



ERSTELLUNG VON VERFAHRENSVERZEICHNISSEN UND DURCHFÜHRUNG VON VORABKONTROLLEN

PERSICON@night | 17. September 2009

Verfahrensverzeichnis

Zusammenhang zwischen Meldepflicht und Verzeichnis

- Grundsatz:
 - Meldepflicht der Unternehmen für automatisierte Verarbeitungen bei der Aufsichtsbehörde vor Inbetriebnahme
 - Inhalt der Meldepflicht ergibt sich aus § 4e S. 1 BDSG.
 - Das Verzeichnis ist für jeden bei der Aufsichtsbehörde einsehbar.
- Ausnahme:
 - Die Meldepflicht entfällt, wenn ein Datenschutzbeauftragter bestellt wurde
→ es ist dann die Aufgabe des Unternehmens, ein Verzeichnis zu führen.
 - Die Meldepflicht für automatisierte Verfahren ist in Form eines Verzeichnisses umzusetzen.

Verfahrensverzeichnis (1)

- Das Verfahrensverzeichnis dient als Übersicht für die in einem Unternehmen eingesetzten Verfahren.
 - Art der personenbezogenen Daten
 - Welche automatisierte Verfahren werden verwendet
 - Art der Datenerhebung-, verarbeitung oder -nutzung
 - Art der Datenschutzmaßnahmen
- Ein Verfahren ist die Gesamtheit an Verarbeitungen, mit deren Hilfe ein gewisser Zweck realisiert wird.
- Es ist zu unterscheiden:
 - öffentliches/externes Verfahrensverzeichnis → Auskunftsanspruch des Betroffenen
 - nicht-öffentliches/internes Verfahrensverzeichnis → betriebsinterne Selbstkontrolle

Verfahrensverzeichnis (2)

- Verantwortung für die Erstellung von Verfahrensverzeichnissen:
 - Formal → die verantwortliche Stelle, d.h. immer die übergeordnete juristische Personen, der die Organisationseinheit gehört (z. B. GmbH, AG)
 - Das Unternehmen muss die erforderlichen Informationen für das Verzeichnis liefern und bleibt formal dafür verantwortlich.
- Verantwortung im Rahmen der Auftragsdatenverarbeitung:
 - Der Auftraggeber bleibt verantwortlich.
 - Ggf. Mitwirkungspflichten des Auftragnehmers im Vertrag definieren
- Die Art der Veröffentlichung liegt im Ermessen der verantwortlichen Stelle (z. B. Internet, Weitergabe der Information in Form eines Formulars)

Beispiele

- TK-Anlage
- Videoüberwachung
- Personalmanagementsysteme
- Buchhaltung, sofern personenbezogene Daten enthalten sind (z. B. Lohnbuchhaltung)
- Verwaltung des Fuhrparks
- Einsatz von Spezialsoftware
 - Customer Relationship Managementsysteme (CRM)
 - SAP HCM
 - SAP HR
 - Etc.
- Office
 - Erstellung von Berichten
 - Erstellung von Auswertungen mit Standardwerkzeugen der Bürokommunikation
- Produktion/Vertrieb
 - Dokumentation der für Kunden erstellten Angebote sowie der erteilten Kundenaufträge in Verbindung mit personenbezogenen Daten von Mietern, Käufern, Dienstleistungsempfängern etc.
 - Verarbeitung von personenbezogenen Daten zur Auftragsabwicklung und Service-Bereitstellung

Inhalt des Verfahrensverzeichnis

Inhalt des Verfahrensverzeichnis → Mindestanforderungen:

1. Name oder Firma der verantwortlichen Stelle
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen
3. Anschrift der verantwortlichen Stelle
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung
5. Eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
7. Regelfristen für die Löschung der Daten
8. Eine geplante Datenübermittlung in Drittstaaten
9. Eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind. (internes Verfahrensverzeichnis)

Erstellung von Verfahrensverzeichnis (1)

- Identifizierung automatisierter Verfahren
 - Sichtung des Organigramms
 - Übersicht der im Unternehmen eingesetzten Anwendungen → Netzwerkstrukturplan
- Sensibilisierung der Fachabteilungen
- Interviews zwischen Datenschutzbeauftragten und Fachverantwortlichen
 - Vorbereitete Fragebögen → Festlegung von Rückgabeterminen
 - Terminverfolgung durch den Datenschutzbeauftragten
 - Abstimmung zu Rückfragen → direkter Dialog
 - Inhaltliche Prüfung der Meldungen

Erstellung von Verfahrensverzeichnissen (2)

- Erstellung des Verfahrensverzeichnisses
 - Papierform
 - Excel-Tabellen
 - Access-Datenbank
 - HTML-Format
 - (Selbst erstellte) Softwareprogramme
 - Etc.
- Freigabe des Verfahrensverzeichnisses durch den jeweiligen Fachverantwortlichen unter Einbeziehung des Datenschutzbeauftragten
- Regelmäßige Aktualisierung und Prüfung auf Vollständigkeit

Durchführung von Vorabkontrollen

Vorabkontrolle (1)

- Vor Einrichtung bestimmter automatisierter Verfahren muss grundsätzlich eine besondere Rechtmäßigkeitskontrolle vorgenommen werden, sog. Vorabkontrolle:
 - Verarbeitung „besonderer Arten“ personenbezogener Daten
 - Bewertung der Persönlichkeit, Fähigkeiten, Leistung oder des Verhaltens
- Beispiele:
 - Videoüberwachung
 - Zutrittskontrollsysteme
 - Bewertung des Kaufverhaltens
 - Scoring-Verfahren
- Zuständigkeit:
 - Datenschutzbeauftragter
 - Aufsichtsbehörden

Vorabkontrolle (2)

- Im Rahmen der Vorabkontrolle wird die materielle Rechtmäßigkeit der Datenverarbeitung durch den DSB vorgenommen.
- Dabei wird z. B. geprüft:
 - Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (§ 4 BDSG)
 - Voraussetzungen der Einwilligung (§ 4a BDSG)
 - Feststellung der Minderung besonderer Risiken für die Rechte und Freiheiten der Betroffenen vermindert worden
 - Einhaltung des Systemdatenschutzes (§ 3a BDSG)

Vorabkontrolle (3)

- Darüber hinaus prüft der DSB das für dieses Verfahren erstellte Verzeichnis gemäß § 4e BDSG.
- *Wichtig:*
 - Die Vorabkontrolle hat vor Inbetriebnahme zu erfolgen!
 - Ein Verstoß gegen die Meldepflicht stellt eine Ordnungswidrigkeit gemäß § 43 BDSG dar.

Mitwirkung von Verantwortlichen bei der Vorabkontrolle und Erstellung von Verfahrensverzeichnis

Management und Datenschutzbeauftragter (1)

- Es ist die nachdrückliche und aktive Unterstützung des Managements notwendig.
- Die Aufmerksamkeit für das Thema Sicherheit muss geschaffen werden.
- Das Interesse an angemessener Sicherheit muss geweckt/intensiviert werden:
 - Persönliche Haftung der Organisationsleitung
 - Rechtliche Anforderungen
 - Sicherheit als Wettbewerbsfaktor und Geschäftsvoraussetzung
- **Marketing in „eigener Sache“**

Management und Datenschutzbeauftragter (2)

- Sensibilisierung und Motivation des Managements:
 - Z. B. persönliche Absicherung durch unabhängige Zertifizierung
 - Wertbeitrag transparent kommunizieren (Nutzen und Maßnahmen eines IT-Risiko Management Systems verdeutlichen).
 - Für Veränderung motivieren (z. B. Negativ-Beispiele, Branchenvergleich - Vorbilder/Konkurrenz).
- Es sollte ein Mindestmaß an grundlegenden Fachkenntnissen vermittelt werden.
- Kombination aus technischen, organisatorischen und personellen Maßnahmen ist erforderlich.

Management und Datenschutzbeauftragter (3)

Risiko- und Kontrollkultur:

- Gemeinsames, grundlegendes Normen- und Wertegerüst
- Bildet das Fundament für die einzelnen Maßnahmen
- Bestimmt die Effektivität des Risikomanagements
- Schlägt sich im Wissen, den Fähigkeiten und der Einstellung der Mitarbeiter nieder
- Lässt sich nicht von heute auf morgen durch einige Strukturveränderungen „organisieren“

Management und Datenschutzbeauftragter (4)

Risiko- und Kontrollkultur:

- Die Sensibilisierung aller Mitarbeiter (inklusive Management) für die dem Unternehmen, dem Geschäftsbetrieb sowie seinen Aktivitäten und Werte innewohnenden Risiken (inhärente Risiken).
- Etablierung einer funktionierenden Kommunikation - sowohl vertikal als auch horizontal.
- Etablierung einer risikoorientierten Unternehmenskultur, initiiert und geprägt durch:
 - Risikopolitik
 - Vorbildfunktion der Unternehmensleitung und Management

Management und Datenschutzbeauftragter (5)

- „Verbündete suchen“
- Gemeinsame Ziele und Methoden identifizieren (z. B. Umsetzung der technischen/organisatorischen Maßnahmen gemäß der Anlage zu § 9 BDSG nach IT-Grundschutz)
- Mitwirkung bzw. Information anstreben:
 - Einladung zu Kick-off-Meeting
 - Arbeitsgruppen
 - Datenschutzteam
 - Gemeinsame Abstimmungsgespräche

Welche Fragen haben Sie?

Vielen Dank für Ihre Aufmerksamkeit.

www.persicon.com