Datenschutz als Menschenrecht

Am Beispiel des BKiSchG-E

Werner Baulig
beim
Landesbeauftragten für
Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

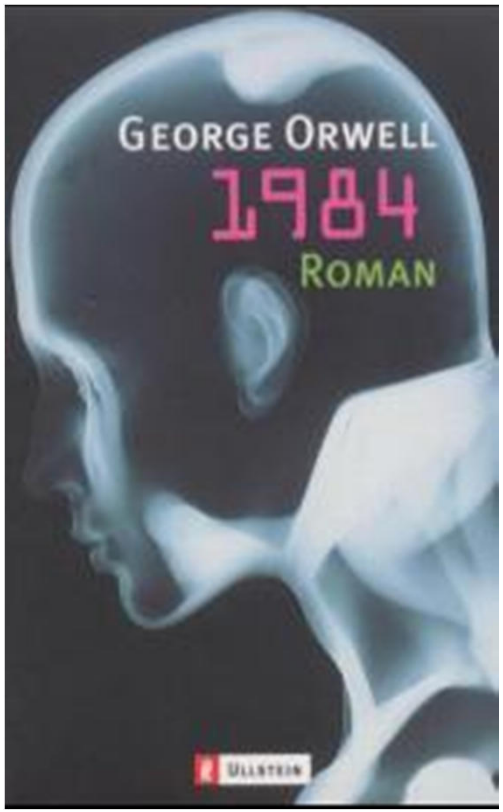
Bad Sülze,
28. Oktober 2011

Datenschutz durch geschriebene Rechte

Rechte und Freiheiten im **Zivilpakt** als Teil der Charta der Vereinten Nationen und der Allgemeinen Erklärung der Menschenrechte (AMER) (bürgerl. und politische Rechte)

Diese Rechte und Freiheiten sind u.a.:

- Gleichstellung von Mann und Frau bei der Ausübung aller in diesem Pakt festgelegten Rechte)
- Das Verbot der Folter (Art. 7)
- Das Verbot der Sklaverei (Art. 8)
- Das Recht auf persönliche Freiheit und Sicherheit
- Das Recht sich frei zu bewegen
- Das Recht vor Gericht gleich zu sein
- Die Gedanken-, Gewissens- und Religionsfreiheit (Art. 18)
- Das Recht sich friedlich zu versammeln
- Das Recht sich frei mit anderen zusammenzuschließen



Normative Struktur

Datenschutz: das **rechtliche** Konzept

1. Datenschutz im europäischen Recht
2. Datenschutz im Bundesrecht
3. Datenschutz im Landesrecht
4. Datenschutz im **untergesetzlichen** Bereich

(z.B. Satzungen, Richtlinien, Verwaltungsvorschriften, Verträge)

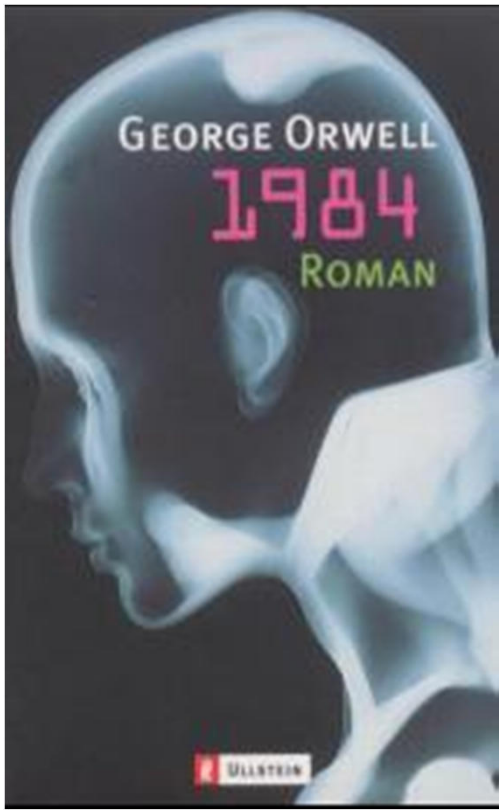
Datenschutz im deutschen Grundgesetz

- **Art. 1 Grundgesetz**

  „Die Würde des Menschen ist unantastbar.“

- **Art. 2 Abs. 1 Grundgesetz:**

  „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“



Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

- **Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83u.a. – Leitsätze:**

1. Unter den Bedingungen der modernen Datenverarbeitung wird der **Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten** von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs.1 GG umfasst.

   Das Grundrecht gewährleistet insoweit die **Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.**

Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

- ...Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichts- und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.
- ...Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

- Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.

- Art. 6 Abs. 1:

- „Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. Dieses Recht findet seine Grenzen in den Rechten Dritter und in den überwiegenden Interessen der Allgemeinheit.“

Datengeheimnis von 1776

„Wir verbieten bei unserer königlichen Ungnade allen und jedem nachzuforschen, wie viel ein anderer auf seinem Folio zu Gute habe, auch soll niemand von den Bank-Schreibern sich unterstehen, solches zu offenbaren:

Weder durch Worte, Zeichen oder Schrift – bei Verlust ihrer Bedienungen, und bei den Strafen, die Meineidige zu erwarten haben.

Zu dem Ende sollen sie bei Antretung ihres Amtes besonderes schwören, dass sie alle Geschäfte, die sie als Bedienstete der Bank unter Händen haben werden, als das größte Geheimnis mit in die Grube nehmen werden.“

Erlass Friedrichs des Großen 1776

Datenschutz im Wandel

- Data-Warehouse, Datamining, Adresshandel, Scoring
- RFID-Chips und Bionik – die „Intelligenz“ der Technik: ubiques Computing
- Smart Metering
- Barcodes und deren Weiterentwicklung
- anonyme Kommunikation oder Signatur
- der Mensch als Datensammlung: Genetik und Wissenschaftsethik, Gesundheits-Card und Identitätsmanagement
- Spannungsfeld: Informationsfreiheit und informationelle Selbstbestimmung

Datenschutz gegenüber wem ?

- Staat (Behörden, Justiz, Polizei,Militär)bisweilen quasimonopolistisch ohne Gewaltenteilung und ohne Vieraugenprinzip
- Schulen,Hochschulen
- Arbeitgeber und Arbeitskollegen
- Wirtschaft (Banken, Versicherungen,Verkaufsunternehmen)
- Bekannten und unbekannten Dritten
- Automatische Erfassungen und Erhebungen ohne klare Abnehmer und Verwendungen („vorsorglich“)
- Convenience (Bequemlichkeit)als Basis für Manipulation und Kontrolle (Minimum an Aufwand und Maximum an Ertrag)

Datenschutz als deutsche Spezialität?

Woher kommt die offenbar besondere Affinität der Deutschen zum Datenschutz – gleichgültig ob Ost oder West ? Z.B. :

- Behördenvielfalt
- Gesetzliche Diversifizierung
- Widerstand gegen Vorratsdatenspeicherung u. Zensus
- Widerstand gegen den Lauschangriff
- Betrieblicher Datenschutzbeauftragter

Die Affinität sowie die sich daraus ergebende Rechtsprechung der Obergerichte hat vor allem historische Ursachen – Stichwort: Diktaturen und Verwaltungs – sowie Regelungsdichte

Alternativen zum Datenschutz ?

Datenschutz wird häufig als Fortschrittsbremse, Täterschutz oder als besonderes Beispiel für „deutsche Ängstlichkeit“, Rechthaberei und Pedanterie angeführt. Folgte man dieser Argumentation, welche Alternativen wären denkbar ? Ist Datenschutz vor dem Hintergrund der heutigen Situation noch eine realistische Zielstellung ?

- Vertrauenskultur ?
- Transparenz als Chance und Leistungsmotor im internationalen Wettbewerb?
- Transparenz als notwendiger sozialpolitischer sowie ordnungspolitischer Stabilisator in überbevölkerten bzw. multiethnischen Staaten ?

Was sind denn eigentlich Daten ?

Singular: Datum

Definition allgemein:

Daten sind zum Zweck der Verarbeitung zusammengefasste Zeichen, die aufgrund bekannter oder unterstellter Abmachungen Informationen (d. h. Angaben über Sachverhalte und Vorgänge) darstellen

Relevante **Definition im Datenschutz** (mit Wertungsinhalt):

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), (siehe § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG).

Beispiele:

1. Name
2. Vorname
3. Wohnanschrift
4. Jahrgang
5. Schulabschluss
6. Studiengang
7. Studienleistungen
8. Nebenwohnung
9. Hobby
10. Freund/in
11. Gesundheitszustand
12. Religion
13. Parteipräferenz
14. kontoführende Bank
15. Kontostand
16. Vermögen
17. Grundeigentum
18. Schulden
19. Zahlungsrückstände
20. Krediteinkäufe
21. Vorstrafen
22. wer bist DU?

Grundrecht auf informationelle Selbstbestimmung – das Volkszählungsurteil

Datenschutz ist ein **Grundrecht:**

Recht auf informationelle Selbstbestimmung, d.h.:

*Befugnis des Einzelnen, grundsätzlich **selbst** über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen*

Verbot mit Erlaubnisvorbehalt:

gesetzliche Ermächtigung

normenklar

verhältnismäßig

„organisatorischer und verfahrensmäßiger Schutz vor Missbrauch“

Oder:

Wirksame Einwilligung des Betroffenen z.B. § 4 Abs. 1 BDSG

Wirksame Einwilligung

- Wirksamkeit setzt Einsichtsfähigkeit voraus, d.h. Fähigkeit, Tragweite und Folgen der Erklärung abzuschätzen (nicht an Altersgrenzen gebunden, aber §§ 104, 106 – 113 BGB !)

- Formen der Einwilligung:

1. Ausdrücklich, schriftlich
2. Konkludent
3. Mutmaßlich

- Wichtig: In einigen Gesetzen sind schriftliche Einwilligungserklärungen vorgeschrieben (BDSG, § 67b SGB X, § 8 DSG M-V etc.)

Bereichsspezifische Datenschutzgesetze/ Jugendhilfe

- §§ 61 – 68 SGB VIII (Datenschutz in der JH)
- § 35 SGB I (Sozialgeheimnis)
- §§ 67 – 85 SGB X (Datenschutz in Sozialbehörden)
- §§ 203, 34 StGB (Strafrechtliche Schweigepflicht, Rechtfertigender Notstand)
- **Zukünftig:** Bundeskinderschutzgesetz ,insb. § 2 (Informationsbefugnis), § 4 (Datenübermittlung) ,§ 8 a Absätze 4 u. 5,§ 16 Abs. 3, 37 Abs. 2 a, § 72a Abs. 5, § 86 c Abs. 2, § 99 Abs. 6 sowie § 2 Abs. 1 Schwangerschaftskonfliktgesetz (neu)
- **Subsidiär:** Bundesdatenschutzgesetz (BDSG), DSG MV, Datenschutzvorschriften freier Träger (z.B. kirchlicher Datenschutz)

Datenschutz im SGB VIII

- § 61 (Anwendungsbereich, freie Träger, SGB X)
- § 62 (Erhebung von Daten)
- § 63 (Speicherung von Daten, Aufbewahrung, Aktenführung)
- § 64 (Übermittlung und Nutzung, Zweckbindung, **Anonymisierung, Pseudonymisierung**) s.a. § 4 Abs. 3, Satz 2 BKSchG-E als abweichende Regelung
- § 65 (besonderer Vertrauensschutz hier: **Abs. 1 Nr. 4 !)**
- § 68 (Amtsvormundschaft, Amtspflegschaft etc. **Zweckbindung im Abs. 4 !**

Ärztliche Schweigepflicht bisher – ist das BSchKG-E notwendig ?

Verpflichtung, anvertraute Geheimnisse nicht unbefugt zu offenbaren (§ 203 StGB, Berufsrecht, Standesethik)

- **Geheimnis:** jede in Zusammenhang mit der ärztl. Tätigkeit erlangte Information über eine Person
- **Offenbaren:** jede Weitergabe personenbezogener Daten
- **Unbefugt:** Ohne Einwilligung (i.o.S.) oder gesetzliche Grundlage ; Ausnahmen: § 138 StGB (Anzeigepflicht) oder Rechtfertigender Notstand nach § 34 StGB

Ärztliche Schweigepflicht bisher – ist das BSchKG-E notwendig ?

Rechtfertigender Notstand nach § 34 StGB

Stufenmodell nach Fegert u.a.(das Jugendamt 2009, S. 352)

1. Prüfung der eigenen fachlichen Mittel zur G-Abwehr
2. Direktes Einwirken auf die Personensorgeberechtigten zur Inanspruchnahme von Jugendhilfe
3. Mitteilung an das JA, wenn dessen Aktivität dringend **erforderlich** ist
4. Dokumentation dieser Vorgehensweise – Grundsatz: nicht ohne Wissen der Beteiligten – aber u.U. ohne deren Willen

Schutzauftrag nach § 8a SGB VIII und Vertraulichkeit in der Jugendhilfe

- Informationsgewinnung: Erhebung beim Betroffenen als Grundsatz (§ 62 Abs. 2 SGB VIII) – ohne Mitwirkung des Betroffenen nur Erhebung, wenn die Kenntnis der Daten **erforderlich** ist für die Erfüllung des Schutzauftrages nach § 8 a (§ 62 Abs. 3, Nr. 2 d SGB VIII)

- Risikoabschätzung: Weitergabe anvertrauter Daten nur bei Zuständigkeitswechsel und Gefährdung des Kindeswohls sowie an andere Fachkräfte, die zum Zweck der Abschätzung des Gefährdungsrisikos nach § 8 a hinzugezogen werden (s.a. § 65 Abs. 1 Nr. 3 und 4 SGB VIII).

Was ändert sich nun durch das BKSchG-E ?

Einschätzung:

Datenschutzrechtlich gibt es im BKScHG-E kaum harte Änderungen – es gibt nach wie vor jedoch Problemlagen, die durch die Schaffung des BKSchG-E kaum verschärft wurden – sie bestanden im Wesentlichen auch schon vorher.

Die datenschutzrechtlichen – oder datenschutzrelevanten Regelungen des BKSchG-E sind eher grundsätzlicher Natur und greifen nur selten in die Verfahrensregeln des SGB VIII und der allgemeinen datenschutzrechtlichen Regelungen ein. Hier wird die obligate Datenschutzkompatibilität vor allem von der individuellen praktischen Umsetzung dieser allgemeinen Regelungen abhängen. Dabei spielen die Grundsätze der **Datensparsamkeit, der Zweckbindung und der Transparenz** die entscheidende Rolle.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 2 Information der Eltern über Unterstützungsangebote in Fragen der Kindesentwicklung

  Problem: falls keine entsprechende landesrechtliche Zuweisung vorgenommen wird, stellt sich die Frage: *woher und wie bekommt der örtliche Träger der Jugendhilfe die erforderlichen Daten, um die Angebotbefugnis nach Absatz 2 durchsetzen zu können? Wie werden die Daten zu den Angeboten nach Abs. 1 z.B. für werdende Väter erhoben ?*

- § 2 ist **keine Datenübermittlungsbefugnisnorm** – insoweit käme hier das Regelwerk von SGB VIII und SBG I vorrangig zur Geltung – je nach erhebender und übermittelnder Stelle auch SGB X (2. Kapitel - §§ 67 ff). Die Umsetzung dieser Befugnis kann nur anhand der zu beachtenden Grundsätze Datensparsamkeit, Transparenz und Zweckbindung datenschutzkonform gestaltet werden.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 4 Beratung und Übermittlung von Informationen durch Geheimnisträger bei Kindeswohlgefährdung

  Einschätzung: Die Absätze 2 (Satz 2) und 3 (letzter Satz) sind hinreichende Befugnisnormen zur Übermittlung von Sozialdaten als lex specialis. Durch die jeweilige Hinzufügung des Rechtsbegriffs „erforderlichen..“ wird hinsichtlich des konkreten Verfahrens auf die allgemeinen Grundsätze des Datenschutzrechtes verwiesen, die subsidiär auch hier gelten. Dies gilt hier insb. für die Grundsätze der Datensparsamkeit und der Zweckbindung. Der Verzicht auf die grds. vorrangige Anonymisierung (teilweise zugunsten einer Pseudonymisierung im Absatz 2) ist aufgrund der Natur der Sache (Erfüllung des gesetzlichen Auftrages) angemessen und wird in manchen Fällen zudem mit dem Instrument der „mutmaßlichen Einwilligung“ zusätzlich gerechtfertigt sein. Der Grundsatz der Transparenz und der sozialrechtlich vorrangigen Mitwirkung des Betroffenen ist dann nachrangig, wenn die existentielle Kindeswohlgewährleistung auf anderem Wege nicht erreichbar ist.

- *Unnötig weit bzw. wenig konkret ist die Festlegung des „Jugendamtes“ als Adressat der Übermittlung nach Absatz 3 (Satz 1 , 2. Halbsatz und letzter Satz), hier wäre die Bezeichnung „ zuständige Stelle im Jugendamt“ möglicherweise hilfreicher gewesen, um eine unnötige Datenstreuung innerhalb des Jugendamtes und seiner unterschiedlichen Stellen weniger wahrscheinlich zu machen.*

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 8 a Abs. 4 (Vereinbarungen) und 5 (Datenübermittlung)

Zur Informationspflicht gegenüber dem „Jugendamt“ gelten auch hier die kritischen Ausführen zu § 4. Bei Absatz 5 handelt es sich um eine Verpflichtungsnorm zur Datenübermittlung, die leider relativ allgemein und unbestimmt ist – dies ist wohl auch eine Folge der Entscheidung hier eine Verpflichtung und keine bloße Befugnis wie bei den Berufsgruppen nach § 4 zu wählen. Dabei handelt es sich bei dem Weg der Übermittlung (im Rahmen eines Gespräches) um eine Soll-Verpflichtung, die – erforderlichenfalls – auch Alternativen offen lässt. Die hier vorgenommene schrankenlose Kopplung der „Erforderlichkeit“ des Datenumfanges an den gesamten Aufgabenkatalog des § 8a und seines dortigen Stufenmodells mit (je nach Sichtweise) etwa 6-8 hochrelevanten unbestimmten Rechtsbegriffen, macht die Bestimmung des Begriffs „Erforderlichkeit“ als einzig verbliebenes Datenschutzregulativ sehr schwer – wenn nicht in der Praxis irrelevant. Auch hier wird es in der Praxis auf die Sensibilität der Akteure für die Grundsätze der Datensparsamkeit und Zweckbindung ankommen. Dies gilt auch für die Lagerung und Löschung der entsprechend gewonnen Daten.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 16 Abs. 3 (neu) (Beratungsangebote für Mütter, Väter und Schwangeren

  Problem: Wer pflegt wie (und woher) die Adressen der oben genannten Zielgruppen ? Dann unschädlich, wenn es sich (wie wohl bisher) um eine Komm-Struktur handelt. Eine **Datenerhebungsbefugnis** enthält Abs. 3 **nicht**.

- § 37 Abs. 2 a (neu) (Hilfeplanerweiterung)

  Durch die Erweiterung der Dokumentationen um sensible Datensätze (jedenfalls Sozialdaten, evtl. auch sensible Daten i.S. des DSG M-V, § 7 Abs. 2) steigen die Sicherungsanforderungen hinsichtlich Verarbeitung, Lagerung etc. Zudem dürfte es sich bald ausnahmslos um automatisierte Datenverarbeitung handeln, mit entsprechenden Verfahrensanforderungen nach dem DSG M-V. Insoweit wären die jeweiligen vor Ort gewählten Verfahren zu prüfen.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 72 a Abs. 5 (Erweitertes Führungszeugnis – jetzt auch nach § 30 a Abs. 1 BZRG)

Prof Salgo (im Rahmen der Anhörung zum Entwurf):

„Die Verpflichtung zur Vorlage von erweiterten Führungszeugnissen scheint geeignet und erforderlich, um einschlägig vorbestrafte Personen aus dem Tätigkeitsfeld fernzuhalten, unabhängig davon, ob sie haupt- oder nebenberuflich oder ehrenamtlich tätig sind, auch wenn ein Fernhalten von Personen mit pädosexueller Veranlagung aus den Arbeitsfeldern damit nicht umfassend sichergestellt werden kann."

Problem:

Potentiell verwirrendes Spannungsfeld zwischen „Sollens-Verpflichtung" der Vorlage und der „Erforderlichkeit" des Datenumfanges z.B. im Abs. 5, Satz 2 „…soweit dies…erforderlich ist".

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 81 (Strukturelle Zusammenarbeit)

Allgemeine Einschätzung: Ausweitung und Konkretisierung der bisherigen Norm – zudem möglicherweise Ausweitung **durch** Konkretisierung mit daraus folgendem größeren Organisationsaufwand und **steigender Datenschutzverletzungsaffinität**. Auch hier wird es entscheidend auf die praktische (datenschutzkonforme) Umsetzung dieser Verpflichtung ankommen – wiederum unter der strikten Beachtung der Grundsätze der Datensparsamkeit, Transparenz und Zweckbindung. Durch die geradezu ubiquitäre und daher herausragend intensive Vernetzung der Jugendämter könnte der Datenschutz gerade hier weitgehend zugunsten ökonomischer oder ordnungspolitischer Erwägungen ausgehebelt werden - insoweit werden die konkreten Methoden der Kooperationen vor Ort auch datenschutzrechtlich zu beobachten sein.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- § 86 c Abs. 2 (Datenübermittlung bei Zuständigkeitswechsel)

Hier handelt es sich um eine klassische Datenübermittlungs-**Befugnisnorm**, die sozialrechtliche und datenschutzrechtliche Beteiligungsgrundsätze ausdrücklich berücksichtigt.

Probleme: das Wort „maßgeblichen“ sollte durch das Wort „erforderlichen“ ersetzt werden. Zum einen handelt es sich bei dem gewählten Begriff nicht um einen gebräuchlichen Rechtsbegriff mit gerade im Datenschutzrecht bewährter Praxis und zum anderen stellen sich semantische Unklarheiten ein, wenn die Frage gestellt wird, was z.B. für die Hilfegewährung oder für den Zuständigkeitswechsel „**maß**geblich“ (als primär quantitatives Regulativ) sein soll. Aus datenschutzrechtlicher Sicht kann nur „erforderlich“ (i.S. quantitativer **und** qualitativer Kriterien) „gemeint“ sein – dann wäre es besser, eben diesen Begriff zu benutzen. Zudem wird durch die Anwendung des Begriffes „angemessen“ im Satz 3 eine u.U. auch datenschutzrechtlich relevante Streitmenge provoziert, die bei einem Verzicht auf diesen Begriff möglicherweise nicht aufgetaucht wäre. Auch bleibt unklar, **wann** die Beteiligung zu erfolgen hat und ob zur gewollten Angemessenheit dieser z.B. auch das Kriterium ihrer Rechtszeitigkeit zählt.

Datenschutzrechtliche Bewertung einzelner Normen des BKSchG-E

- Am Beispiel des § 99 Abs. 6 (Erhebungsmerkmale)

Problem: Durch die Art der dort eingeführten Erhebungsmerkmale, wie „die Gefährdungseinschätzung anregende Institution oder Person“, „Art der Kindeswohlgefährdung“, „Geschlecht, Alter und Aufenthaltsort des Kindes zum Zeitpunkt der Meldung“, „Alter der Eltern“ und „Inanspruchnahme einer Leistung gemäß „“ 16 bis 21 sowie §§ 27 bis 35a“ ist die Unverzichtbarkeit einer den Zweck der Erhebung dennoch nicht konterkarierende Anonymisierung evident. So wäre anhand der schlichten Angabe der o.g. Kriterien in überschaubaren Sozialräumen eine Identifizierung von Personen für Dritte gut vorstellbar. In diesem Falle lägen keine bloßen Statistikdaten mehr vor, sondern entweder personenbezogene Daten oder aber personenbeziehbare Daten i.S. des BDSG (§ 3) bzw. der entsprechenden Landesgesetze. Insb. bei der Angabe der anregenden Institution wird es daher auf eine strikt „anonymisierte“ Formulierung ankommen, die eine Reidentifizierung der Einrichtung bzw. mittelbar der betroffenen Kinder nicht oder nur mit unverhältnismäßigem Aufwand zulässt.

Verkürztes Prüfungsschema Datenschutz !

- Daten im Sinne des BDSG oder DSG MV ? Sensible Daten ?
- Datengebrauch i.S. obiger Regelungen ?
- **Rechtsgrundlage** (normenklar) oder informierte Einwilligung ?
- Datenvermeidung und **Datensparsamkeit**
- Erhebung beim Betroffenen möglich und verhältnismäßig?
- **Zweckbindung** der Daten
- Erforderlichkeit des Gebrauchs
- **Transparenz** des gesamten Vorganges bis zur Auskunftsermöglichung
- Ggf. Sicherheitsvorkehrungen (evtl. auch privacy by design als beste Präferenz)
- Ggf. Automatisierte Einzelentscheidung als Ablehnungsgrund ?
- Ggf. Freigabe und Verzeichnis bei automatisierter Bearbeitung

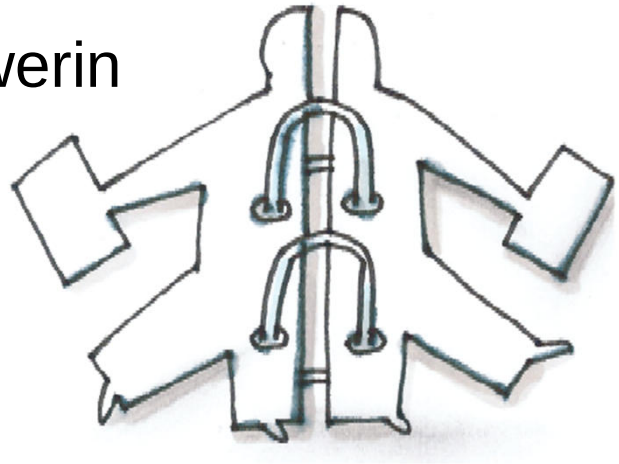
Weitere Informationen:

- www.datenschutz.de
- www.datenschutz-mv.de
- www.informationsfreiheit-mv.de

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Schloss Schwerin, 19053 Schwerin

Tel.: 0385 – 5 94 94 (0) (46)
Fax: 0385 – 5 94 94 58
mail: datenschutz@mvnet.de



Literaturhinweise und Links

- Bernhard C. Witt, Datenschutz kompakt und verständlich, 2. Auflage
- Das berufliche Leitbild des Datenschutzbeauftragten (BvD), April 2010
- Ilija Trojanow und Juli Zeh, Angriff auf die Freiheit, 2009
- Peter Schaar, Das Ende der Privatsphäre, 2009
- Konferenz der Datenschutzbeauftragten, Ein modernes Datenschutzrecht für das 21. Jahrhundert, www.baden-wuertemberg.datenschutz.de

- http://europa.eu/index_de.htm (unter A-Z : Stichwort: Datenschutz)
- www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=de
- www.datenschutz.de
- www.privat-im-internet.de
- www.heise.de
- www.golem.de/specials/Datenschutz
- www.datenschutzverein.de
- www.datenschutz-help.de/deutschland.htm
- www.bfdi.bund.de/cln_134/Vorschaltseite_DE_node.html