Die Neuen Schutzziele

Beherrschbare, faire und vertrauenswürdige IT-Infrastrukturen

Martin Rost

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)

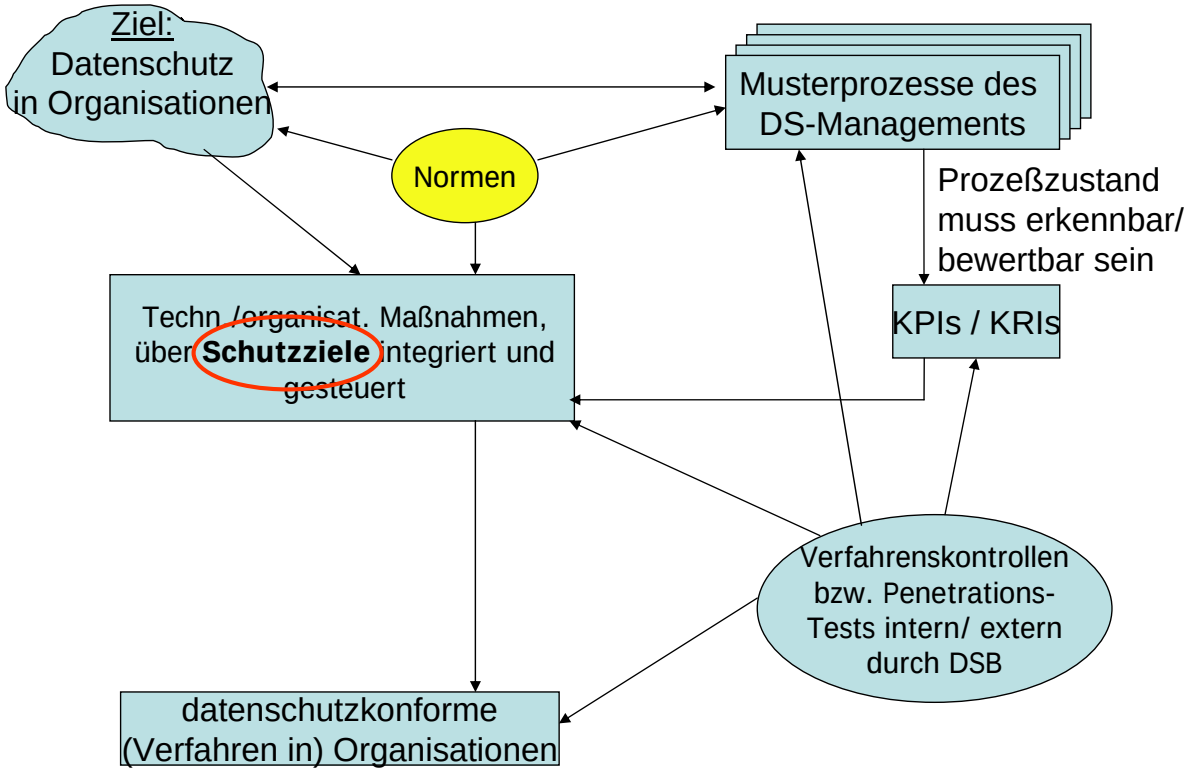
ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Gliederung

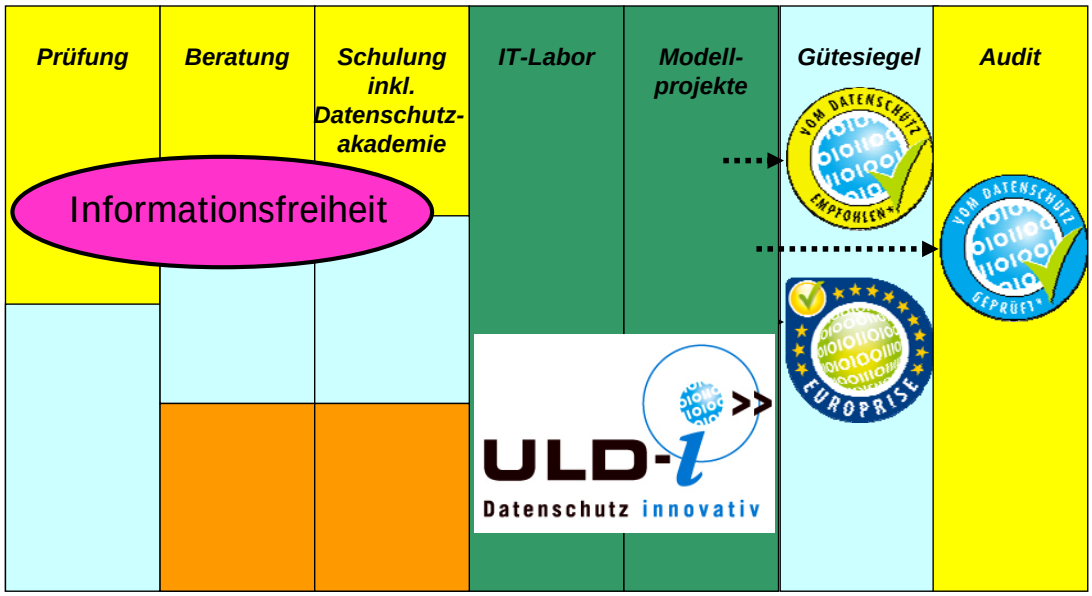
1. „The Big Picture“ - Moderner Datenschutz heute
2. Kurzvorstellung des LfD-Schleswig-Holstein/ ULD
3. Auszug aus dem Koalitionsvertrag von CDU/CSU/FDP zum Thema Datenschutz
4. Datenschutz-Paradigmen und –Recht im Schnelldurchgang, Funktion des Datenschutzes?
5. Die aktuellen Herausforderungen
6. Die „Neuen Datenschutzziele“:
   - Transparenz
   - Intervenierbarkeit
   - Nichtverkettbarkeit
7. Was ist zu tun?

Big Picture

Schutzziele, DS-Managment, KPI/KRI, PenTests



Die 7 Säulen des ULD



Primäre Adressaten:

- *Öffentliche Verwaltungen*
- *Unternehmen*
- *Bürger, Kunden, Klienten, Patienten*
- *Wirtschaft, Wissenschaft, Verwaltung*

40 MA, davon 7 Projektbereich

Projekte und Studien des ULD

https://www.datenschutzzentrum.de/projekte/index.htm

Laufende Projekte

- EuroPriSe - European Privacy Seal
- Identitätsmanagement
  - PRIME - Privacy and Identity Management for Europe
  - FIDIS - Future of Identity in the Information Society
  - Identity Management Systems (IMS): Identification and Comparison Study
- Tclouds - Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructures
- Virtuelles Datenschutzbüro

Abgeschlossene Projekte

- IM-Enabled - Instant Messaging für eGovernment
- AN.ON - Anonymität Online
- Datenschutzaudit
- Datenschutz-Gütesiegel
- P3P - Datenschutz für Internetsurfer
- SPIT-AL – Abwehr von SPAM over Internet Telephony
- Biometrie und Datenschutz
- Schul-CD: Sichere IT-Nutzung für Aus- und Weiterbildung
- PRISE – Datenschutzanforderungen für die Sicherheitsforschung
- RISER - Europaweite Melderegisterauskunft
- DOS - Datenschutz in Onlinespielen

Studien

- Datenschutz und Geoinformationen
- Verkettung digitaler Identitäten
- SOAinVO - Service-orientierte Architekturen in virtuellen Organisationen
- TAUCIS - Allgegenwärtige Datenverarbeitung
- Privacy4DRM
- Erhöhung des Datenschutzniveaus zugunsten der Verbraucher
- Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher

Auszug aus dem Koalitionsvertrag von CDU/CSU/FDP zum Thema Datenschutz (I)

„(...) Wir wollen ein hohes Datenschutzniveau. Die Grundsätze der Verhältnismäßigkeit**, der Datensicherheit und -**sparsamkeit, **der Zweckbindung und der Transparenz** wollen wir im öffentlichen und privaten Bereich noch stärker zur Geltung bringen. Hierzu werden wir das Bundesdatenschutzgesetz unter Berücksichtigung der europäischen Rechtsentwicklung lesbarer und verständlicher machen sowie zukunftsfest und technikneutral ausgestalten. Die **Einwilligung** ist eine wesentliche Säule des informationellen Selbstbestimmungsrechts. Ziel der Reform muss daher auch sein, verbesserte Rahmenbedingungen für informierte und freie Einwilligungen zu schaffen. Dazu sollen Informationspflichten erweitert und der Freiwilligkeit der Einwilligung größere Bedeutung beigemessen werden.“ (S. 106 / 107)

Auszug aus dem Koalitionsvertrag von CDU/CSU/FDP zum Thema Datenschutz (II)

„Darüber hinaus werden wir eine Stiftung Datenschutz errichten, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Wir sind überzeugt, dass mit dieser Lösung auch der **Technologiestandort Deutschland** gestärkt wird, *wenn datenschutzfreundliche Technik aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann.*

Wir werden beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die personelle und sächliche Ausstattung verbessern. (...).“ (vgl. S. 106/ 107)

Datenschutz-Paradigmen und maßgebliche Rechtsfiguren im Schnellaufriss

- *ab 2000*: Ökonomisierung des Datenschutzes, **Datenschutz-Gütesiegel und –Audit.**
- *2006*: „Datenschutz in die **Prozesse**!“ Integration von Datenschutz in Common Criteria, ITIL, CoBIT, BSI-Grundschutz, IFG-Bund, EuroPrise-Gütesiegel.
- *2008.02*: BVerfG: „Gewährleistungsgrundrecht auf **Integrität und Vertraulichkeit** informationstechnischer Systeme“.
- *Ab Sommer 2009*: Entwicklung spezifischer Datenschutz-Schutzziele: **Nicht-Verkettbarkeit, Intervenierbarkeit, Transparenz**

Die aktuell geltenden Datenschutznormen

- **Bundesdatenschutzgesetz** – erstreckt sich auf Privatpersonen, Privatwirtschaft und Bundesbehörden
- **Landesdatenschutzgesetze** – erstreckt sich auf öffentliche Verwaltung in Land und Kommunen
- speziell in SH zusätzlich: **DS-Verordnung**
- **EU:**
  - **Europäische Grundrechte-Charta**
  - **DS-Richtlinie**, Wirkung nur über Import in deutsche Gesetze.
- **Spezialgesetze (haben Vorrang)**:
  - Telemedien-Gesetz, Telekommuniktions-Gesetz,
  - SGB, AO, LandesMeldeGes, LVerwGesetz/ PolizeiGes, PassGes, PersonalausweisGes, AufenthaltsGes., ...

Goldene Regeln des Datenschutzes

(entlehnt aus: Bizer, Johann: Sieben Goldene Regeln des Datenschutzes, in: DuD 2007/05: 350-356)

1. **Rechtmäßigkeit / Einwilligung**
   - Jede Datenverarbeitung mit Personenbezug bedarf einer rechtlichen Grundlage, entweder als Gesetz, Vertrag oder als betriebliche Regelung.
   - Eine Einwilligung ist nur dann wirksam, wenn der Betroffene ausreichend informiert worden ist und seine Einwilligung freiwillig erteilt hat.
2. **Zweckbindung / Erforderlichkeit / Datensparsamkeit**
   - Personen bezogene Daten dürfen nur für den explizierten Zweck verwendet werden.
   - Die Datenverarbeitung ist auf den für den Erhebungszweck notwendigen Umfang zu begrenzen, insbesondere im Hinblick auf Menge und Art der verarbeiteten Daten. Sie umfasst auch Löschung von Teildaten, sobald diese nicht mehr benötigt werden.
3. **Transparenz der Datenverarbeitung / Betroffenenrechte**
   Erhebung und Verarbeitung personenbezogener Daten muss gegenüber Betroffenen transparent sein. Dies schließt Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte ein.
4. **Datensicherheit**
   Datenschutz ist nur dann gewährleistet, wenn personenbezogene Daten sicher verarbeitet werden.
5. **Kontrolle**
   Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen.

Ist nur Teilaspekt des Datenschutzes!

Funktion des institutionalisierten Datenschutzes

Der institutionalisierte Datenschutz prüft und bewertet die Angemessenheit der Informationsverarbeitung und Kommunikation im Zusammenhang von...

- öffentlichen Verwaltungen und deren externen **Bürger**
- privaten Unternehmen und deren externen **Kunden**
- Praxen/ Instituten und deren externen **Patienten, Mandanten, Klienten, Individuen, Subjekte, Menschen.**
- IT-Infrastruktur-Providern und deren **Nutzern** (bspw. Access-Providern, Suchmaschinen-, Mail-, Socialnetwork-Betreiber)
- Institutionen und deren internen **Mitarbeitern oder Mitgliedern**

in den Prozessen der Datenverarbeitung und Kommunikation, wie diese (vornehmlich) aus der Interessenslage von **Personen** heraus unter Bedingungen gestellt werden (können).

Wir haben im Datenschutz mit drei Strukturproblemen zu kämpfen...

- Latente Organisationsübermacht gegenüber Klientel
- Veraltetes Datenschutzrecht
- Vollzugsdefizit

Strukturelle Organisationsübermacht

Organisationen haben durch Informationstechnik die **operativ-kognitive Übermacht gegenüber ihrer Klientel** – und

- unterlaufen dadurch als Unternehmen durch aggressive Kundenbindung latent monopolisierend *Märkte*,
- höhlen als staatliche Institutionen im Konfliktfalle gegenüber dem Bürger latent *Grundrechte* aus oder
- dominieren als Wissenschaftsinstitutionen *Diskurse* und beanspruchen, mit dem Verweis auf Objektivität und Wissenschaftlichkeit gegenüber Patienten oder Ratsuchenden, latent das „letzte Wort“.

Veraltetes Recht

Das BDSG ist veraltet, widersprüchlich, undurchschaubar, bietet für keine Seite hinreichende Erwartungssicherheit.

- „Das bisherige Datenschutzkonzept (...) ist in den 70er Jahren am Paradigma zentraler ***Großrechner*** entwickelt worden, zwischen denen ein Datenaustausch die Ausnahme war.“
  (Roßnagel, Pfitzmann, Garstka 2001: Modernisierung des Datenschutzrechts: 22)
- „Die Forschreibung des BDSG ist anlassbezogene, symbolische Gesetzgebung, die allzu hastig reagiert und damit mehr einer politischen als einer sachlichen Logik folgt. (...) ein funktionsloses Schaustück des Reformwillens (...).“
  (Prof. Thüsing, 2009: Datenschutz im Arbeitsverhältnis, in: NZA 2009/16: 870)
- „Noch keiner BDSG-Novelle zuvor ist es so eindrucksvoll gelungen zu belegen, dass eine Grundsanierung des Datenschutzrechts überfällig ist.“
  (Dirk Fox, 2009: Nach der Novelle ist vor der Sanierung, in DuD 2009/10: 583)

Operatives Vollzugsdefizit

Vollzugsdefizit bei der Aufsicht von Organisationen:

„Bei diesem Strauß von Aufgaben entfällt die Arbeitskraft von 2 bis 2,5 Personen auf die Kontrolle der Beschäftigten-kontrolleure in den 700.000 Unternehmen und allen Behörden in NRW. (...) Das entspricht für ein Unternehmen etwa dem Risiko von ***1 Datenschutzkontrolle in 1000 Jahren.***“

(Bettina Gayk, Referatleiterin bei der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW https://www.datenschutzzentrum.de/sommerakademie/2009/ sak09-gayk-datenschutzkontrolle-der-beschaeftigtenkontrolleure.pdf)

Wie lassen sich diese drei Strukturprobleme konstruktiv lösen?

Gefordert ist die Entwicklung von **Referenzgrößen** für die technisch-organisatorische Umsetzung von Datenschutz-Normen,

1. die Organisationen (Verwaltungen, Unternehmen, Institute) weltweit verstehen und im Hinblick auf ihre Klientel technisch-operativ **beherrschbar**, organisiert **fair** und subjektiv **vertrauenswürdig** umsetzen können,
2. die transparent, verständlich, logisch, valide zugänglich und schlank gehalten den **normative Anforderungen** der Datenschutz-Gesetze entnehmbar sind, und
3. die organisationsextern und weitgehend **automatisierbar** zur Behebung des Vollzugsproblems bei Prüfungen zugänglich sind.

Ein vielversprechender Kandidat für ein normativ steuerbares, technisch-organisatorisches „Referenzkonzept“ sind....

Schutzziele!

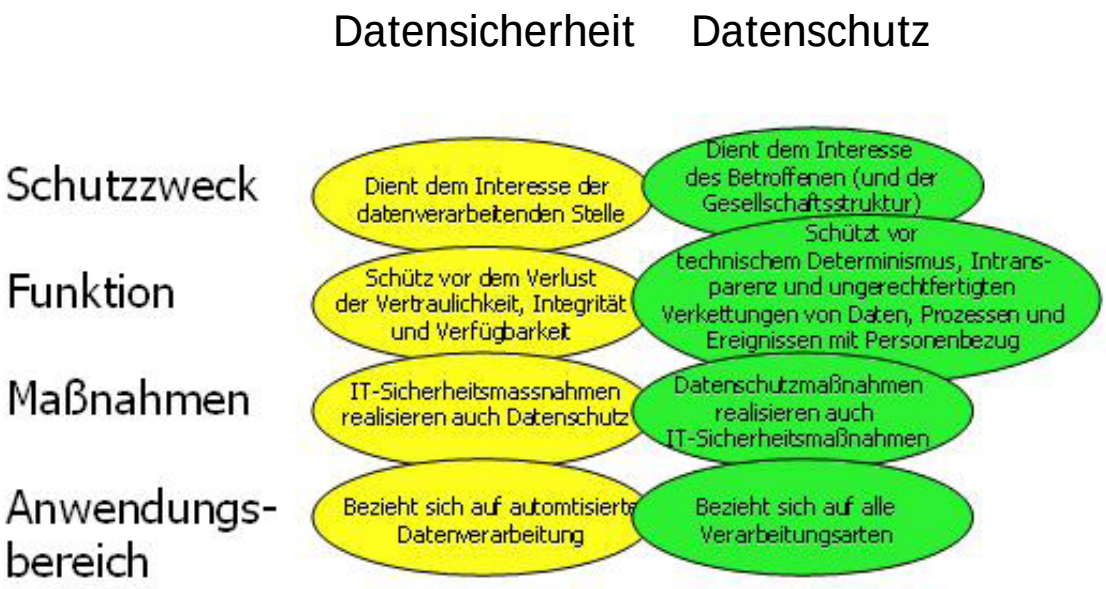
Schutzziele und Methoden

- Schutzziele spielen seit rund **20 Jahren** eine große Rolle im Rahmen der Herstellung von Datensicherheit (DoD, CC, BSI-Grundschutz etc.)
- Konventionelle Schutzziele der Datensicherheit sind die Sicherung der **Verfügbarkeit**, der **Integrität** und der **Vertraulichkeit** von Daten bzw. der Prozesse der Datenverarbeitung.
- Schutzziele werden durch **Maßnahmen** auf dem *Stand der Technik* operationalisiert, Maßnahmen enthalten Regelungsgrößen für Prozesse, die nach *best-practice*-Erwägungen eingerichtet werden.
- In einer Konzeptionsphase eines neuen Verfahrens muss der **Schutzbedarf** von Daten analysiert und festgelegt werden (Schutzbedarfsstufen: normal, hoch, sehr hoch).
- Mit dem **GS-Tool** steht eine Datenbank zur Modellierung von IT-Infrastruktur und der zu treffenden Maßnahmen zur Verfügung.

Schutzziele der Datensicherheit und des Datenschutzes

- Datenschutz setzt zwar im Grundsatz Datensicherheit voraus, kann aber mit Datensicherheit auch im Konflikt liegen (Bsp.: Firewall-Administration)
- Datensicherheit hat primär die Organisation, Datenschutz primär die von den Organisationstätigkeiten betroffenen Personen im Fokus.
- Datenschutz hat immer einen inhaltlichen (semantischen) Überhang, der von gesellschaftlichen Verhältnissen und politischen Konstellationen abhängig ist und sich, anders als die Datensicherheit, nicht rein technisch modellieren und umsetzen lässt.

Abgrenzung Datensicherheit - Datenschutz



Schutzziele in bestehenden Datenschutz-Gesetzen (Beispiel: DSG-NRW)

§ 10 - Technische und organisatorische Maßnahmen

Es ist sicherzustellen, dass ...

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (**Vertraulichkeit**),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),

Primat: Datensicherheit

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).

Primat: Datenschutz

Dieser Schutzzieletext ist textidentischer Bestandteil der aktuellen Landesdatenschutzgesetze von...

- Berlin
- Brandenburg
- Nordrhein-Westfalen
- Mecklenburg-Vorpommern
- Sachsen
- Sachsen-Anhalt
- Thüringen

Schutzziele sind noch nicht Bestandteil des geltenden Bundesdatenschutzgesetzes! (-> Novellierungsempfehlung der DS-Konferenz der Landesbeaufr. für Datenschutz März 2010)

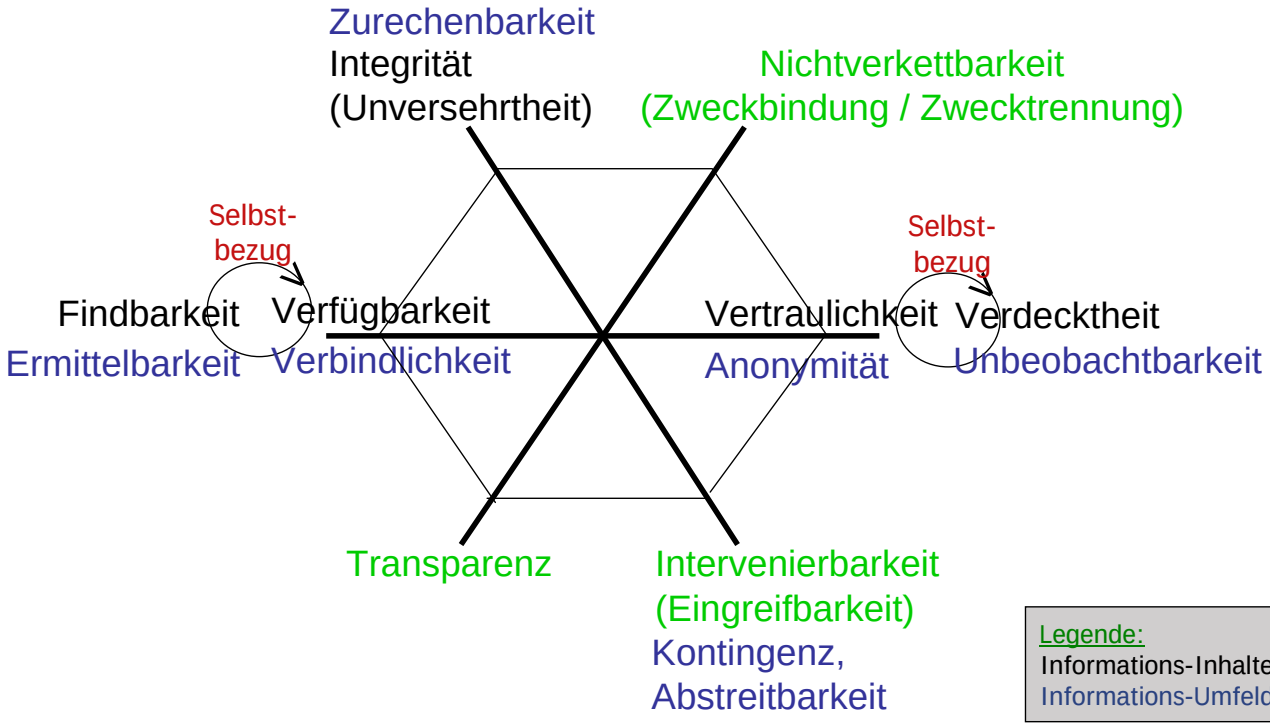
Worin besteht das Problem?

Kann man nicht einfach die bestehenden Schutzziel-Normen übernehmen? Das Problem dabei besteht in der Qualität der **Systematizität** der Schutzziele. Ein paar Fragen:

- Revisionsfähigkeit =: Transparenz!
  Authentizität =: Integrität!
- Verfügbarkeit und Vertraulichkeit sollen zugleich gelten? Widersprüchlich und komplementär: Dual!
- Andere Schutzziele? Was ist bspw. mit Findbarkeit, Anonymität oder gar Unbeobachtbarkeit, Verbindlichkeit usw.?
- Wer kontrolliert anhand welcher Kriterien den Katalog von Schutzzielen? Bestehende Schutzziel-Kataloge ufern aus. Stoppregel? Herleitung? Begründungszusammenhang?

Systematik der Schutzziele

(angelehnt und weiterentwickelt aus: Rost/ Pfitzmann, 2009: Schutzziele revisited; in: DuD 2009/06: 353ff)



Schutzziele (elementare und abgeleitete) auf einen Blick

Inhalte	Umfeld
Verdecktheit	Unentdeckbarkeit Unbeobachtbarkeit
Vertraulichkeit	Anonymität
Intervenierbarkeit	Kontingenz Abstreitbarkeit
Integrität	Zurechenbarkeit
Verfügbarkeit	Verbindlichkeit Erreichbarkeit
Findbarkeit	Ermittelbarkeit
Transparenz *Nichtverkettbarkeit*	

Elementare Schutzziele

Maßnahmen für Verfügbarkeit, Vertraulichkeit, Integrität

Werden personenbezogene Verfahren betrieben, sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten gewährleisten, dass

- Verfahren und Daten zeitgerecht zur Verfügung stehen und diese ordnungsgemäß angewendet werden können (**Verfügbarkeit**). Wesentliche Maßnahme: Redundanz
- nur befugt auf Verfahren und Daten zugegriffen werden kann (**Vertraulichkeit**). Wesentliche Maßnahme: Verschlüsselung von Daten und Kommunikationen sowie Rollentrennungen.
- Daten aus Verfahren unversehrt, zurechenbar und vollständig bleiben (**Integrität**). Wesentliche Maßnahme: Hash-Wert-Vergleiche vorher/nachher

Transparenz
Definition und Maßnahmen

Definition:

„Werden personenbezogene Verfahren betrieben, sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten gewährleisten, *dass die Verfahren zur Erhebung, Verarbeitung in Verfahren und die Nutzung mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.“*

Maßnahmenbündel: „Projektmanagement, Berichtswesen, Verfahrens- bzw. Technikdokumentation, Information und Kommunikation mit den Betroffenen“

- Dokumentation der IT des Verfahrens, der Daten und der Datenflüsse, der Sicherheitsmaßnahmen, der Tests und Freigabe.
- Unterrichtung von Betroffenen (Publikation eines „Datenbriefs“?).
- Die in einem Verfahren beteiligten Entitäten, Daten und Operationen sind in ihrem Zusammenspiel zu konzipieren (Zukunft), zu überwachen im Sinne eines Monitorings (Gegenwart) und zu protokollieren (Vergangenheit).
- Quickfreeze-Option, gesamtverfahrens- oder einzelfallbezogen, um jederzeit einen Systemzustand feststellen zu können.
- Es gelten die Grundsätze ordnungsgemäßer Buchführung.
- Die Dokumentation eines Verfahrens ist ein Bestandteil des Verfahrens.

Nichtverkettbarkeit
Definition und Maßnahmen

Definition:

„Werden personenbezogene Verfahren betrieben, sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten gewährleisten, *dass Verfahren so eingerichtet sind, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.“*

Maßnahmenbündel: „Rollen- und Strukturkonzept“

- Angemessene Funktionstrennungen zwischen oder auch innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente MitarbeiterInnen.
- Kontrollierte Konzeption, Implementierung, Konfiguration, Betriebnahme und Außerbetriebnahme, mit Tests und Simulationen in den jeweiligen Phasen, nach best-practice Gesichtspunkten.
- Steuern von regulierten Prozessen des Erhebens, Verarbeitens, Nutzens, Löschens von Daten mit Techniken jeweils auf dem aktuellen Stand.

Definition:

„Werden personenbezogene Verfahren betrieben, sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten gewährleisten, dass Verfahren so gestaltet werden, *dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.“*

Maßnahmenbündel: „Operativ gegebener Zugriff auf Daten und deren Verarbeitung“

- Einrichtung eines SPOC (Single-Point-Of-Contact) für Betroffene zur Adressierung einer Intervention mit Verfolgbarkeitsoption.
- Fallbezogene Einrichtung und Separierbarkeit von Prozessen, damit sich Interventionen bzw. „Systemstörungen“ nicht systemweit auswirken.
- Sinnvoll wären feingranulare und keine pauschalen Einwilligungen aus Verfahren heraus sowie eine zeitliche Beschränkung von gegebenen Einwilligungen.
- Vorhandene Daten und laufende Verfahren müssen, im Grundsatz auch vom Betroffenen oder von einem von ihm beauftragten Stellvertreter, ausgelöst werden können und einsehbar, änderbar, korrigierbar, sperrbar, löschbar sein.

Funktion der Schutzziele?

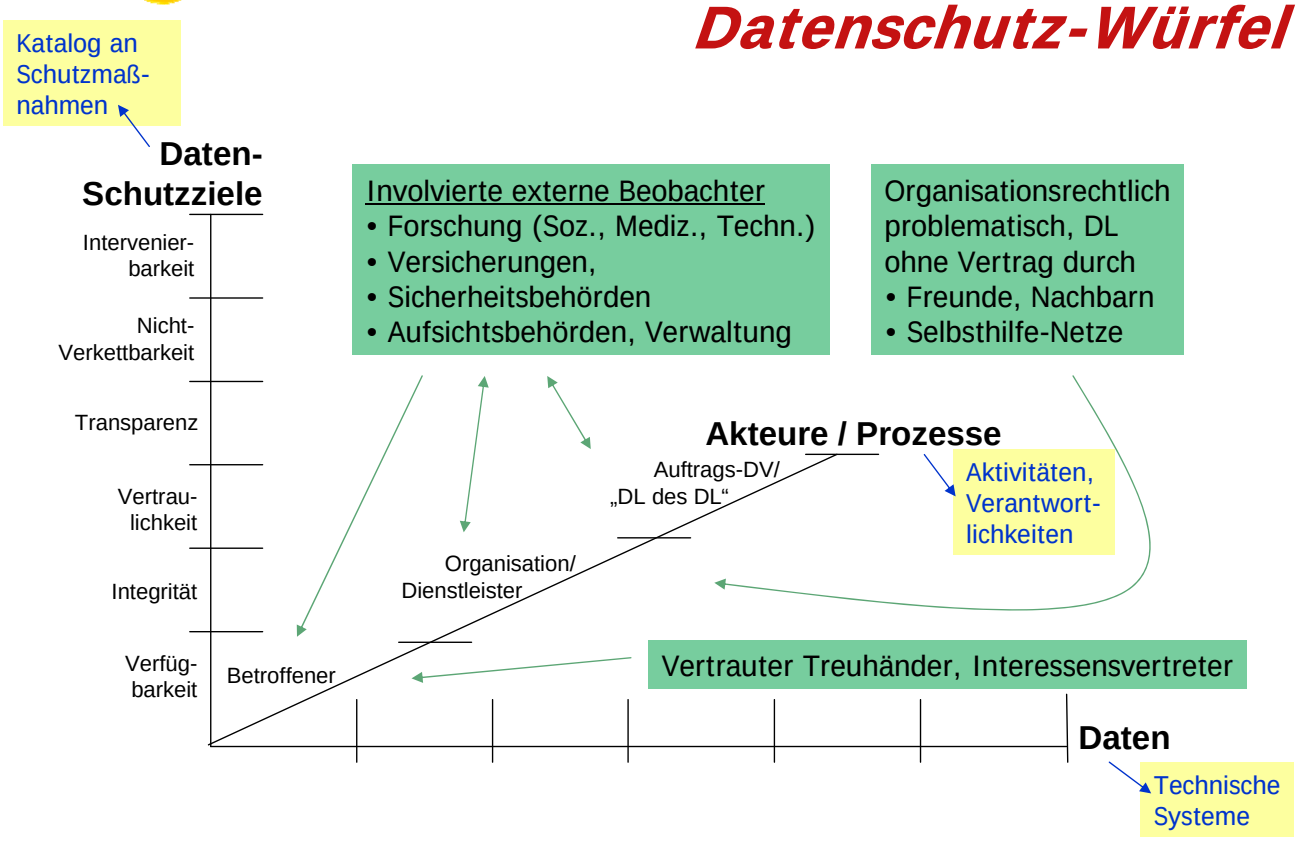
Durch Umsetzung der Schutzziele werden die implizit gegenüber Organisationen im Rechtstaat gestellten Anforderungen operativ erfüllt. Personen unterstellen im Alltagshandeln gegenüber Organisationen vernünftigerweise, dass

- Organisationen ihre Betriebsabläufe **beherrschen**,
- in der Kommunikation/Interaktion zwischen Organsationen und Personen **Fairness** möglich ist,
- subjektive **Vertrauenswürdigkeit** im Verhältnis Organisation/Person gewährt bzw. beansprucht werden kann (was Kommunikationen erleichert, verschlankt, beschleunigt, ...).

Was versprechen die sechs Elementarschutzziele?

- *technisch-pragmatisch*: SZ erzeugen anhand bspw. der ausgewiesenen Maßnahmen **Kontrollfähigkeit** von Organisationen und Testbarkeit von Funktionen und normativen Zusagen
- *rechtsdogmatisch*: SZ erweitern die **Grundrechte um operative Aspekte** staatlicher Gewährleistungen
  -> Der Einstieg war „Integritäts- und Vertraulichkeitsurteil“ des BVerfG!
- *rechtspragmatisch*: SZ erzeugen zwangsläufig die Erwartung, dass auch das **Gesetz** den in ihm formulierten Anforderungen (insbesondere an Transparenz, Zweckbestimmtheit, **Integrität**) genügt.
- *soziologisch*: SZ machen **Systemvertrauen** im Hinblick auf operative Beherrschbarkeit, soziale Fairness und subjektive Vertrauenswürdigkeit von Systemen erwartungsfester und kalkulierbar(er).
- *philosophisch*: SZ ergänzen - als verallgemeinerungsfähige, **vernünftige Anforderungen** an technisch-organisatorische Systeme - die Anforderungen an eine vernünftige Rede (vgl. Jürgen Habermas 1981: Theorie des kommunikativen Handelns). -> Vollständigkeitsvermutung?

Generischer Datenschutz-Würfel



Was ist dafür zu tun: Rechtlich? Technisch? Organisatorisch?

Recht: Schutzziele normativ festlegen!

- Die sechs elementaren Datenschutz-Schutzziele als zentrale *technisch-organisatorische Ziele* in die **Datenschutzgesetze** sowie **Verträge** aufnehmen.
- Die *Schutzmaßnahmen* in einer **Datenschutz-Verordnung** aufführen.
- Erstellen eines **Datenschutz-Handbuches,** darin sollen Referenzen bspw. auf Algorithmen-Kataloge etwa bei der Bundesnetzagentur oder dem BSI zu finden sein, um den *Stand der Technik* und den *Stand der Organisationslehre* konkret fassbar zu machen.

Technik: Schutzziele operativ umsetzen!

- Die Modellierung von IT-Infrastrukturen und Festlegung von Datenschutz-Schutzmaßnahmen sollte datenbankgestützt geschehen.
- Schutzziele sind als ***Policies für WebServices*** im Rahmen der XÖV - bzw. auf Infrastrukturebene des deutschen Standards OSCI2.0 – zu operationalisieren.
- Festlegen welche Instanz verantwortlich
  - rechtliche Normenanweisungen
  - in logische Abläufe
  - in technische Befehle und Formate, bspw. in Form von **WS-Schemata,**

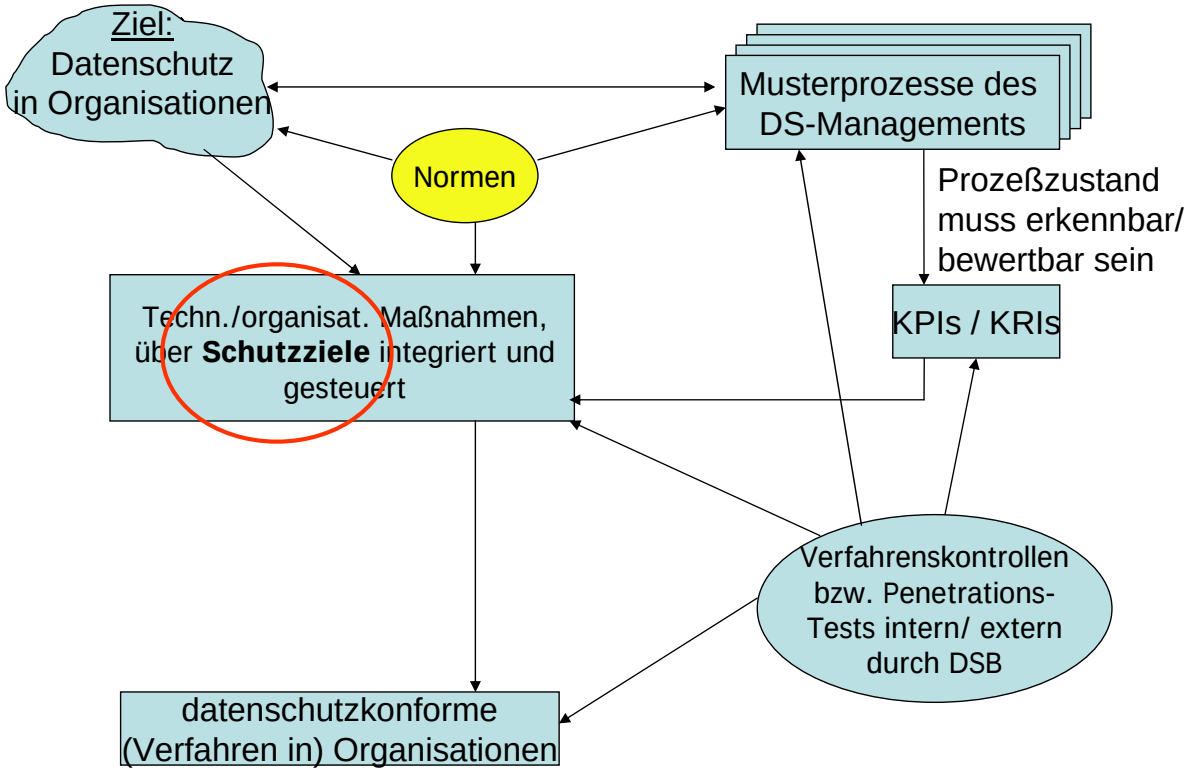
  transformiert.
- Festlegen, wer diese aktuell gültigen Policies für die Schutzziele bei kritischen Infrastrukturen verantwortlich zur Verfügung stellt. Konkret: Den Betreiber festlegen, der integer, hochverfügbar und sicher die zentralen **Policy-Server** betreibt, landesweit, deutschlandweit, EUweit, weltweit.

Organisation: Schutzziele Bestandteile modernen Qualitätsmanagements!

- Schutzziele bilden die Relevanzdimensionen für ein umfassendes **Controlling-Konzept** bzgl. Beherrschbarkeit, Fairness, Vertrauenswürdigkeit
- Öffentliche Institutionen: Der **IT-Planungsrat** muss für E-Government-Prozesse ein an Schutzzielen orientiertes **Betriebskonzept** und **Betriebsmonitoring** aufsetzen, um kritische Infrastrukturen mit Risk- bzw-Qualitätsmanagement zu controllen und zu steuern.
- Private und öffentliche Institutionen: Es müssen, im Rahmen des Compliance- und Datenschutz-Managements, Controlling-Instrumente - **KPI und KRI** - für Datenschutzprozesse zum permanenten Controlling der Umsetzung/ Einhaltung der Schutzziele entwickelt werden.

Big Picture

Schutzziele, DS-Managment, KPI/KRI, PenTests



Referenzen

- **Schutzziel-Kataloge**
  - CAN 1992: The Canadian Trusted Computer Product Evaluation Criteria Version 3.0e, April 1992.
  - Common Criteria/ IST/IEC 15408: http://www.bsi.bund.de/literat/faltbl/F06CommonCriteria.htm, Common Criteria Portal: http://www.commoncriteriaportal.org/
  - DoD, 1985: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225, 711
  - ITSEC 1991: European Communities - Commission: ITSEC: Information Technology Security Evaluation Criteria; (Provisional Harmonised Criteria, Version 1.2, 28 June 1991) Office for Official Publications of the European Communities, Luxembourg 1991.
  - IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- **Systematische Untersuchungen zu Schutzzielen**
  - Wolf, Gritta / Pfitzmann, Andreas; 2000: **Charakteristika von Schutzzielen** und Konsequenzen für Benutzungsschnittstellen; in: Informatik Spektrum, 2000/ 06: 173-191.
  - Federrath, Hannes / Pfitzmann, Andreas, 2000: **Gliederung und Systematisierung von Schutzzielen in IT-Systemen**; in: DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 24/12: S. 704-710.
  - Rost, Martin / Pfitzmann, Andreas, 2009: **Datenschutz-Schutzziele - revisited**; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358
- **Kontext Datenschutz-Schutzziele und Maßnahmen, Informationsfreiheit**
  - Anderson,T. / Lee, P. A., 1981: **Fault Tolerance** - Principles and Practice; Prentice Hall, Englewood Cliffs, New Jersey
  - Rost, Martin 2004: **Verkettbarkeit als Grundbegriff des Datenschutzes**?; in: Innovativer Datenschutz, Für Helmut Bäumler 2004: 315-334, http://www.maroki.de/
  - Rost, Martin (Hrsg.): Schwerpunktthema **Protokollierung**,in: DuD 2006/ 05, DuD 2007/ 10.
  - ULD / TU-Dresden 2007: BMBF-Studie: **Verkettung digitaler Identitäten** https://www.datenschutzzentrum.de/studien/verkettung/
  - BVerfG: **Grundrecht auf Gewährleistung** der Vertraulichkeit und Integrität informationstechnischer Systeme: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
  - Schutzziele in WebService-Policies: Rost, Martin / Speck, Andreas, 2009: Modellgestützte **Validierung von WebService-Ketten**; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 359-363
  - Rost, Martin, 2008: Das etwas andere Modell vom Einheitlichen Ansprechpartner EAP; in: Verwaltung und Management, 14. Jahrgang, Heft 4: 220-223 (**User-Controlled-Workflow**)
  - **Schutzziele als verallgemeinerungsfähige Anforderungen an vernünftig gesteuerte organisatorische und technische Systeme:** Habermas, Jürgen, 1981: Theorie des kommunikativen Handelns, Frankfurt am Main: Suhrkamp
  - Schoch, Fr., 2009: Aktuelle Fragen des **Informationsfreiheitsrechts**; in: NJW 2009/ 41: 2987-2994

Kontakt?

Martin Rost

E-Mail martin.rost@datenschutzzentrum.de
Telefon 0431 9881391
Adresse Holstenstraße 98, 24103 Kiel
Web www.datenschutzzentrum.de