



Datenschutz und Technik – Kartographie eines Feldes

Grundlagen des Datenschutzes

Das Bundesdatenschutzgesetz dient nach § 1 Abs. 1 dem Schutz des Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten.

Das zu schützende Subjekt ist der Mensch (**Betroffener**, *data subject*).

Geschützt wird sein **Persönlichkeitsrecht**, dem – innerhalb der Vergleichbarkeitsgrenzen grundverschiedener Rechtskreise – die amerikanische *privacy* weitgehend entspricht.

Die Schutzgrenze ist wegen der fundamentalen Bedeutung des Persönlichkeitsrechts im liberalen Rechtsstaat sehr weit nach vorn verlagert: Es soll bereits vor Beeinträchtigungen geschützt werden.

Schutzobjekte – und damit Dreh- und Angelpunkt des Datenschutzrechts – sind die **personenbezogenen Daten** (*personal data*), zu denen auch die perso-

nenbeziehbaren Daten gerechnet werden.

Aus historischen Gründen wird der **Umgang** in Verarbeitungsphasen partitioniert und gesetzlich einzeln geregelt. Dass durch die einzelnen Phasen alle Arten des Umgangs abgedeckt werden, folgt – auch wenn manche Formulierungen im Gesetz anderes nahelegen – direkt aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983.

Adressat der Datenschutzgesetze – und damit zur Umsetzung des Schutzes verpflichtet und dem Betroffenen gegenüber verantwortlich – ist die **verantwortliche Stelle** (*data processor*). Damit ist jede Person oder Organisation gemeint, die mit personenbezogenen Daten für sich selbst – mit eigenem Interesse – umgeht oder dies durch andere im Auftrag vornehmen lässt. Die Datenverarbeitung für persönliche oder familiäre Zwecke fällt nicht unter das Datenschutzrecht.

Wer personenbezogene Daten nicht für sich selbst, sondern nur für andere im Auftrag verarbeitet, heißt **Auftragsdatenverarbeiter**.

Dritter ist jede Person oder Stelle, außer der verantwortlichen Stelle und dem Betroffenen. Auch Auftragsdatenverarbeiter, wenn sie im Inland, der EU oder dem EWR ihren Sitz haben, sind nicht Dritte.

Auf zwei Ebenen wird die Datenschutzpraxis kontrolliert – innerhalb der verantwortlichen Stelle durch behördliche und betriebliche **Datenschutzbeauftragte** und extern durch Landes- und Bundesdatenschutzbeauftragte.

Nach der **zentralen Grundregel des Datenschutzes** ist der Umgang mit personenbezogenen Daten verboten, es sei denn, er ist gesetzlich angeordnet oder erlaubt oder der Betroffene hat eingewilligt. In den beiden letzten Fällen müssen die Daten grundsätzlich direkt beim Betroffenen erhoben werden.

Datenschutz und IT-Sicherheit

IT-Sicherheit dient dem Schutz der eigenen Interessen vor den illegitimen Informationsinteressen eines anderen – sie trennt zwischen »Innen« und »Außen«. Hinsichtlich personenbezogener Daten schützt die verantwortliche Stelle die gemeinsamen Interessen von ihr und dem Betroffenen – Stelle und Betroffener sind in diesem Fall zusammen »innen«. **IT-Sicherheit ist somit notwendige, aber nicht hinreichende Bedingung des Datenschutzes.**

Der Datenschutz verpflichtet die verantwortliche Stelle zur Beschränkung ihres eigenen – legitimen – Informationsinteresses zum Schutz des Betroffenen. Es geht dabei also um eine Ausgestaltung des Innenverhältnisses zwischen Stelle und Betroffenen. Wo IT-Sicherheitsmaßnahmen nicht mehr greifen könnten, weil der Andere schon Zugriff auf die Daten hat, liegt der Kernbereich des Datenschutzes.

Datenschutz und Selbstschutz

Der Datenschutz statuiert Anforderungen an die verantwortliche Stelle. Der Selbstschutz hingegen gibt dem Betroffenen vor allem Werkzeuge (z. B. Verschlüsselung oder Anonymizer) und Methoden (z. B. Schulungsmaterial oder Auskunftsvorlagen) an die Hand, um der Informationsmacht der verantwortlichen Stelle – auch gegen deren Willen – wirksam entgegen treten zu können.

Auf Seiten der verantwortlichen Stelle kann Technik dies unterstützen, indem sie es dem Betroffenen etwa ermöglicht, Auskunft über die zu seiner Person gespeicherten Daten zu erlangen, ohne dass er die Stelle um Auskunft »bitten« muss und ohne dass die Stelle davon erfahren und zum Nachteil des Betroffenen reagieren kann. Techniken des Selbstschutzes können somit bei der **Rechtsdurchsetzung** helfen.

Verantwortliche Stelle und Technik

Nur wenige Datenschutzregelungen sind explizit als Anforderungen an die Technik formuliert. Einige dieser Anforderungen beziehen sich dabei auf durchzuführende Abwägungen bei der Gestaltung und Auswahl der einzusetzenden Technik. Insgesamt wird dem Datenverarbeiter hinsichtlich der verwendeten Technik und ihrer Nutzung große Freiheit gelassen.

Die verantwortliche Stelle hat dem Betroffenen gegenüber Datenschutzkonformität zu garantieren. Ihre interne Organisation und ihre Nutzung oder Nichtnutzung von Technik liegen in ihrer alleinigen Verantwortung. Technische Beschränkungen oder Fehler dürfen daher nicht als Ausrede gegenüber dem Betroffenen verwendet werden.

Technik soll die verantwortliche Stelle unterstützen, ihrer Verantwortung gerecht zu werden.

Gründe für Datenschutzverletzungen

Die in der Öffentlichkeit sichtbarsten Datenschutzverletzungen werden in der großen Mehrzahl der Fälle von den Tätern **vorsätzlich** – wissentlich und willentlich – begangen.

Der in absoluten Zahlen größte Teil der Datenschutzverletzungen geschieht jedoch **fahrlässig**: Bei Beachtung der erforderlichen Sorgfalt hätten die Verantwortlichen den Datenschutzverstoß verhindern können. Aus zwei Gründen ist das schwierig. Erstens wissen die meisten Verantwortlichen gar nicht – oder nicht genau –, welche Maßnahmen in welchem Umfang jeweils erforderlich sind. Dies gilt vor allem dann, wenn das bestehende Recht auf neue technische Entwicklungen angewendet werden muss. Und zweitens werden viele Verstöße nur durch Zufall entdeckt, weil notwendige Methoden und Werkzeuge unterentwickelt oder nicht existent sind.

Datenschutz und Technik

Verschiedene Begriffe zur Beschreibung der Datenschutzeigenschaften von Technik werden oftmals gleichbedeutend genutzt. Eine begriffliche Klarstellung ist dringend notwendig.

Datenschutz(rechts)konform kann allein eine Praxis, nicht aber die eingesetzte Technik, sein.

Technik soll **datenschutzfeindlich** heißen, wenn sie nicht datenschutzkonform eingesetzt werden kann. Sie soll als **datenschutzneutral** bezeichnet werden, wenn die Konformität nur von der Art und Weise des konkreten Einsatzes abhängt. Sie soll **datenschutzfreundlich** heißen, wenn sie die verantwortliche Stelle in der datenschutzkonformen Umsetzung der Datenverarbeitung unterstützt. Und sie soll **datenschutzfördernd** heißen, wenn sie unabhängig von der Intention der verantwortlichen Stelle ausschließlich datenschutzkonform eingesetzt werden kann.

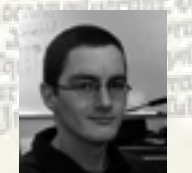
Literatur

Roßnagel / Pfitzmann / Garstka, *Modernisierung des Datenschutzrechts*. Gutachten im Auftrag des Bundesministeriums des Innern, 2005.

Simitis (Hrsg.), *Bundesdatenschutzgesetz*. Baden-Baden: Nomos Verlagsgesellschaft, 7. Auflage, 2011.

Tinnefeld / Ehmann / Gerling, *Einführung in das Datenschutzrecht*. München: Oldenbourg Verlag, 4. Auflage, 2005.

Westin, *Privacy and Freedom*. New York: Atheneum, 1967.



Jörg Pohle