Risiko im Datenschutz (V0.2)

Martin Rost

02./03.11.2017

Berlin / Tagungswerk

Agenda

1. Thesen zum Datenschutz
2. Was meint “Risiko” im Datenschutz?
3. Vorschläge zur Fortentwicklung des Datenschutzes entlang der Bearbeitung sechs typischer Datenschutzrisiken

Risiken und Sicherheit

- **Safety**

  Gilt dem Schutz von Technik vor Risiken des technischen und menschlichen Versagens, z.B. *Systemausfällen*, Leitungsausfällen, Verschleiß, Bedienungsfehlern.

- **IT-Security**

  Gilt dem Schutz vornehmlich vor Risiken die für Geschäftsprozesse von Organisationen bestehen durch zielgerichtete und *böswillige Angriffen* von innen und außen durch Hacker auf Seiten der Organisation.
  (Personal Security: Gilt dem *Selbstschutz von Personen* vor zielgerichteten und böswilligen Angriffen durch Hacker.)

- **Privacy**

  Gilt dem Schutz von Personen vor Übergriffen durch Personen oder Organisationen mit *Schutzvorkehrungen insbesondere auf Seiten der Person*.

- **Data Protection / Datenschutz**

  Gilt dem Schutz a) gesellschaftlicher Strukturen und b) Betroffener vornehmlich vor unnötigen Beeinträchtigungen durch (auch ordnungsgemäß agierende) Organisationen, mit *Schutzvorkehrungen auf Seiten der Organisationen*.

Einige Ausgangsthesen zum Datenschutz

- Datenschutz bearbeitet die **Machtasymmetrie** zwischen verschiedenen Organisationen und Personen (Bürgern, Kunden, Patienten, Individuen, ...).
- Organisationen greifen mit personenbezogenen Verfahren in die **Grundrechte** der Betroffenen ein und greifen darüberhinaus latent moderne Sozialstrukturen an.
- **Die Intensität des Grundrechtseingriff - und nicht der Personenbezug von Daten und auch nicht die eingesetzte Technik -** bildet den Ausgangspunkt für Datenschutzaktivitäten.
- **Grundrechte bedürfen nicht der privaten Zustimmung** durch Betroffene, noch wird deren Geltung durch private Ablehnung obsolet.
- „Informationelle Selbstbestimmung“ steht nicht für **ein privates Bedürfnis nach Privatheit**, sondern ist eine funktionale Konstruktion moderner „funktional differenzierter” Gesellschaften (N. Luhmann).

Maßnahmen zur Verringerung der Eingriffsintensität und Risiken von pers.-bez. Verfahren

Sicherstellung von *Verfügbarkeit*

Redundanz (Backup, Reparatur, Vertretungsregeln)

Sicherstellung von *Integrität*

Verstandene, gesteuerte, **beherschte Prozesse** in Organisationen, Hashwert-Management

Sicherstellung von *Vertraulichkeit*

Verschlüsselung von Daten und Kommunikationsverbindungen, Containern zum Schutz von Betroffenen

Sicherstellen von *Nichtverkettbarkeit* durch Zweckbestimmung/-bindung

Rollen & Berechtigungen, **Trennungsmaßnahmen**, Pseudonymität, Anonymität für Daten und Kommunikationsverbindungen (ABCs)**,** Identitätenmanagement, Audit

Sicherstellen von *Transparenz* durch Herstellen von Beurteilbarkeit personenbezogener Verfahren durch **Spezifikation**, **Protokollierung, Dokumentation**

Sicherstellen von *Intervenierbarkeit* durch Ankerpunkte

SPOC für Änderungen, Korrekturen, Löschen, **Aus-Schalter**, **Changemanagement**

Art. 24 DSGVO: „Verantwortung des für die Verarbeitung Verantwortlichen“

„(1) Der **Verantwortliche** setzt unter Berücksichtigung der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der **Verarbeitung** sowie der unterschiedlichen ***Eintrittswahrscheinlichkeit*** *und* ***Schwere*** *der* ***Risiken*** für die **Rechte und Freiheiten natürlicher Personen** geeignete **technische und organisatorische Maßnahmen** um, um **sicherzustellen** und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

Risikoformel der DSGVO:
Eintrittswahrscheinlichkeit x Schwere des Risikos = Schadenshöhe

Verfahrenseigenschaften → wann besteht hohes Risiko?

- Art → wenn Daten sensibel, IT-Systeme unsicher, Prozesse undefiniert
- Umfang → wenn massenhafte Betroffenheit
- Umstände → wenn sensible Kontexte (Abhängigkeiten)
- Zwecke -> wenn Verfahren keine hinreichende legitime Zwecksetzung/ praktikable Zweckbindung aufweisen?

Ermittlung der Schwere speziell eines Grundrechtseingriffs

- Eintrittswahrscheinlichkeit des Risikos -> 100%
- Schwere des Risikos-> hoch (Angriff auf die Souveränität der Betroffenen beeinträchtigt deren Würde)

Grundrechtseingriff und die dadurch erzeugten Risiken

a) Ein **Grundrechts-Eingriff** durch ein personenbezogenes Verfahren ist ein Fakt, ein bereits „eingetretenes Risiko“ („Risiko 1. Ordnung“).

- Die Intensität eines Eingrifsf muss durch technisch-organisatorische Datenschutz-Schutzmaßnahmen auf das unbedingt erforderliche Maß verringert werden.
- Ein Eingriff bleibt Eingriff auch bei vollständiger Rechtskonformität und nachgewiesen sicherer Informationstechnik.

b) *Darüber hinaus* erzeugt ein Eingriff **Risiken** für Betroffene („Risiken 2. Ordnung“),

- mit *mittelbaren Folgen* für alle Personen aufgrund gesellschaftlicher Strukturschädigungen;
- mit *unmittelbaren Folgen* für Betroffene.

*6 typische Risiken durch einen Grundrechtseingriff mit **unmittelbaren Folgen** für Personen*

Risiko 1	*Risiko 2*	*Risiko 3*	*Risiko 4*	*Risiko 5*	*Risiko 6*
Eine Organisation betreibt ein **nicht legitimes personen-bezogenes Verfahren**.	Die **Schwere des Grundrechts-eingriffs** durch ein legitimes pbV wird gar nicht oder falsch bestimmt, die Rechtsgrundlage reicht nicht oder wird nicht aus-reichend geprüft, Verantwortungs-übernahme diffus.	Eine Organisation betreibt im Grund-satz ein ordnungs-gemäßes pbV, **dehnt oder ändert jedoch den Zweck** (Vorratsdaten-speicherung, Big Data).	Eine Organisation betreibt ein pbV ohne hinreichend wirksame **Maßnahmen der IT-Sicherheit.**	Eine Organisation betreibt ein pbV mit Maßnahmen der **IT-Sicherheit, die nicht grund-rechtskonform betrieben werden.**	Die pbV einer Organisation werden **nicht ausreichend geprüft und beurteilt.**

Risiko 1 – Legitimität eines Verfahrens ist ungeklärt

Risiko 1

Eine Organisation betreibt ein **nicht legitimes personenbezogenes Verfahren**.

- Illegitime Verfahren lassen sich nicht legitimieren/legalisieren durch Gesetz oder Einwilligungen oder das Installieren von Schutzmaßnahmen.
- Der **Verantwortliche, die Datenschutzaufsichtsbehörden und Gerichte** müssen Legitimität von Verfahren(stypen) kontrollieren, prüfen, beurteilen.
- Immerhin: Art. 35 DSGVO **Datenschutz-Folgenabschätzung kann** Schutz vor nicht-legitimen Verfahren entfalten, weil konsistenter als bislang jedes Verfahren zu prüfen ist.
- Allerdings: Eine nachhaltig wirksame **Datenschutzaufsicht findet derzeit nicht statt**. Vollkommen offen ist auch, wie die Qualität der DS-Folgenabschätzungen der Organisationen geprüft werden. Frage ist auch, ob Datenschutzaufsichtsbehörden überhaupt methodisch prüfen können.

Eintrittswahrscheinlichkeit? *hoch*
Durch bspw. Facebook, Google / Apple **findet Vollüberwachung von Personen statt**; inzw. ist eine kulturelle Gewöhnung an eine Vollüberwachung von Personen eingetreten, to big to fail.

Schwere des Risikos? *hoch*
Illegitime Verfahren unterlaufen soziale Schutzvorkehrungen moderner Gesellschaften, sie führen zur **Delegitimierung des Rechts und der Institutionen**, Auslieferung von Personen an Privatorganisationen findet statt, die staatliche Exekutive bedient sich zudem der Infrastrukturen und Datenbestände der Kommunikationsunternehmen zur Vollüberwachung der Bürger.

Risiko 2 – Falsche Bestimmung der Schwere des Grundrechteeingriffs

Risiko 2

Die **Schwere des Grundrechts-eingriffs** durch ein legitimes pbV wird gar nicht oder falsch bestimmt, die Rechtsgrundlage reicht nicht oder wird nicht ausreichend geprüft, Verant-wortungsüber-nahme diffus.

- Nach der Alexy-Formel* lassen sich **Grundrechtseingriffe typisieren** („leicht, mittel, schwer“). Diese Typisierung vorzunehmen ist jedoch bislang keine Übung in der juristischen Prüfpraxis.
- Nicht die Sensitivität personenbezogener Daten, sondern die Eingriffsintensität der Angreifer ist maßgeblich. Es bedarf eines umfassenden spezifischen **Angreifermodells des Datenschutzes**, in Abgrenzung zum Angreifermodell der IT-Sicherheit.
- Die falsche Bestimmung der Schwere eines Grundrechteeingriffs führt zu einer **falschen Bestimmung der Wirksamkeit der zu treffenden Schutzmaßnahmen**, die die Eingriffsintensität auf das geringst mögliche Maß mildern könnten.

Eintrittswahrscheinlichkeit? *hoch*
weil **keine Übung in der juristischen Entscheidungsfindung**, und wenn ausnahmsweise doch dann ist es folgenlos für Bestimmung der Maßnahmen.

Schwere des Risikos? *hoch*
Beeinträchtigt Personen unmittelbar. Eine unangemessen leichte beliebige Verkettbarkeit von Daten unterläuft strukturelle Schutzvorkehrungen moderner Gesellschaften mit der Folge der Zerstörung von Strukturen und **Auslieferung von Personen an rechtlich nicht eingefangene Organisationen.**

* Alexy, Robert, 2003: Die Gewichtsformel, in: Jickeli, J.; Kreutz, P.; Reuter, D., 2003: Gedächtnisschrift für Jürgen Sonnenschein, Berlin, De Gruyter Verlag, S. 777ff.

Spezifische „Angreifer“ des Datenschutzes

- Der Hauptangreifer zur Bestimmung des Risikos für Grundrechtseingriffe ist stets die datenverarbeitende Organisation selbst, unter Beachtung von Motiven und Ressourcen.
- Darüber hinaus gibt es weitere typische Angreifer-Organisationen auf Personen:
  - Sicherheitsbehörden
  - Leistungsverwaltung
  - Bereitsteller von IT-(Infrastruktur)Diensten
  - Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
  - Versicherungen und Banken
  - Forschungsinstitute, insbes. psychologischer und sozialwissenschaftlicher Art
  - Krankenhäuser, Ärzte, Rechtsanwälte
  - Aggressive Startups, Werbeagenturen
  - Untätige Aufsichtsbehörden
  - Hacker

Zweckküberdehnung bei der Anwendung eines Verfahrens

Risiko 3

Eine Organisation betreibt im Grundsatz ein ordnungsgemäßes pbV, **dehnt oder ändert jedoch den Zweck** (Vorratsdatenspeicherung, Big Data).

- Die **Zwecksetzung** muss legitim sein, die **Zweckbestimmung** muss hinreichend eng und prüfbar erfolgen, die **Zwecktrennung** und die **Zweckbindung** erleichtern die operative Umsetzung und die Prüfbarkeit eines Verfahrens.
- Die Zweckbestimmung bildet den **definitorischen Kern eines pb Verfahrens**, aus der heraus die erforderlichen Daten, IT-Systeme und Prozesse sowie die Schutzmaßnahmen zu bestimmen sind.
- Zweckdehnung durch **Fetischisierung der Einwilligung** als vermeintlich souveränem Akt.
- Zweckdehnung/-entfremdung sind in der Praxis von Big Data zum Alltag geworden.
- Abhilfe durch breite Nutzung von **anyonymen Transaktions-Credentials** in Kommunikationsbeziehungen möglich.

Eintrittswahrscheinlichkeit? *hoch*
Eine Organisation, die nicht ihren maximal möglichen Informationsschatz hebt, gerät **im Benchmark mit anderen Organisationen ins Hintertreffen**, zumal keine gleichmäßig gestreuten, sondern nur punktuelle Datenschutzprüfungen erfolgen (dadurch „Marktverzerrung“m insofern: race-2-the-bottom-Risiko).

Schwere des Risikos? *hoch*
Beeinträchtigt Personen unmittelbar. **Kein fairer Tausch**. Eine Ausweitung der Zweckbestimmung unterläuft ebenfalls strukturelle Schutzvorkehrungen moderner Gesellschaften mit der Folge der Auslieferung von Personen an Organisationen.

Risiko 4

Mangelhafte IT-Sicherheitsmaßnahmen

Risiko 4:

Eine Organisation betreibt ein pbV ohne hinreichend wirksame **Maßnahmen der IT-Sicherheit.**

- Die IT- bzw. Informationssicherheit bspw. nach **IT-Grundschutz schützt die Assets einer Organisationen,** es sind aber keine Vorkehrungen zum Schutz durch eine nicht rechtliche abgedeckte Nutzung der Organisation selber vorgesehen.
- Kriterien Erwägungsgrund 75 DSGVO:
  - Diskriminierung,
  - Identitätsdiebstahl oder-betrug,
  - finanzieller Verlust,
  - Rufschädigung,
  - wirtschaftliche oder gesellschaftliche Nachteile,
  - Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

Eintrittswahrscheinlichkeit? *hoch*
Die Leitung von Organisationen wissen inzwischen, dass sie ihre IT mit Schutzmaßnahmen ausstatten müssen. These: Gute IT-Sicherheit = guter Datenschutz ist falsch. Und: **Es gibt zudem keine sichere IT.**

Schwere des Risikos? *hoch*
Ein unbefugter Zugriff auf ein Verfahren (auf Daten, IT-Systeme und Prozesse) führt zu einer beliebigen Daten-verarbeitung mit teilweise konkreten **materiellen und imateriellen Schäden und unabsehbaren Folgen** für Betroffene und für Gesellschaft (bspw. Wahlbeeinflussung).

Risiko 5

Mangelhafte Datenschutzgerechtigkeit auch von IT-Sicherheitsmaßnahmen

Risiko 5

Eine Organisation betreibt ein pbV mit Maßnahmen der **IT-Sicherheit, die nicht grundrechtskonform betrieben werden.**

- Das IT-Sicherheitsmanagement ist etabliert und hat in den letzten 10 Jahren drastisch an Qualität gewonnen, **methodisch sind IT-SiBe ungleich besser ausgebildet und ausgerüstet als Datenschutzbeauftragte,** sie haben in den Organisationen gestalterisch gleich nach dem CIO den größten Einfluss.
- **Rechtsdogmatisch muss Datenschutz die IT-Sicherheit führen, in der Praxis läuft es genau umgekehrt**.
- **Ganz schlechte Datenschutz-Awareness bei Administratoren bzw. „ITlern“**, diese setzen erfahrungsgemäß Maßnahmen der IT-Sicherheit mit denen des operativen Datenschutzes gleich, im Konfliktfall zu Lasten der Betroffenen.

Eintrittswahrscheinlichkeit? *hoch*
ITler agieren im Auftrag der Organisationsleitung und verstehen den **Unterschied zw. IT-Sicherheit für personenbezogene Daten und operativem Datenschutz** als Grundrechteschutz in der Regel nicht.

Schwere des Risikos? *hoch*
Schutzmaßnahmen der IT-Sicherheit im Interesse der Organisation dominieren in der Praxis die spezifischen Schutzmaßnahmen des Datenschutzes.

Mangelhafte Datenschutzkontrolle: Institutionenversagen

Risiko 6

Die pbV von Organisationen werden **nicht ausreichend geprüft und beurteilt.**

- Personenbezogene Verfahren (pbV) werden ***nicht durch unabhängige Datenschutz-aufsichtsbehörden geprüft***; oder
- pb Verfahren werden zwar geprüft aber die ***Prüfungen sind unsystematisch oder methodisch falsch oder*** unvollständig; oder
- Prüfungen werden zwar integer durchgeführt, aber negative Prüfergebnisse seitens der Datenschutzaufsicht ***bleiben ohne nachhaltige Konsequenzen*** für den verantwortlichen Datenverarbeiter; oder
- die Datenschutzaufsicht bringt zwar Konflikte vor Gericht, aber das ***Gericht entscheidet nicht in der Sache***; oder
- das Gericht entscheidet zwar in der Sache, aber unzulänglich, weil die ***gesetzlichen Regelungen nicht zureichen***.

Eintrittswahrscheinlichkeit? *hoch*
Die Zahl der externen, methodisch integren Datenschutzprüfungen sowie der datenschutzrelevanten Gerichtsentscheidungen ist, gemessen an der Zahl der Verstöße, verschwindend gering.

Schwere des Risikos? *hoch*
Willkürlich erfolgende Sanktionen delegitimieren das Rechts- und Politiksystem und zerstören dadurch wesentliche gesellschaftliche Schutzstrukturen zur Pazifizierung von Organisationen gegenüber Personen.

*Risiken für Personen mit **mittelbaren Folgen** durch Nichtbeachtung des Datenschutzes*

Organisationen lösen mit einem nicht datenschutzkonformen Zugriff auf Personen spezifisch moderne gesellschaftliche Strukturen auf. Dadurch entsteht das **Risiko einer Regression einer Gesellschaft auf vormoderne Sozialstrukturen, mit wiederum regressiven Folgen für die Personenkonzepte der Organisationen.**

- Verwaltung: Aus **Bürgern werden wieder Untertanen**, wenn Gewaltenteilung durch Dominanz der Exekutive operativ unterlaufen wird.
- Unternehmen: Aus **Kunden werden wieder Bittsteller**, wenn Markt durch Monopolbildung (bei Plattformen und Integration von Diensten, Betriebssystemen, Hardware) kollabiert.
- Institute: Aus **WissenschaftlerInnen werden wieder Ordensbrüder und -schwestern**, wenn freie Diskurse in den Reputation spendenden Kommunikationsmedien durch dominante Paradigmen dogmatisch veröden (keine peer-reviews).
- Organisationen: Aus **Subjekten werden Objekte** durch willkürlich agierende, nicht-legitime Verfügungsgewalt von Organisationen über Personen (mit den Indikatoren: Fetischisierung von „Transparenz“ als Selbstzweck und der Einwilligung als vermeintlichem Ausdruck eines souveränen Akts).

Fortentwicklung des Datenschutzes durch Bearbeitung der aufgeführten Risiken

Fortentwicklung des Datenschutzes durch wirksame Risikobearbeitung (1)

- **Bearbeitung Risiko 1, Betrieb nichtlegitimer Verfahren erschweren**: Personenbezogene Verfahren, neue Überwachungs und Infrastrukturtechniken müssen *vor Inbetriebnahme genehmigt* werden. (Erfordert bspw. die Bereitstellung einer vollständig prüffähigen Spezifikation und Dokumentation eines Verfahrens inklusive Datenschutz-Folgenabschätzung durch den Antragsteller.)

- **Bearbeitung Risiko 2, falsche Bestimmung der Grundrechtsintensität erschweren:** Spezialisierte *Ausbildung* von SoziologInnen, DatenschutzjuristInnen, InformatikerInnen und SpezialistInnen für Infrastrukturen (Middleware, Netzwerk) und Modellierung von IT-Verbünden.

Fortentwicklung des Datenschutzes durch wirksame Risikobearbeitung (2)

Bearbeitung Risiko 3, Zweckdehnung erschweren:

- Privatbereich: *Stillegung des Verfahrens* oder der verwendeten Techniken bis zur Heilung (Verwaltungsakt der DS-Aufsichtsbehörde), hohes Bußgeld.
- Öffentlicher Bereich / Verwaltung, Polizei: Sofortige Veröffentlichung des Vorfalls und Bildung eines Untersuchungsausschusses zur Verortung (auch der politischen) Verantwortung sowie einer Projektgruppe zur Behebung des Problems, Prüfung auf *strafrechtliche Sanktionierung des Verantwortlichen.*
- Öffentlicher Bereich / Ministerien, Hochschulen: *Stilllegung des Verfahrens* oder der verwendeten Techniken bis zur Heilung, sofortige Veröffentlichung des Vorfalls, sofortige Bildung eines Untersuchungsausschusses zur Verortung (auch der politischen) Verantwortung sowie einer Projektgruppe zur Behebung des Problems, Prüfung auf strafrechtliche Sanktionierung des Verantwortlichen.

Fortentwicklung des Datenschutzes durch wirksame Risikobearbeitung (3)

Bearbeitung Risiko 4, Betrieb mit mangelnder IT-Sicherheit erschweren
Bearbeitung Risiko 5, Betrieb von IT-Sicherheit ohne Datenschutzprofilierung erschweren

- Privatbereich: *Stillegung des Verfahrens* oder der verwendeten Techniken bis zur Heilung, hohes Bußgeld.
- Öffentlicher Bereich / Verwaltung, Polizei: Sofortige Veröffentlichung des Vorfalls, sofortige Bildung eines Untersuchungsausschusses zur Verortung (auch der politischen) Verantwortung sowie einer Projektgruppe zur Behebung des Problems, *Prüfung auf strafrechtliche Sanktionierung des Verantwortlichen.*
- Öffentlicher Bereich / Ministerien, Hochschulen: *Stilllegung des Verfahrens* oder der verwendeten Techniken bis zur Heilung, sofortige Veröffentlichung des Vorfalls, sofortige Bildung eines Untersuchungsausschusses zur Verortung (auch der politischen) Verantwortung sowie einer Projektgruppe zur Behebung des Problems, Prüfung auf strafrechtliche Sanktionierung des Verantwortlichen.

Fortentwicklung des Datenschutzes durch wirksame Risikobearbeitung (4)

Bearbeitung Risiko 6, Datenschutzaufsicht wirksam machen:

- **Schulung von DatenschutzmitarbeiterInnen** (systematisches trainee on job) zu spezialisierten DatenschutzprüferInnen von Organisationen und Verfahren,
- **Standardisierung von Datenschutzprüfmethoden**, Prüfungen, Prüfberichten
- Festlegen von jährlich zu erbringenden **Prüfquoten** (z.B. 50 Initiativ-Prüfungen im Jahr bei verschiedenen Organisationstypen (Sicherheitsbehörden, Leistungs-verwaltung, Hochschulen, Arztpraxis, Bank oder Versicherung, Detekteien, Adresshandel, Kommunalverwaltung, Rechenzentren, Internetprovider)
- **Durchgriff der Datenschutzaufsicht** auf Organisationen analog zu Steuerbehörden
- **Sanktionen bei Untätigkeit** der öffentlichen Datenschutzaufsichtsbehörde (Vorschläge wie bei Risiko 4/5)
- regelmäßige **Audits der Aktivitäten von Aufsichtsbehörden**, zentral durch EU-Kommission
- **Mehr Ressourcen** (Budget, Personal, Prüftechniken) für Aufsichtsbehörden.

Fortentwicklung des Datenschutzes durch LfD / Datenschutzaufsicht

- Aktive Unterstützung bei **Kartellverfahren** sowie von **Verbraucherschutzorganisationen** etwa bei Gerichtsverfahren;
- aktive **Unterstützung der Legislative** (bei Gesetzgebungsverfahren) und **Judikative** (durch Expertise) gegenüber der Exekutive;
- **aktive Unterstüzung der Exekutive durch Machbarkeitsprojekte**, „dass es auch anders geht“;
- Teilnahme an politischen **Kundgebungen und Demonstrationen mit Grundrechtsbezug**;
- Teilnahme an relevanten **Debatten in relevanten Medien** (warum vertreten bspw. Sascha Lobo oder NGO-AktivistInnen Datenschutzpositionen bei Maybritt Illner , nicht aber LfDe?);
- Stabile Kontakte zu allen **politischen Parteien** pflegen;
- Wesentlich mehr **Gerichtsverfahren aktiv herbeiführen** als bislang geschehen;
- Unterstützung von **Peer-Review**-Prozessen bei Selektionsverfahren (von Autoren und von Lehr- und Forschungspersonal);
- Aktive Unterstützung und Betreiben von **Forschungsprojekten**, in denen Maßnahmen zur Minderung der Eingriffsintensität von Verfahren und Techniken entwickelt werden.

Fortentwicklung des Datenschutzes durch spezifische Forschung zu Datenschutzrisiken?

- **Es bedarf einer relevanten transdisziplinäre Datenschutzforschung**, die konzentriert die spezifischen Risiken des Datenschutzes theoretisch gestützt in den Blick nimmt und bearbeitet.
- Es reicht jedoch nicht eine
  - **Projektbegleitungforschung** zu heiklen, latent datenschutz-unfreundlichen Verfahren (bspw. KfZ2KfZ-Kommunikation, Gesichtserkennung, pay-as-you-drive);
  - **technikorientierte Forschung**, die primär auf Aspekte der Risiken der IT-Sicherheit fokussiert.
  - **juristische Forschung** in Qualifizierungsarbeiten, deren Nutzen für die Praxis schwer abzuschätzen ist.
  - **sozialwissenschaftlich inspirierte Privacy-Forschung**, die bspw. den Datenschutz konstituierenden Konflikt nicht bearbeitet oder ihn unkenntlich werden lässt.
  - **psychologisch inspirierte Befindlichkeitsforschung** zur Änderung der Wahrnehmung von Privatheit oder Grundrechten, die bestenfalls zur Fortsetzung der Privatisierung des Datenschutzproblems führt.
  - **philosophisch inspirierte Verethisierung von Konflikten**, die bereits vom bestehenden Recht klar erfasst werden und geregelt sind. Eine bloß affirmative Thematisierung des Vorhandenen führt zur *Delegetimation von Grundrechten* und der Kontroll-Institutionen sowie zur *kulturellen Legitimierung massiver Grundrechtsverstöße* insbesondere totalitär agierender Politbüros wie Google, Facebook, Apple usw..

Literatur

- Alexy, Robert, 2003: Die Gewichtsformel, in: Jickeli, J.; Kreutz, P.; Reuter, D., 2003: Gedächtnisschrift für Jürgen Sonnenschein, Berlin, De Gruyter Verlag, S. 777ff.
- Bieker, Felix, 2018: Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, in DuD 2018/01 (im Erscheinen).
- DSBK 2016: Standard-Datenschutzmodell, Handbuch, V1.0 (herunterladbar von fast allen Webservern der deutschen Datenschutzaufsichtsbehörden, z.B. https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methode_V_1_0.pdf).
- Rost, Martin, 2013: Zur Soziologie des Datenschutzes; in: DuD- Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 85-91.
- Rost, Martin; Storf, Katalin, 2013: Zur Konditionierung von Technik und Recht mittels Schutzzielen; in: Horbach, Matthias (Hrsg.), 2013: Informatik 2013- Informatik angepasst an Mensch, Organisation und Umwelt, 16.-20. September 2013, Koblenz, Lecture Notes in Informatics (LNI)- Proceedings, Series of the Gesellschaft für Informatik e.V. (GI), Volume P-220: 2149-2166.
- Rost, Martin, 2013: Eine kurze Geschichte des Prüfens; in: BSI 2013: Informationssicherheit stärken, Vertrauen in die Zukunft schaffen, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, Gau Algesheim, Secumedia-Verlag: 25-35.
- Rost, Martin, 2014: 9 Thesen zum Datenschutz; in: Pohle, Jörg; Knaut, Andrea (Hsrg), 2014: Fundationes I: Geschichte und Theorie des Datenschutzes.
- Rost, Martin, 2017: Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten; in: Sowa, Aleksandra (Hrsg.), 2017: IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, neue Ansätze für die IT-Revision, Wiesbaden, Springer Vieweg: 23-56.
- Rost, Martin, 2017: Bob, es ist Bob! FiFF-Kommunikation 2017/04 (im Erscheinen).

Viele Texte unter *https://www.maroki.de* verfügbar.

Vielen Dank für Ihre Aufmerksamkeit!

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon: 0431 988 – 1200
uld32@datenschutzzentrum.de
http://www.datenschutzzentrum.de/