AK Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Orientierungshilfen für die Datenschutzpraxis

Am 2. November 2009 hat der AK Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder drei neue bzw. aktualisierte Orientierungshilfen herausgegeben.

Orientierungshilfe zum Thema Biometrische Authentisierung – Möglichkeiten und Grenzen

Die Authentisierung von Personen mit bestimmten körperlichen Merkmalen wie z. B. Fingerabdrücken, Gesichtsgeometrie oder Irismuster wird gelegentlich als Alternative zu den Authentisierungsverfahren durch Besitz und/oder Wissen angesehen. In dieser Orientierungshilfe geht es nicht um die spezifischen Datenschutzfragen beim Einsatz biometrischer Verfahren, sondern um die Möglichkeiten und Grenzen dieser Verfahren bei der Authentisierung.

Die biometrischen Daten sind – im Gegensatz zu UserID und Passwort und zu Verfahren von Besitz und Wissen – eindeutig und potenziell lebenslang mit der Betroffenen verbunden.

Deshalb sind für biometrische Authentisierungsverfahren – unabhängig vom verwendeten biometrischen Verfahren – besondere Vorkehrungen zu treffen, damit sich die Stärke biometrischer Verfahren zur Authentisierung entfalten kann:

- Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.
- Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z. B. auf einer Chipkarte, realisiert werden.
- Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptografischer Verfahren.

Die biometrischen Daten sind nicht geheim und sie können nach Bekanntwerden oder Missbrauch nicht verändert oder gesperrt werden. Deshalb ist folgendes wichtig:

- Die biometrischen Daten dürfen nicht allein zur Authentisierung herangezogen werden, sondern sie sind mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

Orientierungshilfe zum Thema Protokollierung

Sowohl die Datenschutzgesetze der Länder als auch das Bundesdatenschutzgesetz enthalten Regelungen, aus denen sich die Pflicht zur Protokollierung ergibt oder zumindest ableiten lässt. In einigen Landesdatenschutzgesetzen findet man das Regelungsziel Revisionsfähigkeit, das insbesondere durch die Maßnahme der Protokollierung umgesetzt werden kann. Das Bundesdatenschutzgesetz (BDSG) und andere Landesdatenschutzgesetze normieren Kontrollziele wie Eingabekontrolle oder Verantwortlichkeitskontrolle, aus denen sich ebenfalls die Pflicht zur Protokollierung ableiten lässt. Im BDSG zeigt sich am Beispiel der Anlage zu § 9, dass praktisch keine der dort konkret aufgeführten technisch-organisatorischen Maßnahmen ohne das Vorsehen einer Nachweismöglichkeit, die typischerweise in Form eines Protokolls geschieht, umsetzbar ist. Für eine Reihe von Verwaltungsverfahren gelten zudem bereichsspezifische, vom Datenschutzrecht des Bundes bzw. des betreffenden Landes abweichende, oft wesentlich konkretere Protokollierungsvorschriften (Beispiele: Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze usw.). Obwohl die Datenschutzgesetze von Bund und Ländern Regelungen enthalten, aus denen sich die Pflicht zur Protokollierung ableiten lässt, gibt es nur wenige Vorgaben für die konkrete Ausgestaltung der Protokollierung. Dennoch haben sich auf Basis der Anforderungen erprobte Vorgehensweisen entwickelt, die in dieser Orientierungshilfe als grundlegende Empfehlungen dargestellt werden.

Orientierungshilfe zum Thema Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb

Personenbezogene Daten sind vor der Freigabe eines Systems nicht weniger schutzbedürftig als nach dessen Freigabe. Die Regelungen der Landesdatenschutzgesetze und des Bundesdatenschutzgesetzes gelten für die Verarbeitung personenbezogener Daten ungeachtet der Frage, ob die Datenverarbeitung bereits im Produktivbetrieb oder noch in einer Projektphase erfolgt.

Unabhängig von der jeweiligen Phase, in der sich ein Projekt befindet, ist eine Dokumentation erforderlich, der die definierten Ziele, die technischen Mittel und Instrumente, die Festlegung der einzelnen Projektphasen mit Beginn und Ende, die Benennung der verantwortlichen Personen und die Entscheidung der verantwortlichen Person über den Beginn einer Projektphase, die Dokumentation des Projektverlaufes sowie die Ergebnisse und Schlussfolgerungen zu entnehmen sind.

Der Detaillierungsgrad dieser Dokumentation kann sich nach der Entwicklungsphase richten, in der sich ein Verfahren zur Verarbeitung personenbezogener Daten befindet.

In dieser Orientierungshilfe werden die wesentlichen zu beachtenden datenschutzrechtlichen Protokollierungsaspekte in den Ablaufphasen

- Projektbetrieb, mit Funktionstest sowie Integrations- und Abnahmetest
- Produktivbetrieb mit Pilot- und Regelbetrieb

dargestellt.

Die drei neuen Orientierungshilfen können über die Adressen
http://www.lfd.m-v.de/dschutz/informat/biometrie/oh-biometrie.pdf
http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf
http://www.lfd.m-v.de/dschutz/informat/projekt/oh_projekt.pdf
bezogen werden.