UNIVERSITÄT LEIPZIG

Lehrstuhl für Strafrecht, Strafprozessrecht,
Kriminologie, Jugendstrafrecht und
Strafvollzugsrecht

Compliance By Design?

Strafrechtliche Grenzen der Leistungsdelegation

DGRI e.V. Beiratstagung am 12.05.2012

“Cloud Services und Compliance by Design”

Prof. Dr. Hendrik Schneider

Einstiegsfall

Ein Krankenhaus arbeitet mit einer Software (Krankenhausinformationssystem, KIS), die Patientendaten verwaltet. Es existiert ein Zugriffsberechtigungsschlüssel, der über einen Notfallbutton überwunden werden kann. Der Notfallbutton ist erforderlich, um z.B. im Fall einer Einlieferung auf der Intensivmedizin unabhängig von der Zugriffsberechtigung alle Daten sofort verfügbar zu haben.

Einstiegsfall

Praxisfall 1: Das freigestellte Betriebsratsmitglied X des KH verfügt über einen abteilungsbezogenen Zugriffsschlüssel. Man hatte im Rahmen seiner Freistellung vergessen, diesen zu löschen. Er will Munition gegen den Geschäftsführer sammeln und besorgt sich (durch Benutzung des Notfallbuttons) die Laborwerte des GF aus der Datenbank. Schon bald kursieren Gerüchte im Unternehmen, GF habe die Leberwerte eines Alkoholikers. Eine Prüfung des GF ergibt, dass der Notfallbutton seit Jahren die Standardroutine des Zugriffs auf Patientendaten im KH darstellt.

Einstiegsfall

Praxisfall 2: Vertragsarzt Dr. X, der im KH als Honorararzt tätig ist, erzielt beträchtliche Nebeneinnahmen aus klinischen Studien. Um eine möglichste breite Fallbasis von Studienteilnehmern zu generieren, „screent“ er mittels Notfallbutton die Patientendaten und spricht gezielt Patienten auf seine Studie an. Erst als gegen Dr. X wegen § 299 StGB ermittelt wird, fliegt auch die innovative Strategie der Patientenrekrutierung auf.

Ergänzende Informationen zu KIS

KIS ist ein dezentrales System mit Arbeitsplatzsystemen, Abteilungssytemen und einer zentralen Datenbank. Folgende Anforderungen ergeben sich:

- Verfügbarkeit der Daten zur rechten Zeit am rechten Ort.
- Sicherer Datenverkehr nach dem need to know Prinzip, z.B. zur Abteilung Medizincontroling und zur Abrechnung.
- Gewährleistung reibungsloser Kommunikation der Subsysteme.
- Definition von Verantwortlichkeiten, Prozeduren und Zugriffsrechten.

Konsequenzen & Fragestellungen

In beiden Fällen liegen gewichtige Verletzungen von Datenschutzbestimmungen vor. Es drohen (Fall 2) Reputationsschäden:

Welche Präventionsinstrumente sind tragfähig? Compliance by design? Compliance by detection? Automatisierung von Compliance?

Das Strafrecht/OWiG ist zuständig! Wer ist strafrechtlich verantwortlich? Risiko-outsourcing?

Agenda

1. **Möglichkeiten & Strukturen automatisierter Compliance**

2. **Konsequenzen für die Zuordnung strafrechtlicher Verantwortlichkeit**

3. **Schlussbetrachtung**

Grundbegriffe

Compliance: („Regeltreue“) = Inbegriff von Maßnahmen zur Einhaltung von Gesetzen und Unternehmensrichtlinien

Zwei Ansätze:

- präventiv/prospektiv = Compliance by Design (CbDgn)
- reaktiv/retrospektiv = Compliance by Detection (CbDet)

Automatisierung von Compliance = methodischer Ansatz, durch den Gesetzestexte und Regelungswerke in IT Systeme übersetzt werden

Grundbegriffe

Compliance by Design

- Prozesse oder IT Produkte werden so strukturiert, dass Compliance Verstöße nicht vorkommen können oder die Wahrscheinlichkeit ihres Auftretens reduziert wird.
- Dominante Perspektive, soweit Juristen mit Compliance Aufgaben betraut werden.
- Bisheriger Schwerpunkt: Strukturierung von Arbeitsabläufen über vordefinierte Prozesse, die bei regelkonformer Anwendung Compliance sicherstellen. Bsp.: Begrenzung des Handlungsspielraums der Abteilung „Vertrieb“ eines Unternehmens durch eine Anti-Korruptionsrichtlinie.

Compliance by Detection

- Im Rahmen eines Audits werden tatsächliche Ereignisse mit Compliance Regularien verglichen und Compliance Verstöße identifiziert.
- Dominante Perspektive, soweit Compliance Aufgaben primär durch die Innenrevision wahrgenommen werden.
- Bisher dominieren anlassbezogene Compliance Audits, z.B. bei Vorliegen von Verdachtsmomenten oder im Rahmen von Integrity Due Diligence Prüfungen.

Automatisierung von Compliance

Hypothesen:

- Die Verbindung beider Compliance Ansätze im Rahmen technischer Lösungen ist möglich!
- Compliance as a Service ist denkbar!
- In abzusteckenden Grenzen können auch Haftungsrisiken ausgelagert werden!

Abläufe – Compliance by Design

1. <u>Aus der Perspektive der Macher von KIS:</u>

Ermittlung regulatorischer Anforderungen. Welche Bestimmungen des Datenschutzes müssen im Gesundheitswesen beachtet werden, z.B. SächsDschG (§ 9ff.), § 203 StGB: adäquate Balance zwischen **Verfügbarkeit**, **Vertraulichkeit** und **Integrität**.

Abläufe – Compliance by Design

2. Ableitung der Compliance Anforderungen:

2.1 Identifikation von Bedrohungsszenarien:

- Besucher an unbeaufsichtigten Geräten
- Nichtmedizinisches Personal (Putzdienste)
- Reparaturdienst (Austausch von Festplatten)
- Presse (Promis im KH)

Abläufe – Compliance by Design

2.2 Identifikation von Zugriffsrechten

2.3 Identifikation von Schutzstufen für Daten:

- Patientenstammdaten
- Medizinische Patientendaten
- Besonders empfindliche Patientendaten (Unterbringungen, psych. Diagnosen)

Abläufe – Compliance by Design

3. Übersetzung der Compliance Anforderungen in eine formale Form = Policy Sprache

- Definition erlaubter Aktionen und Zustände (Zugriff auf Daten, Löschen von Daten, Eingabe von Daten).
- Definition verbotener Aktionen und Zustände
- Definition von Verpflichtungen, zum Beispiel Sicherung

⇒ Schlüssel zur Automatisierung, weil die Strukturvorgaben den Grad der möglichen Automatisierung bestimmen

Abläufe – Compliance by Design

4. <u>Identifikation von Regeln, die nicht zur Laufzeit umgesetzt werden können:</u>

   - Identifikation von Red Flags! Z.B. Automatischer Report an Datenschutzbeauftragten des KH, wenn die Betätigung des Notfallbuttons eine definierte Häufigkeitsgrenze übersteigt oder wenn zeitliche Grenzen von Zugriffsberechtigungen abgelaufen sind.
   - Automatischer Report von Obligationen, z.B. Datensatz muss zu einem bestimmten Zeitpunkt gelöscht werden.

Zurück zu den Beispielfällen

Verantwortlichkeit der beiden Täter gem. §§ 38, 39 Sächsisches Datenschutzgesetz:

- § 38 Absatz 1: Ordnungswidrig handelt, wer
  1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind [...]
  c) für sich oder einen anderen abruft oder auf andere Weise verschafft.
- § 39:

  Wer eine der in § 38 Abs. 1 Nr. 1 bis 8 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

Verantwortlichkeit der GF

⇒ Im Fall 2 steht der Landesdatenschutzbeauftragte vor der Tür.

⇒ Ferner steht eine Verantwortlichkeit der Organe des KH wegen § 130 OWiG im Raum.

Delegation strafrechtlicher Haftungsrisiken?

Geschäftsführung

- Bei Vorsatz: Beihilfe zu einer Haupttat durch Unterlassen (Ausnahme)
- Bei Verletzung der Aufsichtspflicht, §§ 130, 9 OWiG (Regel)

Datenschutzbeauftragter oder Compliance Verantwortlicher auf Unternehmensebene

- Bei Vorsatz: Beihilfe zu einer Haupttat durch Unterlassen (Ausnahme)
- Eigene Verantwortlichkeit gem. § 130 OWiG aus Rechtsgründen unmöglich (kein tauglicher Täter)

Vertragspartner/KIS

- Keine eigenen strafrechtlichen Risiken
- Begründung: Die einschlägigen Delikte sind als Tätigkeitsdelikte ausgestaltet (verarbeiten, abrufen, verschaffen). Bei Erfolgsdelikten scheitert ein Regress idR an der objektiven Zurechnung, am Vorsatz, am Eigenverantwortlichkeitsprinzip.

2. Konsequenzen für die Zuordnung strafrechtlicher Verantwortlichkeit

Delegation strafrechtlicher Haftungsrisiken?

GF hat Interesse an **Verantwortungsdelegation**:

- Die Implementierung eines CO oder Datenschutzbeauftragten kann ihn vor § 130 OWiG schützen
- „Compliance as a Service“ kann ihn schützen sofern über das Produkt die Sicherheit gewährleistet ist und kein Anwendungsfehler vorliegt

Schlussbetrachtung

- Die zunehmende Diskussion der strafrechtlichen Verantwortlichkeit und Verantwortlichkeit der GF gem. § 130 OWiG generiert ein Bedürfnis nach outsourcing.

- Standardisierung und Automatisierung per CbDgn verbessern die Transparenz und Auditierbarkeit und ermöglichen dem Kunden die Einhaltung von Compliance Vorgaben. Dies ist auch als Einhaltung der Aufsichtspflicht interpretierbar.

- Missbrauchsrisiken sind nicht delegierbar. Hier kommt immer eine Teilnahme an dem Delikt eines möglichen Begehungstäters in Betracht.

Schlussbetrachtung

In den Beispielsfällen:

- Zeigt sich, dass Compliance Vorgaben bei KIS nicht Rechnung getragen wurden.

- Insbes. fehlen Elemente von CbDet: Keine red flag bei inflationärem Gebrauch des Notfallbuttons, kein Alert bei lange bestehenden Zugriffsberechtigungen.

- Weiterhin Defizite bei CbDgn: Keine Differenzierung nach der Schutzbedürftigkeit der Daten (Blutwerte des GF), keine rollenspezifischen Zugriffslimits (Honorararzt darf alle Patientendaten sehen).

Ihre Fragen bitte!