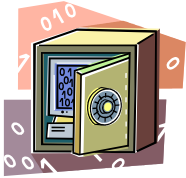


Datenschutz - Umsetzung in der Sozialversicherung



SVS Zentralschweiz
9. September 2008

Corinne Zbären-Lutz,
Rechtsanwältin

„Information ist Macht“

(frei nach Francis Bacon)

2

Schlagzeilen

Wie viele Patientendaten für die Versicherer?
(Hanspeter Thür)
Datentransfer ist illegal (Margrit Kessler betreffend
Krankenversicherer)
Entblöste Computer im Café und der Datenhunger
der Suchmaschinen: Der Umgang mit
persönlichen Daten
Klinsmann überwacht seine Bayern-Stars mit dem
Handy

3

Übersicht des heutigen Referates

Geschichte
1x1 des Datenschutzes: Prinzipien
Umsetzung in der (Sozial)Versicherung
Rechtsetzung und Lehre
„Datenaustausch“: Datenbekanntgabe,
Akteneinsicht
Massnahmen innerhalb eines Sozialversicherers
Argumentarium für Versicherer

Exkurs I und II für Interessierte

4

Geschichte

...schon die alten Römer?

5

Geschichte (1)

Berufsgeheimnisse
Individualität und „Right to Privacy“
Schutz des Privatlebens durch
- Art. 28 ZGB
- **Persönliche Freiheit (ungeschriebenes
Verfassungsrecht)**
- Art. 8 EMRK

Technologischer Fortschritt und immer wichtiger werdender
Gebrauch von persönlichen Informationen

6

Geschichte (2)

Nationale Gesetze (Land Hessen 1970, Schweden 1973)

1971 Motion Bussey

Umfeld der Erarbeitung des Datenschutzgesetzes

Stichwort: Fichenskandal

1993 Bundesgesetz über den Datenschutz (DSG)

1999 Art. 13 Abs. 2 der neuen Bundesverfassung

Stichwort: Schutz der Privatsphäre

2008 revidiertes DSG tritt in Kraft

7

Multiple choice

Der Datenschutz schützt?

- den Arzt
- die Persönlichkeit
- den (Sozial)Versicherer
- die Daten

8

Missverständnis

Der Datenschutz schützt nicht Daten,
sondern die Persönlichkeit:

Datenschutz ist also nicht Selbstzweck.

Datenschutz will das Recht des einzelnen auf
„**informationelle Selbstbestimmung**“ gewährleisten und
den Schutz der Privatsphäre.

9

Man sollte nur von Datenschutzverletzung sprechen, wenn
die Persönlichkeit verletzt worden ist und nicht bei jeder
Datenbearbeitung.

Die Migros verletzt nicht den Datenschutz, wenn sie dank
Ihrer Cumulus-Karte über Sie Daten erhält.
Es ist keine Datenschutzverletzung, wenn Sie in Ihrer
Firma das EDV-System zum Schutz überwachen
Versicherer A muss die Daten von Z nicht vor Versicherer
B verstecken, damit dieser sie nochmals erheben muss.

10

Spezialität im Gesundheitswesen

**Daten über die Gesundheit gelten als „besonders
schützenswerte Daten im Sinne des DSG“**
(Art. 3 lit. c DSG)

Datenprofile (Art. 3 lit. d DSG)

Strafbarkeit für Verletzungen gemäss Art. 79 ATSG,
Art. 92 KVG, Art. 34 und 35 DSG.

11

1x1 des Datenschutzes

12

Multiple choice

Der Regeln des DSG gelten ...?

- nur, wenn ich sie unterschrieben habe
- für alle Mitarbeiter der (Sozial)Versicherer
- nur für bestimmte Mitarbeiter (Versicherungsarzt)
- einzig für die Mitarbeiter, die sensible Daten bearbeiten

13

1 x 1 des Datenschutzes

Grundsätze des Datenschutzes

Diese gelten in der Sozialversicherung, wo die Sozialversicherer als Bundesorgane Daten bearbeiten. Mit Ausnahme des Legalitätsprinzips gelten sie aber genauso in den „Zusatzversicherungen“, wo z.B. die Krankenversicherer oder Unfallversicherer als (juristische) Personen des Privatrechts Daten bearbeiten.*
Grundsätze gelten für alle Mitarbeitenden unabhängig von Funktion und Hierarchie

*separates Dokument

14

Alle Grundsätze des DSG

Legalitätsprinzip
Treu und Glauben/Transparenzprinzip
Verhältnismässigkeitsprinzip
Zweckbindungsgebot
Datenrichtigkeit
Datensicherheit
Auskunftsrecht

15

Art. 4 Abs. 1 und Art. 17 DSG

Legalitätsprinzip

Für die Bearbeitung von Personendaten ist eine gesetzliche Grundlage nötig.
Prinzip der Spezialermächtigung
Die Ermächtigung zur Datenbearbeitung findet sich im Spezialgesetz also: AHVG, IVG, KVG etc.

16

Gesetzliche Grundlage für das Bearbeiten im KVG als Beispiel

Art. 84 KVG Bearbeiten von Personendaten

Die mit der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrauten Organe sind befugt, die Personendaten, (...), zu bearbeiten
bearbeiten zu lassen, die sie benötigen, um die ihnen nach diesem Gesetz übertragenen Aufgaben zu erfüllen, namentlich um:

...

17

Art. 4 Abs. 2 DSG

Treu und Glauben /Transparenzprinzip

Die Bearbeitung von Personendaten hat nach Treu und Glauben zu erfolgen. Datenbearbeitung muss für die betroffene Person erkennbar sein.

Das Beschaffen von Personendaten sollte bei der betroffenen Person selbst erfolgen oder zumindest nicht ohne deren Wissen.

18

Art. 4 Abs. 2 DSGVO

Verhältnismässigkeitsprinzip

Es dürfen nicht mehr Personendaten und Datenbearbeitungen vorgenommen werden, als zur Erfüllung der gesetzlichen Aufgaben erforderlich sind. Es muss ein vernünftiges Verhältnis zwischen den Daten resp. dem Bearbeitungszweck und der Persönlichkeitsbeeinträchtigung bestehen.

19

Art. 4 Abs. 3 DSGVO

Zweckbindungsgebot

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Heutige Kommunikationstechnik kann zu vermehrten Verstössen dagegen führen (papierloses Büro, elektr. Verarbeitung, Zugriffsrechte, Data Warehouse).

20

Art. 5 DSGVO

Datenrichtigkeit

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

Da auch auf Vorrat gesammelte Daten richtig sein müssten, sollte der Sozialversicherer kein Interesse haben, unnötige Daten zu sammeln.

21

Art. 7 DSGVO

Datensicherheit

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

Stichwort: Aufbewahrung, Archivierung, Vernichtung. Delegation?

22

Art. 8 DSGVO

Auskunftsrecht

Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, **ob und welche Daten** über sie bearbeitet werden.

Das Auskunftsrecht ist voraussetzungslos

23

Art. 3 lit. e DSGVO

Bearbeiten ist ...

... jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das **Beschaffen**, Aufbewahren, **Verwenden**, Umarbeiten, **Bekanntgeben**, Archivieren oder **Vernichten** von Daten;

24

Umsetzung in der Sozialversicherung Anwendungsbeispiele

25

These

Das DSG wird nicht überall gleich angewendet.

Richtig oder falsch?



26

Beispiele Informationen über die Person

Darf der Krankenversicherer Sie fragen nach:
Ihrer Adresse, Ihrem Geburtsdatum, Ihrem Zivilstand?
Anzahl Kinder?

Darf der Krankenversicherer Sie fragen
nach Ihrem Gewicht?
- in der Grundversicherung (unter welchen Bedingungen?)
- in der Zusatzversicherung

27

Beispiele Informationen über Ihren Beruf

Darf der Krankenversicherer Sie fragen nach:

- Ihrem Gehalt?
- Ihrem Beruf? Ihrer Ausbildung?
- Ihrem Arbeitgeber? Ihren Arbeitsausfällen?

Darf die die IV-Stelle Sie fragen nach

- Ihrem Gehalt?
- Ihrem Beruf? Ihrer Ausbildung?
- Ihrem Arbeitgeber? Ihren Arbeitsausfällen?

28

Beispiele Informationen über Privates und Finanzielles

Ihre Grossmutter hat sich bei der AHV für eine
Hilflosenentschädigung angemeldet. Darf die
Versicherung sie zuhause besuchen? Darf sie sich für
die finanzielle Situation Ihrer Grossmutter
interessieren?

Ihre Grossmutter hat sich für den Bezug von
Ergänzungsleistungen angemeldet. Darf ein
Mitarbeiter der AHV sie zuhause besuchen? Darf
dieser sich für die finanziellen Verhältnisse
(Einkommen, Vermögen) Ihrer Grossmutter
interessieren?

29

Beispiele Gesundheit

Darf der Unfallversicherer Sie nach dem Datum Ihres
Unfalls fragen? zu den Umständen?

Darf der Krankenversicherer Sie nach den « Gründen »
Ihrer Krankheit fragen? nach den Umständen der
Ansteckung?

30

All diese Beispiele zeigen Ihnen ...

... dass die gleichen Fragen und Antworten (also Daten) für einen Sozialversicherer zulässig sind **und für den anderen nicht.**

Übersetzt auf die Anwendung des DSG bedeutet dies: die gleichen Daten können in einem Zusammenhang « sammelbar », « bearbeitbar » und « austauschbar » sein und **in einem anderen nicht.**

31

Die These ist ... ? richtig!

Das DSG wird nicht überall gleich angewendet - **kann gar nicht überall gleich angewendet werden**, wenn wir es korrekt anwenden wollen.

Gerade die Prinzipien der Transparenz, der Verhältnismässigkeit und der Zweckbindung ...

... führen dazu, **dass die Anwendung sehr stark vom Einzelfall und der betreffenden Sozialversicherung resp. den beantragten Leistungen abhängt.**

32

Rechtsprechung und Lehre

Urteile des Bundesgerichts www.bger.ch
(siehe separate Aufstellung)

Literatur
Leitfäden und Merkblätter des EDÖB www.edoeb.ch
Fachbücher, DSG-Kommentar

Studien
Bericht Geiser, Persönlichkeitsschutz in KV und UV, 2001
Studie IDS, Regelungslücken im med. Datenschutz? 2005

33

Aufsicht

Kreisschreiben des BAG 7.1. vom 1.4.2005
Daten und Persönlichkeitsschutz im KVG

Kreisschreiben des BAG 7.4. vom 1.1.2007
Auskunfts- und Akteneinsichtsrechte im KVG

Kreisscheiben über das Verfahren in der IV (KSIV)
Kreisschreiben über die Rechtspflege in der AHV ... (KSRP)

34

Datenaustausch



35

Welche Daten „kommen hinein“? Welche Daten „gehen hinaus“?



36

Datenaustausch Datenbekanntgabe

Grundsatz: Art. 33 ATSG Schweigepflicht
Geht nichts hinaus?



Die gesetzlichen Grundlagen für den Datenaustausch stellen in diesem Sinn „Ausnahmen“ von der Schweigepflicht dar.

Die Ausnahmen sind im Gesetz klar als solche bezeichnet und leicht erkennbar durch die Einführung „in Abweichung von Art. 33 ATSG ...“

37

1. Ausnahme im ATSG

Art. 32 ATSG Amts- und Verwaltungshilfe

¹ ... geben ... auf schriftliche und begründete Anfrage
² Unter den gleichen Bedingungen leisten **die Organe der einzelnen Sozialversicherungen*** einander Verwaltungshilfe.

→ Datenaustausch innerhalb des Systems der Sozialversicherungen. Die Versicherungsträger sind juristisch gesehen Vollzugsorgane des Verwaltungsrecht.

*Art. 87 BVG Amtshilfe für die Berufliche Vorsorge, für die Art. 32 Abs. 2 ATSG nicht anwendbar ist. .

38

2. Ausnahme im Spezialgesetz

Art. 82 KVG - Besondere Amts und Verwaltungshilfe
In Abweichung von Art. 33 ATSG geben die Versicherer den zuständigen Behörden auf Anfrage kostenlos die notwendigen Auskünfte und Unterlagen für: ...

Diese Aufzählung ist abschliessend!

Analoge Bestimmungen in allen Spezialgesetzen: Art. 50b AHVG, Art. 66b et Art. 68^{bis} IVG, Art. 98 UVG, Art. 95b MVG, Art. 96a AVIG, Art. 87 BVG

39

3. Ausnahme im Spezialgesetz

Art. 84a KVG - Datenbekanntgabe

¹ *Sofern keine überwiegendes Privatinteresse entgegensteht, dürfen Organe, die mit der Durchführung sowie Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betraut sind, Daten in Abweichung von Art. 33 ATSG bekannt geben:*

...

Diese Aufzählung ist abschliessend!

Analoge Bestimmungen in allen Spezialgesetzen:
Art. 50a AHVG, Art. 66a IVG, Art. 29a EOG, Art. 97 UVG, Art. 95a MVG, Art. 97a AVIG, Art. 86a BVG

40

Multiple choice

Wem geben Sie in der Sozialversicherung auch ohne Vollmacht Auskunft?

- dem Arbeitgeber
- dem/der Freund/in der versicherten Person
- einen anderen Sozialversicherer
- dem Anwalt

41

Welche Fälle « ohne Vollmacht »?

Der Datenaustausch kommt zur Anwendung einzig in den im Gesetz aufgeführten Fällen erfolgt ohne Vollmacht und auf schriftliches und begründetes Gesuch hin nur erforderliche Daten

Die gesetzlichen Bestimmungen sprechen von **Datenaustausch oder Datenbekanntgabe**

Die Verwechslung entsteht dadurch, dass man - rechtlich nicht korrekt - auch in diesen Fällen von **Akteneinsicht (Terminus der nur für die versicherte Person gilt)** spricht.

42

Welche Fälle „mit Vollmacht“?

Alle andern Personen und Institutionen, die nicht unter den gesetzlich vorgesehenen Ausnahmen aufgeführt sind, müssen eine Vollmacht vorweisen, wenn sie Informationen erhalten oder das ganze „Dossier“ einsehen möchten.

Zum Beispiel:

- Anwälte und andere Vertreter
- Verwandte der versicherten Person
- Privatversicherer
- Sozialhilfe
- Patientenorganisationen
- etc.



43

Akteneinsicht der versicherten Person

Art. 47 ATSG Akteneinsicht

¹ Sofern überwiegende Privatinteressen gewahrt bleiben, steht die Akteneinsicht zu:

- der versicherten Person für die sie betreffenden Daten;

Art. 8 DSG Auskunftsrecht

¹ Jede Person kann vom Inhaber der Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

44

Didaktische Eselsleiter 1-2-3

„Erste Person“: die versicherte Person hat ein Einsichtsrecht ins gesamt Dossier - somit auf alle Daten - und zwar voraussetzungslos.

„Drittperson“: kann Einsicht ins Dossier nur mit Vollmacht erhalten, dann auch ganzes Dossier.

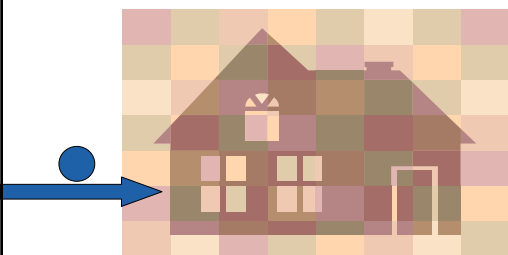
„Zweitperson“: Austausch zwischen Sozialversicherungen und Institutionen gemäss abschliessender Liste im Gesetz, nur die „notwendigen“ Daten werden ausgetauscht.

45

Repetition Zusammenfassung

46

Welche Daten „kommen hinein“?



47

Daten beschaffen/erhalten

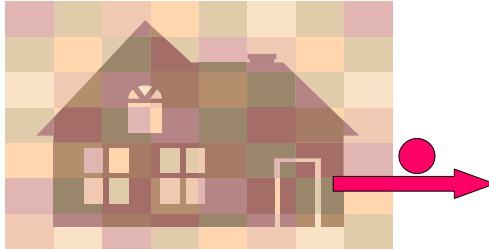
Bei/von der versicherten Person, die mitwirkungspflichtig ist (Art. 28 ATSG)

Beim/vom Leistungserbringer, der auskunftspflichtig ist (Art. 42 KVG, 6a IVG)

Bei/von anderen Sozialversicherern im Rahmen der Leistungscoordination (Art. 32, 49 und 63 ATSG)

48

Welche Daten „gehen hinaus“?



49

Daten bekanntgeben

der versicherten Person (Art. 8 DSG)

→ Bekanntgabe **aller** Daten

Ev. Ausnahme gemäss Art. 47 Abs. 2 ATSG und Art. 8 Abs. 3 DSG

berechtigte Behörden (Art. 19 DSG, Art. 32 ATSG, Art. 82 und 84a KVG)

Bekanntgabe der **notwendige** Daten

Abschliessende Aufzählung: Andere Bekanntgabe ist rechtlich nicht zulässig und strafbar!

50

Massnahmen innerhalb eines Sozialversicherers



51

These: Die neuen Mittel ändern gar nichts

Zugriff auf die Daten in der guten alten Zeit (= Papierdossier)?

Ihr **Schlüssel** wird ersetzt durch ein Passwort

Ihre **Dossiers auf dem Pult** durch Ihren Benutzernamen

Ihr **“Bigla“-Schrank** durch eine Datenbank

... und wie in der guten alten Zeit, wenn Sie eine neue Person anstellen, müssen Sie überlegen, welche Schlüssel Sie ihr geben. Ist das der Passepartout oder nicht doch eher der Schlüssel zur Eingangstür und zu ihrem Büro im 2. Stock?

52

Bespiele für Zugriffseinschränkungen ...

... zur Datenbank:

Das KVG verpflichtet die Krankenversicherer mindestens zu zwei separaten Datenbanken: diejenige mit den Daten der Administration und diejenige mit den Daten des VAD.

53

Eingeschränkter Zugriff ..

... zu bestimmten Daten gemäss einem internen Reglement:

Mit Ihrem Passwort kommen Sie nur an die Daten

- des Kanton X, der Gemeinde Y
- der Minderjährigen, der Volljährigen
- der Inkassoabteilung (Betreibungen)
- des Rechtsdienstes
- der Prämien-/Beitragsabteilung
- der Leistungsabteilung
- etc.

54

Eingeschränkter Zugriff ...

... zu den Dossiers gemäss Versichertennummer etc. etc.

Machen Sie den Vergleich mit der guten alten Zeit, als Sie nur auf „Ihre“ Papierdossier Zugriff hatten und nur auf die Dossiers auf Ihrem Pult!

Die Dossiers des Kollegen nebenan waren tabu.
Man schnüffelte nicht in den Dossiers der anderen.

Warum sollten Sie dies heute elektronisch machen?

55

Tempora mutantur

Weil es einfacher ist, anonym und teilweise fast wie „Surfen“, im Internet. Die neuen Informatik-Mittel und Informatik-Systeme bergen dieses Risiko sozusagen in sich selbst.

Diesem Risiko müssen Sie - im Voraus - intern mit einem strikten, klaren, transparenten Reglement und mit definierten Zugriffprofilen entgegen treten.

56

Die These ist ... ?

Richtig! Es ändert sich nichts.

Die zu beantwortende Frage lautet nach wie vor:

Wer muss Zugriff auf welche Daten haben, um seine Arbeit korrekt machen zu können?

Falsch! Alles ändert sich.

Mit den Mitteln ändern sich auch die zu ergreifenden Massnahmen.

57

Kritik und Kreuzfeuer Argumentarium für Versicherer

58

Argumente für Ihr Unternehmen

Ausgangslage
Versicherungsanträge im Altpapier
Einholen von unnötigen Informationen oder auf Vorrat
Keine Trennung Administration – VA-Dienst

Die Datensicherheit?
Daten sammeln?
Datenweitergabe?

(Zusammenstellung separat)

59

Argumentation und Credo

Wir - Sozialversicherer - bearbeiten sensible Daten im Sinne des Gesetzes ...

(und hypersensible Daten aus Sicht der versicherten Person)

... aber wir schützen sie!

durch Schulung unserer Mitarbeiter
durch angemessene technische Mittel



60

**Behandle die Daten anderer so,
wie Du Deine Daten behandelt
haben möchtest.**

Frei nach Emanuel Kant

61

Corinne Zbären-Lutz

Geschäftsadresse:
IV-Stellen-Konferenz IVSK
Geschäftsstelle IVSK
Landenbergstrasse 39
6005 Luzern

corinne.zbaeren@ivsk.ch

041 369 08 09

62

Exkurs I
Outsourcing
Sperrung

63

Datenbearbeitung durch Dritte Art. 10a

Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn:

- der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selber tun dürfte
- keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet

64

Datenbearbeitung durch Dritte Art. 10a

Beachten Sie beim Outsourcing:

Vertrag zwischen Versicherer und Beauftragtem abschliessen!

Sorgfaltspflichtserklärung des Beauftragten einfordern, worin die DSGVO-Pflichten überbunden werden!

65

Datensperrung Art. 20 DSGVO

= Löschen von Daten im Dossier

Daten können aber nicht beliebig gesperrt werden, sondern die versicherte Person muss ein schutzwürdiges Interesse haben

Fazit: Besser als Sperrung ist, die Daten nicht einzureichen (Selbstzahler). Denn Daten, die der Versicherer nicht hat, kann er auch nicht bearbeiten und weitergeben.

66

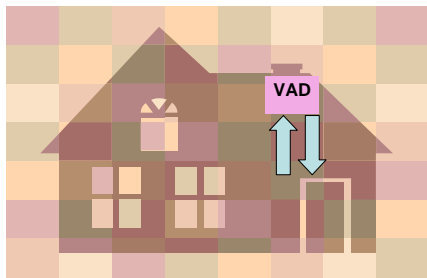
Exkurs II Vertrauensarzt KVG Versicherungsarzt UVG/IVG/MVG etc

67

VA-Modell in der Krankenversicherung

68

Wie werden die Daten intern behandelt?



69

Modell

Das VA-Modell existiert im System der Sozialen Sicherheit
nur in der KV

Das VA-Modell existiert nur in der Schweiz

Die gesetzliche Grundlage dafür ist (einzig) Art. 57 KVG

70

Aufgaben des VA

Der VA ist unabhängig

Der VA gibt Empfehlungen ab. Der Entscheid über das
Leistungsgesuch liegt bei der Administration der KV

Art. 57 Abs. 4 und 5

Der VA ist Datenfilter gegenüber der Administration der KV

Art. 57 Abs. 7

Prüft Wirtschaftlichkeit einer Behandlung

Art. 32, 42, 58 KVG

71

Beispiele

Der VA muss **zwingend** angefragt werden, wo dies im
KVG, KLV, SL, MiGel, AL etc . vorgesehen ist.

→ Der KV hat keinen Spielraum

Der VA kann jederzeit und in jedem Fall als **medizinischer
Experte** um seine Meinung angefragt werden.

→ Der KV hat hier volle Freiheit und wird intern
Regelungen treffen.

72

6 Empfehlungen des EDÖB

Empfehlung 1

Getrennte Räumlichkeiten zwischen VA und Administration; eigene Infrastruktur

Empfehlung 2

Personelle Trennung VA KVG und Versicherungsarzt für Zusatzversicherung

Empfehlung 3

VA-Dienst als Stabsstelle der Geschäftsleitung (sic!)

73

6 Empfehlungen des EDÖB

Empfehlung 4

Zugriffsrecht auf VA-Akten nur für VA und Hilfsperson VA

Empfehlung 5

Möglichst kleine Anzahl von Zugriffsberechtigten

Empfehlung 6

Externes Audit/Zertifizierung

74

... und bei Ihnen?

Die Empfehlungen gelten für alle Krankenversicherer

Wie sieht das bei Ihrem Krankenversicherer aus?
Kennen Sie Ihre internen Richtlinien und Reglemente?

75