TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

IT-Sicherheitsrechtstag 2026

Berlin, 24.09.2026

IT-Sicherheit und Datenschutz - Zwischen Zielkonflikt, Praxisbewältigung und Gesetzgebungsbedarf

Dr. Joanna Reutner LL.M., 4YOU Abiscon GmbH

Für tiefergehende Analysen:

Dissertation: „Die ambivalente Rolle der IT-Sicherheit im Kontext des Datenschutzrechts“

Strukturierung

IT-Sicherheit und Datenschutz - Zwischen **Zielkonflikt** (1), **Praxisbewältigung** (2) und **Gesetzgebungsbedarf** (3)

Begriffsklärung

- Datenschutz
- „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“
- Schützt das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 GG
- Ziel ist die informationelle Autonomie und Integrität des Betroffenen
- Schutz jeglicher personenbezogenen Daten vor missbräuchlicher Verwendung und Verarbeitung
- Zentrale Norm: DSGVO und nationale Datenschutzgesetze

- IT-Sicherheit
- entspricht normativ der „Sicherheit in der Informationstechnik", §2 Nr. 39 BSIG
- „sicher“: „Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen [...]“
- Grundrecht aus Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 Abs. 1 GG („IT-Grundrecht“)

Schutzziele

- Datenschutz: Art. 5 DSGVO
  - Transparenz für Betroffene von Verarbeitungen personenbezogener Daten
  - Zweckbindung der Verarbeitung personenbezogener Daten
  - Datenminimierung einer Verarbeitung personenbezogener Daten
  - Richtigkeit personenbezogener Daten
  - Integrität personenbezogener Daten
  - Vertraulichkeit personenbezogener Daten

- IT-Sicherheit: §2 Nr. 39 BSIG
  - Sicherstellung der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen durch die Definition von Sicherheitsstandards
  - Weitere Schutzziele: Authentitizität, Verdecktheit, Nachweisbarkeit, Verlässlichkeit, Revisionsfähigkeit oder Anonymität

§ 31 BSIG – Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- (1) […]
- (2) Betreiber Kritischer Infrastrukturen sind verpflichtet, für die informationstechnischen Systeme […] Systeme zur Angriffserkennung einzusetzen.

Die Rolle der IT-Sicherheit im Regelungsregime der DSGVO

- Art. 5 Abs. 1 lit. f DSGVO: Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch **geeignete technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“).

- Art. 4 Nr. 12 DSGVO: „Verletzung des Schutzes personenbezogener Daten“: eine Verletzung der **Sicherheit**, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Die Rolle der IT-Sicherheit im Regelungsregime der DSGVO

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Art. 24 Abs. 1 DSGVO: Der Verantwortliche setzt […] geeignete **technische und organisatorische Maßnahmen** um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

- Art. 25 Abs. 1 DSGVO: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten […] trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete **technische und organisatorische Maßnahmen** – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

- **Art. 32 DSGVO:** Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische** Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

IT-Sicherheitsmaßahmen können aus unterschiedlichen Motivationen des Systembetreibers eingesetzt werden:

- Verpflichtung aus IT-Sicherheitsrechts, z.B. §8a Abs. 1 a BSIG,
- als freiwillige Maßnahme zum Schutz von sensiblen Unternehmensinterna oder
- in Gestalt einer technischen oder organisatorischen Maßnahme nach Art. 32 Abs. 1 DSGVO.

Bei allen Fällen gilt:

- Sobald personenbezogene Daten im Rahmen von IT-Sicherheitsmaßnahmen verarbeitet werden, findet laut Art. 2 die DSGVO Anwendung
- Datenverarbeitung sind nur rechtmäßig, wenn sie Art. 6 Abs. 1 DSGVO
- Sowie die Verarbeitungsgrundsätze nach Art. 5 Abs. 1 DSGVO erfüllen
- Abwägungserfordernis innerhalb der Rechtsgrundlage (z.B. Art. 32 DSGVO)

Die Rechtmäßigkeit von Datenverarbeitungen

Art. 6 Abs. 1 DSGVO:

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

lit. c: die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

[…]

lit. f: die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen […]

Technische Schutzmaßnahmen und ihre datenschutzrechtliche Problematik: Beispiele aus der Praxis

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Log-Dateien
- Softwaretests mit Originaldaten
- Erstellung von Berechtigungskonzepten
- Zugriffsrechte von Systemadministratoren
- SIEM-Systeme

Umgang mit dem Spannungsverhältnis

Ergebnis: Unverbundenes Nebeneinander von Datenschutz und IT-Sicherheit und Bedürfnis nach Rechtssicherheit seitens der Normadressaten

Mittel bzw. Instrument der Zusammenführung der beiden Materien zur Klarstellung der datenschutzrechtlichen Zulässigkeit von IT-Sicherheitsmaßnahmen?

- BSI-IT-Grundschutz-Kompendium (-)
- Risikobasierte Managementsysteme: ISMS/ DSMS (-)
- PIMS/ ISO 27701 (-)
- Standard-Datenschutz-Modell (-)

Beispiel: Erstellung eines Berechtigungskonzepts

BSI-IT—Grundschutz: Baustein ORP.4, verweist auf Anhang A9 der ISO/IEC 27001:2013 ->keine Behandlung der datenschutzrechtlichen Fragestellungen

SDM Referenzmaßnahmenkatalog, Baustein 51

Zwischenfazit: Rechtsanwender bleibt mit unbestimmten Rechtsbegriffen und komplexen und aufwändigen Abwägungserfordernissen zurück

Lösungsansätze im Spannungsverhältnis IT-Sicherheit vs. Datenschutz

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Lösung über teleologische Auslegung des Begriffs der „Geeignetheit“
- Lösung durch rechtsadäquate Technikgestaltung
- Lösung durch gesetzliche Herstellung eines Gleichgewichts: Privilegierungstatbestand: eigene Erlaubnisnorm im Katalog des Art. 6 Abs. 1 DSGVO
- Abkehr vom risikobasierten Ansatz
- Gesetzliches Risikomanagement
- Lösung durch Anerkennung harmonisierter Normen nach dem Vorbild des ProdSG G i. V. m. VO(EU) 1025/2012 bzw. Art. 40 Abs. 1 KI-VO i. V. m. VO(EU) 1025/2012
- Lösung durch delegierte und Durchführungsrechtsakte