D2.1.2 Legal and Regulatory Constraints on epSOS Design- Participating Member States, January 31,2010, Final version, p. 14 (Rechtliche und regulatorische Vorgaben für Mitgliedstaaten, die am Entwurf von epSOS teilnehmen, 31. Januar 2010, endgültige Fassung, S. 14).

[13] Beispielsweise in dezentralisierten Systemen. Siehe die Antworten auf Frage 8e in dem Fragebogen zum epSOS-Projekt, Patienten-Kurzakte und elektronischen Rezept (August 2011). S. 27f (als Anlage beigefügt).

[14] In manchen Ländern gilt jeder einzelne Anbieter von Gesundheitsdienstleistungen als Stelle, die gemeinsam mit der nationalen Kontaktstelle für die Verarbeitung durch die nationale Kontaktstelle verantwortlich ist.

eine zentrale Rolle (Artikel 18 bis 21). Und schließlich haftet der für die Verarbeitung Verantwortliche auch grundsätzlich für jeden Schaden, der wegen einer rechtswidrigen Verarbeitung entsteht (Artikel 23).

Dies bedeutet, dass der Begriff „für die Verarbeitung Verantwortlicher" in erster Linie dazu dient zu bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und wie die betroffenen Personen ihre Rechte in der Praxis ausüben können. Anders ausgedrückt: Er dient dazu, Verantwortung zuzuweisen." (S. 6)

Diese Funktion bestimmt (mit), inwieweit gemeinsame Kontrolle annehmbar ist.
„Bei der Bewertung der gemeinsamen Kontrolle ist somit zu beachten, dass einerseits eine vollständige Einhaltung der Datenschutzbestimmungen gewährleistet sein muss, andererseits aber eine größere Zahl von für die Verarbeitung Verantwortlichen auch zu einer größeren Komplexität und zu einer mangelnden Klarheit bei der Zuweisung der Verantwortung führen kann. Letzteres würde das Risiko bergen, dass die gesamte Verarbeitung aufgrund mangelnder Transparenz unrechtmäßig wäre, und würde den Grundsatz der Verarbeitung nach Treu und Glauben verletzen." (S. 29)

Wenn also alle in einem Land teilnehmenden Anbieter von Gesundheitsdienstleistungen als gemeinsam für die Verarbeitung durch die nationale Kontaktstelle Verantwortliche gelten[15], kann eine solch weit gestreute Kontrolle erhebliche Bedenken hervorrufen.[16] **Gemindert werden könnten diese Bedenken, indem angemessene Maßnahmen zum Schutz der Patientenrechte**[17] **ergriffen werden und für Transparenz gesorgt wird.**

- **Schlussbemerkung zur Regulierung von epSOS**

Sind die Zwecke und Mittel der epSOS-Verarbeitung in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtvorschriften bestimmt werden (Artikel 2 Buchstabe d der Richtlinie).

- **Kontrolle, Vorabkontrolle und Meldungen**

Nach dieser Analyse gibt es derzeit keine Stelle, die gemäß den Artikeln 4 und 28 der Richtlinie die Einhaltung der Datenschutzbestimmungen bei den epSOS-Verarbeitungen insgesamt kontrolliert. Jeder Datenschutzbehörde kontrolliert die eigene nationale Kontaktstelle. In Anbetracht des grenzüberschreitenden Charakters der epSOS-Verarbeitung ist eine Zusammenarbeit zwischen nationalen Datenschutzbehörden bei der Kontrolle des epSOS-Projekts dringend angeraten (siehe Artikel 28 Absatz 6 zweiter Satz der Richtlinie).

Sofern im anwendbaren einzelstaatlichen Recht vorgesehen, hat jeder für die Verarbeitung Verantwortliche vor Aufnahme irgendeiner Verarbeitung bei der Datenschutzbehörde seines eigenen Mitgliedstaats diese Verarbeitung zu melden (Artikel 18 Absatz 1 der Richtlinie).

---

15 Oder wenn davon ausgegangen wird, dass jeder einzelne Anbieter von Gesundheitsdienstleistungen gemeinsam mit der nationalen Kontaktstelle für die Verarbeitung Verantwortlicher ist.

16 Siehe auch Beispiel Nr. 15 in WP 169, S. 29.

17 Siehe S. 17 Absatz 3 mit einem Beispiel für eine solche Maßnahme.

Je nach einzelstaatlichem Recht wird die Verarbeitung vor ihrem Beginn geprüft (Artikel 20 der Richtlinie).

5. Transparenz

- **Auskunft und Berichtigung, Löschung und Sperrung**

Unrichtige oder unvollständige Daten sind zu löschen, zu berichtigen oder zu sperren. Bei der Beurteilung der Frage, ob Daten sachlich richtig sind, ist den Zwecken, für die die Daten erhoben wurden oder für die sie weiter verarbeitet werden, Rechnung zu tragen. Das bedeutet, dass die Richtigkeit einer ärztlichen Diagnose unter Berufung auf die Grundsätze des Datenschutzes nur dann angefochten werden kann, wenn die Identität des Patienten falsch angegeben oder ein ähnlicher grober Fehler begangen wurde.

Damit betroffene Personen ihre Rechte wahren können, sollte eine gemeinsame epSOS-Website eingerichtet werden, auf der die in den einzelstaatlichen Rechtsvorschriften aller teilnehmenden Länder verankerten Rechte betroffener Personen dargestellt werden. Die Angaben auf dieser Website sollten genau die Rechte, Bedingungen und praktischen Modalitäten im Einklang mit den jeweiligen einzelstaatlichen Rechtsvorschriften beschreiben. Diese Informationen sollten verständlich formuliert und im Internet in den Sprachen der teilnehmenden Staaten leicht abrufbar sein.

Eine betroffene Person sollte allen für die Verarbeitung Verantwortlichen sowie allen anderen am Informationsaustausch im Rahmen des epSOS-Projekts Beteiligten Fragen zum Thema Auskunft und zur Möglichkeit der Berichtigung, Löschung oder Sperrung stellen können. Ein Antrag auf Auskunft oder auf Berichtigung/Löschung/Sperrung von Daten, der bei einem epSOS-Partner eingereicht wird, der die Daten des Antragstellers nicht verarbeitet, ist an den zuständigen für die Verarbeitung Verantwortlichen innerhalb des epSOS-Systems weiterzuleiten, auch wenn dieser seinen Sitz in einem anderen Mitgliedstaat hat.

Das epSOS-Projekt sollte prüfen, ob betroffenen Personen nicht (auf elektronischem Wege) ein direkter Lesezugriff auf ihre jeweiligen Daten gewährt werden kann. Das Datenschutzrecht auf Auskunft beispielsweise nach Artikel 12 der Richtlinie 95/46/EG muss nicht immer zwangsläufig *direkte* Auskunft bedeuten. Direkte Auskunft könnte natürlich erheblich das Vertrauen in das epSOS-System fördern. Aus Sicht des Datenschutzes wäre die Vorbedingung für die Gewährung eines direkten Zugriffs eine sichere elektronische Personenidentifizierung und –Authentisierung, um zu verhindern, dass sich Unbefugte Zugang zu den Daten verschaffen können. (siehe WP 131, S. 17)

Alle für die Verarbeitung Verantwortlichen, die mit epSOS-Daten umgehen, müssen unabhängig von der Ebene, auf der sie angesiedelt sind, oder von ihrer Rolle (z. B. als Anbieter von Gesundheitsdienstleistungen, Aussteller von elektronischen Verschreibungen, nationale Kontaktstelle usw.) betroffenen Personen das *Recht auf Auskunft und das Recht auf Berichtigung/Löschung/Sperrung der eigenen Daten* einräumen, unabhängig davon, ob die betroffene Person ihren Wohnsitz im eigenen oder in einem anderen Mitgliedstaat hat und unabhängig davon, ob die betreffenden Daten von für die Verarbeitung Verantwortlichen in anderen Mitgliedstaaten stammen.

Das Recht auf Auskunft und auf Berichtigung/Löschung/Sperrung ist im Einklang mit den einzelstaatlichen Rechtsvorschriften anzuwenden, denen der für die Verarbeitung Verantwortliche unterliegt. In Ausnahmefällen kann das Recht betroffener Personen auf Auskunft und Berichtigung/Löschung/Sperrung von Daten gemäß einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG eingeschränkt oder beschränkt werden.

Kein für die Verarbeitung Verantwortlicher, der Daten im Rahmen des epSOS-Projekts verarbeitet, darf die Auskunft über Daten oder deren Berichtigung/Löschung/Sperrung nur mit der Begründung verweigern, der für die Verarbeitung Verantwortliche habe die Daten nicht selber in epSOS eingegeben.

Einschlägiges Recht: Gemäß Artikel 12 der Richtlinie garantieren die Mitgliedstaaten jeder betroffenen Person das Recht auf Berichtigung, Löschung oder Sperrung von Daten und auf bestimmte Auskünfte von Seiten des für die Verarbeitung Verantwortlichen. Gemäß Artikel 13 Absatz 1 der Richtlinie können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Pflichten und Rechte gemäß Artikel 12 beschränken, sofern eine solche Beschränkung zum Schutz besonderer, genau spezifizierter Interessen notwendig ist.

- **Meldung**

Alle für die Verarbeitung Verantwortlichen, die mit epSOS-Daten umgehen, *müssen* unabhängig von der Ebene, auf der sie angesiedelt sind, oder von ihrer Rolle (z. B. als Anbieter von Gesundheitsdienstleistungen, Aussteller von elektronischen Verschreibungen, nationale Kontaktstelle usw.) den Vorgang bei ihrer nationalen Kontrollstelle gemäß den einschlägigen nationalen Rechtsvorschriften *melden*, unabhängig davon, ob die betroffene Person ihren Wohnsitz im eigenen oder einem anderen Mitgliedstaat hat und unabhängig davon, ob die betreffenden Daten von für die Verarbeitung Verantwortlichen in anderen Mitgliedstaaten stammen.

Einschlägiges Recht: Artikel 18 der Richtlinie 95/46/EG sieht die Pflicht zur Meldung bei der Kontrollstelle vor, bevor eine teilweise oder vollständig automatisierte Verarbeitung durchgeführt wird, und benennt auch die Fälle, in denen dieser Pflicht nicht nachzukommen ist.

6. Datensicherheit

In Anbetracht der Arbeitsweise von epSOS und des hochsensiblen Charakters der verarbeiteten Daten sind technische und organisatorische Maßnahmen zu treffen, um einer Vernichtung, einem zufälligen Verlust, einer Veränderung sowie unbefugtem Zugriff auf die personenbezogenen Daten vorzubeugen. Darüber hinaus soll mit solchen Maßnahmen jeder anderen Form der unrechtmäßigen Verarbeitung der Daten vorgebeugt werden (siehe Artikel 17 der Richtlinie 95/6/EG).

Diese Maßnahmen sollten dem hochsensiblen Charakter der zu verarbeitenden Daten, der zentralen Rolle der IKT im Rahmen des Projekts und der grenzüberschreitenden Dimension der Datenübermittlungen im Rahmen von epSOS Rechnung tragen. Folglich ist ein hohes Datenschutzniveau einzuhalten, das den aus dem epSOS-System resultierenden Risiken in angemessener Weise Rechnung tragen sollte.

Dieser Schutz muss während der gesamten Verarbeitung wirksam sein. Zu diesem Zweck sollten eine Verständigung aller Beteiligten auf gemeinsame Mindeststandards erfolgen.

Es sind also angemessene Maßnahmen und Regelungen erforderlich, mit denen unter den epSOS-Partnern Folgendes gewährleistet wird:

a) Vertraulichkeit – Daten sind gegen unbefugten Zugriff oder unbeabsichtigte Weitergabe geschützt - nur befugte Nutzer haben Zugang zu den Informationen und anderen Systemressourcen;

b) Integrität – die Daten sind gegen unbefugte Änderungen geschützt;

c) Rückverfolgbarkeit - jede Mitteilung und jede Datentransaktion lässt sich auf eine leicht nachprüfbare Weise bis zu einem bestimmten Urheber zurückverfolgen.

Um den Sicherheitsgrundsätzen und den spezifischen Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten im epSOS-System in vollem Umfang Rechnung tragen zu können, sind insbesondere folgende Maßnahmen und Regelungen erforderlich:

- Erstens sollten jedem Einzelnen, der mit der Durchführung des Projekts befasst ist, eindeutige schriftliche Weisungen für eine ordnungsgemäße Nutzung des epSOS-Systems an die Hand gegeben werden, damit keine Sicherheitsrisiken entstehen und nicht gegen die Sicherheitsvorschriften verstoßen wird. Solche Weisungen sollten den Rollen/Funktionen der einzelnen Beteiligten (ärztliches Personal, Beschäftigte in Apotheken, Personal an Behandlungsorten) Rechnung tragen. Die jeweiligen Funktionen und Zuständigkeiten der einzelnen Kategorien sind klar zu benennen, damit ihre Verantwortlichkeiten bezüglich der Datenverarbeitung festgelegt werden können.

- Zweitens sollten entsprechende Vorkehrungen im Hinblick auf die Speicher- und Archivierungssysteme der Patienten-Kurzakten und elektronischen Verschreibungen getroffen werden, um die Daten gegen ungefugten Zugriff, Diebstahl und/oder teilweisen/völligen Verlust von Speichermedien und tragbaren/fest installierten Verarbeitungssystemen zu schützen; dabei sollten Verschlüsselungstechniken[18] angewandt werden.

- Ebenso sind für den Datenaustausch sichere Kommunikationsprotokolle und ein Verschlüsseln der Daten von Endstelle zu Endstelle vorzusehen, die auf Verschlüsselungsstandards für eine sichere elektronische Kommunikation basieren. Dies ist erforderlich, um die Erlangung/Weitergabe der Informationen in Gegenwart von Dritten zu verhindern, über die der Patient oder die befugten Organisationen des Gesundheitswesens keine Kontrolle haben. Die Endpunkte der Verschlüsselung müssen sich in Umgebungen befinden, die entweder direkt vom Patienten oder von den vom Patienten zur Verarbeitung seiner medizinischen Daten ermächtigten professionellen Organisationen des Gesundheitswesens kontrolliert werden. Werden Gesundheitsdaten mit Anwendungen übermittelt, die sich öffentlich zugänglicher

[18] Die Verschlüsselung sensibler personenbezogener Daten ist in mehreren Mitgliedstaaten vorgeschrieben.

Netze (z. B. Internet) bedienen, sollte das System die Nutzung zuverlässiger digitaler Zertifikate sowohl für die Serversysteme, die den Dienst erbringen, als auch für die Client-Geräte vorsehen, mit denen die Daten abgerufen werden. Die Integrität und Authentizität der Gesundheitsdaten von einem Endpunkt zum anderen muss sich lückenlos nachweisen lassen.

- Besondere Aufmerksamkeit ist dem Aufbau eines zuverlässigen und wirksamen elektronischen Identifizierungssystems mit eindeutiger Authentisierung zu widmen. Dies gilt gleichermaßen für medizinisches Fachpersonal wie für die Patienten.

  Weiter sollten Verfahren zur regelmäßigen Überprüfung der Authentifizierungsdaten und der dem Fachpersonal zugeteilten Berechtigungsprofile eingeführt werden. Der für die Verarbeitung der Daten Verantwortliche sollte mit besonderen Verfahren den Online-Zugang und die Online-Abfrage durch die betroffenen Personen verhindern, wenn die Gefahr besteht, dass die Vertraulichkeit der Daten nicht mehr gewährleistet ist – gleichgültig, ob die Gefahr von dem für die Verarbeitung der Daten Verantwortlichen entdeckt oder von der betroffenen Person gemeldet wurde (z. B. bei Diebstahl/Verlust von Authentifizierungsdaten, unbefugtem Zugang zum System und anderen Verstößen gegen die Datenschutzvorschriften usw.).

- Ob ein Sicherheitsniveau angemessen ist, hängt auch von der Fähigkeit des Systems ab, in nachprüfbarer Weise die einzelnen Vorgänge, die die Datenverarbeitung insgesamt ausmachen, korrekt aufzuzeichnen und rückzuverfolgen; dies gilt insbesondere für Anträge auf Datenzugriff und jeglichen Umgang mit den Daten. Das System sollte ferner regelmäßige interne Kontrollen und Überprüfungen der Echtheit der Berechtigungen umfassen. Dementsprechend sollten zur Überprüfung der Zugriffe auf die Datenbank angemessene interne und externe Kontrollen in Form von Audit-Log-Systemen durchgeführt und spezifische Warnungen ergehen, wenn riskantes und/oder von der Norm abweichendes Verhalten festgestellt wird. Um ein reibungsloses Funktionieren all dieser Elemente zu gewährleisten, sollte das System regelmäßig einer Überprüfung unterzogen werden.

- Bei der Übermittlung und/oder Speicherung der Back-up-Daten sollte (z. B. durch Verschlüsselung) ein unbefugter Zugriff auf die Daten und/oder ihre unbefugte Änderung verhindert werden. Es sollte gewährleistet sein, dass alle epSOS-Akteure dem Berufsgeheimnis oder ähnlichen Regelwerken unterliegen, wie dies auch für Angehörige der Gesundheitsberufe gilt.

- Insbesondere im Hinblick auf das System der elektronischen Verschreibungen sollten die vorstehend genannten Anforderungen mit zusätzlichen Maßnahmen einhergehen, mit denen sichergestellt wird, dass Akteure aus dem pharmazeutischen Bereich Zugang zu digitalen Verschreibungen nur erhalten, um die verschriebenen Medikamente abzugeben, und sie sollten verhindern, dass in der Apotheke in irgendeiner Form eine mit epSOS in Zusammenhang stehende Rezeptdatenbank aufgebaut wird.

- Stellt sich in Notsituationen heraus, dass auf Informationen ohne die erforderlichen Genehmigungen zugegriffen werden muss, ist dies ebenso wie jeder spätere Zugang zu den Daten (einschließlich aller Datenverarbeitungsvorgänge) aufzuzeichnen und zu

prüfen; auch zu den Gründen für den besonderen Zugriff auf die Daten sind Aufzeichnungen aufzubewahren.

7. Schlussfolgerungen und Empfehlungen

- Alle in medizinischen Unterlagen, elektronischen Patientenakten und EPA-Systemen gespeicherten Daten sind „sensible personenbezogene Daten“ und unterliegen damit Artikel 8 der Richtlinie.
- Für die Verarbeitung von Daten im Bereich der Gesundheitsversorgung muss eine klare Rechtsgrundlage gegeben sein. In Ermangelung anderer legitimer Grundlagen kann es sich hierbei um die zweistufige Einwilligung der betroffenen Person handeln (zunächst in die Teilnahme am System im Allgemeinen und sodann für eine konkrete Behandlung/Medikamentenabgabe). Das epSOS-Projekt könnte prüfen, ob nicht den Patienten die Möglichkeit gegeben werden sollte, ihre erste Einwilligung auch im Land B zu geben, beispielsweise über eine gesicherte Internetverbindung.
- Die Verarbeitung personenbezogener und sensibler Daten kann ohne zweite Einwilligung im Land B geboten sein, wenn die lebenswichtigen Interessen einer betroffenen Person oder eines Dritten geschützt werden müssen und die betroffene Person in der betreffenden Situation physisch oder rechtlich außerstande ist, ihre Einwilligung zu geben.
- Eine der Hauptvoraussetzungen für die Gültigkeit einer Einwilligung besteht darin, dass die der betroffenen Person gegebenen Informationen den Anforderungen von Artikel 10 und 11 der Richtlinie genügen.
- Die Verarbeitung personenbezogener Daten ist strikt auf das Mindestmaß zu beschränken, das für das Erreichen der Zwecke von epSOS erforderlich ist, die wiederum genau festgelegt, eindeutig und rechtmäßig sein müssen.
- Um zu gewährleisten, dass Daten nicht länger als erforderlich im epSOS-System gespeichert werden, sollte eine Höchstspeicherfrist beschlossen und ein gemeinsames Verfahren für den Umgang mit den Daten nach Ablauf dieser Speicherfrist festgelegt werden.
- Jeder Abfrage von personenbezogenen Daten aus dem epSOS-System sollte ein tatsächlicher Bedarf an spezifischen Daten zu der zu erbringenden medizinischen Versorgungsleistung oder Behandlung oder zu dem zu verschreibenden oder abzugebenden Medikament zugrunde liegen.
- Aufgrund des grenzüberschreitenden Charakters der epSOS-Verarbeitung wird eine Zusammenarbeit zwischen den Datenschutzbehörden bei der Kontrolle von epSOS nachdrücklich empfohlen.
- Alle für die Verarbeitung Verantwortlichen, die mit epSOS-Daten umgehen, müssen den Vorgang bei ihrer nationalen Kontrollstelle gemäß den nationalen Rechtsvorschriften melden, unabhängig davon, ob die betroffene Person ihren Wohnsitz im eigenen oder in einem anderen Mitgliedstaat hat und unabhängig davon, ob die betreffenden Daten von für die Verarbeitung Verantwortlichen in anderen Mitgliedstaaten stammen.
- epSOS benötigt ein hohes Maß an IT-Sicherheit. Um den in der Richtlinie niedergelegten Sicherheitsgrundsätzen und den spezifischen Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten im epSOS-System in vollem Umfang Rechnung tragen zu können, sind insbesondere folgende Maßnahmen und Regelungen erforderlich:

- Allen Personen, die mit der Durchführung des Projekts befasst sind, sollten eindeutige schriftliche Weisungen für eine ordnungsgemäße Nutzung des epSOS-Systems an die Hand gegeben werden, damit keine Sicherheitsrisiken entstehen und nicht gegen die Sicherheitsvorschriften verstoßen wird.
- Durch entsprechende Vorkehrungen in den Systemen zur Speicherung und Archivierung der Patienten-Kurzakten und Verschreibungen ist sicherzustellen, dass die Daten gegen unbefugten Zugriff, Diebstahl und/oder vor dem teilweisen/völligen Verlust geschützt sind.
- Für den Datenaustausch sind mit Hilfe von Verschlüsselungsstandards für eine sichere elektronische Kommunikation sichere Kommunikationsprotokolle und ein Verschlüsseln der Daten von Endstelle zu Endstelle vorzusehen.
- Besondere Aufmerksamkeit ist dem Aufbau eines zuverlässigen und wirksamen elektronischen Identifizierungssystems mit eindeutiger Authentisierung (sowohl des teilnehmenden Fachkräfte als auch der teilnehmenden Patienten) zu widmen.
- Das System muss in der Lage sein, in nachprüfbarer Weise die einzelnen Vorgänge, die die Datenverarbeitung insgesamt ausmachen, korrekt aufzuzeichnen und rückzuverfolgen.
- Bei der Übermittlung und/oder Speicherung der Back-up-Daten sollte (z. B. durch Verschlüsselung) ein unbefugter Zugriff auf die Daten und/oder ihre unbefugte Änderung verhindert werden.
- Im Hinblick auf das System der elektronischen Verschreibungen sollten zusätzliche Maßnahmen ergriffen werden, mit denen sichergestellt wird, dass Akteure aus dem pharmazeutischen Bereich Zugang zu digitalen Rezepten nur erhalten, um die verschriebenen Medikamente abzugeben.
- In Notfällen sollte jeder Zugriff aufgezeichnet und nachgeprüft werden.

- Alle für die Verarbeitung der Daten Verantwortlichen, die mit epSOS-Daten umgehen, müssen betroffenen Personen das Recht auf Auskunft und das Recht auf Berichtigung, Löschung oder Sperrung der eigenen Daten einräumen.
- Eine betroffene Person sollte allen für die Verarbeitung Verantwortlichen sowie allen anderen am Informationsaustausch im Rahmen von epSOS Beteiligten Fragen zu ihrem Auskunftsrecht sowie zu Anträgen auf Berichtigung/Löschung/Sperrung stellen können. Ein Antrag auf Auskunft oder auf Berichtigung/Löschung/Sperrung von Daten, der bei einem epSOS-Partner eingereicht wird, der die Daten über die betroffene Person nicht verarbeitet, ist an den zuständigen für die Verarbeitung Verantwortlichen innerhalb des epSOS-Systems weiterzuleiten, auch wenn dieser seinen Sitz in einem anderen Mitgliedstaat hat.
- epSOS sollte prüfen, ob betroffenen Personen nicht (auf elektronischem Wege) ein direkter Lesezugriff auf ihre jeweiligen Daten gewährt werden kann.
- Es sollte eine gemeinsame epSOS-Website eingerichtet werden, auf der die betroffenen Personen über ihre Rechte aufgeklärt werden, die sie gemäß den Rechtsvorschriften der einzelnen teilnehmenden Länder besitzen. Die Website sollte eine genaue Beschreibung der in den einzelnen Mitgliedstaaten geltenden Rechte, Bedingungen und praktischen Modalitäten enthalten.

Brüssel, den 25. Januar 2012

Für die Arbeitsgruppe
Der Vorsitzende