Die EU-Datenschutz-Grundverordnung und ihre Auswirkungen auf das Institut der behördlichen/betrieblichen Datenschutzbeauftragten

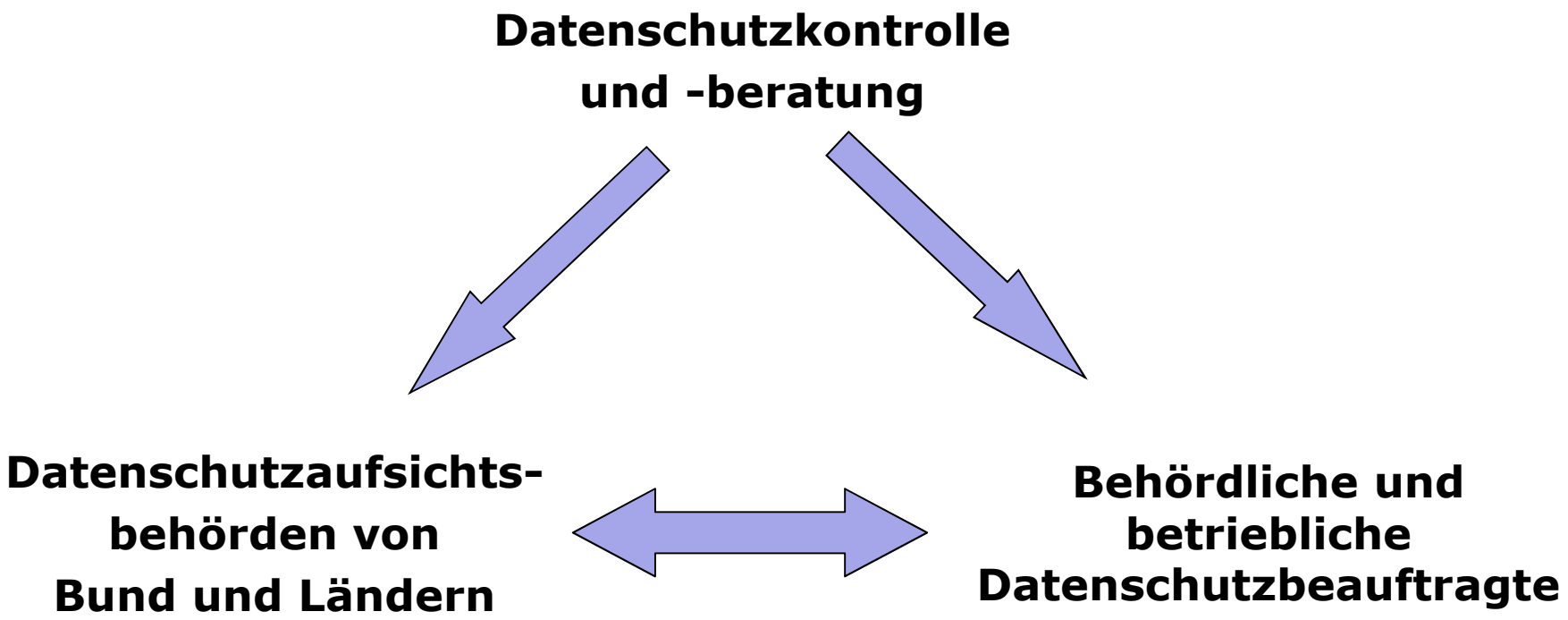
Barbara Thiel
Landesbeauftragte für den Datenschutz Niedersachsen

29.11.2016

Agenda

1. Einleitung
2. Das deutsche Datenschutzkontrollmodell – eine Erfolgsgeschichte
3. Wer muss nach EU-Recht Datenschutz-beauftragte (DSB) benennen?
4. Die Stellung des DSB nach der DS-GVO
5. Die Aufgaben des DSB nach der DS-GVO
   - Übersicht inkl. Vergleich mit dem heutigen Recht
   - Risikobasierter Ansatz
   - „Accountability" als neuer Grundsatz
   - Datenschutzmanagement-System
6. Fazit

Das deutsche Datenschutzkontrollmodell – eine Erfolgsgeschichte



Wer muss nach der DS-GVO (Art. 37 Abs. 1) einen DSB benennen?

- **Behörden oder öffentliche Stellen mit Ausnahme von Gerichten**
- **Unternehmen**, wenn **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters **Verarbeitungsvorgänge** sind, welche eine umfangreiche regelmäßige und systematische **Überwachung von betroffenen Personen** erforderlich machen
- **Unternehmen**, wenn die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** gem. Art. 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht

Beachte:

Art. 37 Abs. 4 DS-GVO enthält Öffnungsklausel für strengere nationale Regelungen

Die Stellung des DSB nach der DS-GVO im Vergleich zum BDSG

BDSG	EU DS GVO
DSB unmittelbar der Unternehmensleitung unterstellt	DSB berichtend an die höchste Ebene (Art. 38 Abs. 3):
Fachkunde und Zuverlässigkeit	Berufliche Qualifikation; Fachwissen auf dem Gebiet Datenschutzrecht und –praxis und die Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben (Art. 37 Abs. 5)
Fortbildungsanspruch	Erhalt der Fachkenntnisse (Art. 38 Abs. 2)
Unterstützungspflicht durch das Unternehmen	Unterstützungspflicht durch Unternehmen: erforderliche Ressourcen, Zugang zu pb Daten und Verarbeitungsvorgängen (Art. 38 Abs. 2)
Weisungsfreiheit bei der Ausübung der Fachkunde	Weisungsfreiheit bzgl. der Ausübung d. Aufgaben (Art. 38 Abs. 3)
Unterrichtungspflicht über „Vorhaben der automatisierten Verarbeitung personenbezogener Daten“	„Ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ (Art. 38 Abs. 1)
Kündigungs- sowie Abberufungsschutz	Abberufungsschutz und Benachteiligungsverbot (Art. 38 Abs. 3)

Stärkung des Überwachungs- und Beratungsauftrags

BDSG	EU DS GVO
Mitarbeiterinformation	Unterrichtungs- und Beratungspflichten (Art. 39 Abs. 1)
Verfügbarmachung des Verfahrensverzeichnisses für Jedermann im Antragsverfahren	–
Vorabkontrolle kritischer Datenverarbeitung	Datenschutzfolgenabschätzung (Art. 35)
Recht zur Konsultation der Aufsichtsbehörde	Kontaktstelle zur bzw. Zusammenarbeit mit Aufsichtsbehörde (Art. 39 Abs. 1 lit. b)
Überwachung der DV-Programme und Hinwirken auf die Einhaltung der Gesetze und Vorschriften zur Datenschutz	Überwachung der Einhaltung DS-GVO, weiterer Rechtsvorschriften sowie der Strategien des Verantwortlichen/Auftragsdatenverarbeiters (Art. 39 Abs. 1 lit. b)
–	**Rechenschaftspflicht** (Accountability) (Art. 5 Abs. 2)

Risikobasierter Ansatz der DS-GVO

Artikel 24

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. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert

Artikel 32

Sicherheit der Verarbeitung

(1)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; diese Maßnahmen schließen unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1)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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen 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 — trifft, 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.

Artikel 35

Datenschutz-Folgenabschätzung

(1)Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Risikobasierter Ansatz – (sämtliche) Maßnahmen müssen risikoangemessen sein!

Die Landesbeauftragte für den Datenschutz Niedersachsen

Definition „Accountability“, Art. 5 Abs. 2 DS-GVO

Artikel 5 Absatz 2: „Rechenschaftspflicht“

Der Verantwortliche ist für die Einhaltung des Absatzes 1 **verantwortlich** und muss dessen Einhaltung **nachweisen** können.

Art. 5 Abs. 1

Die sechs Grundsätze der Verarbeitung

1. Rechtmäßigkeit, Transparenz
2. Zweckbindung
3. Datenminimierung
4. Integrität und Vertraulichkeit
5. Richtigkeit
6. Speicherbegrenzung

Konkretisierung der Accountability durch Art. 24 DS-GVO

Abschnitt 1

Allgemeine Pflichten

Artikel 24

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. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Erwägungsgrund 74

Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

- **Nachweispflicht**
- **Management der Datenschutz-Risiken**
- **Pflicht zur Datenschutz-Organisation**

Wesentliche Elemente sind:

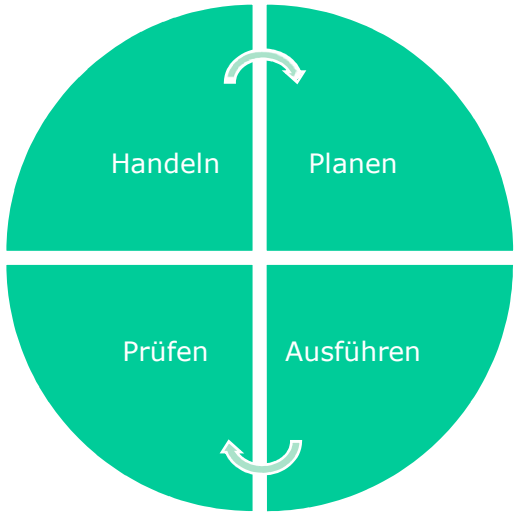
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutzfolgenabschätzung für risikobehaftete Datenverarbeitungen
- Datenschutzkonzepte/Datenschutzrichtlinie
- IT-Sicherheitskonzept mit Beschreibung der getroffenen technischen und organisatorischen Datensicherungsmaßnahmen
- Dokumentation von Einwilligungserklärungen, Vereinbarungen zur Auftragsverarbeitung und Schulungsmaßnahmen
- Zertifikat/Datenschutzaudit eines unabhängigen Dritten

Ein Datenschutzmanagement-System stellt

- die **Gesamtheit aller**
- dokumentierten und implementierten **Regelungen, Prozesse und Maßnahmen** dar,
- mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen systematisch gesteuert wird

In der Gesamtschau der Regelungen der DS-GVO wird ein Datenschutzmanagement-System nunmehr ein verpflichtendes Element für die Datenschutzorganisation sein, um die zahlreichen Pflichten umzusetzen und ihre Erfüllung im Zweifel nachweisen zu können.

PDCA-Zirkel



Fazit

1. Stellung des DSB nach DS-GVO mit BDSG vergleichbar

- Stellung des DSB in der Organisation des Verantwortlichen entspricht weitgehend dem jetzigen Recht, jedoch mit angepasstem Aufgabenfokus

2. Aufgaben des DSB mit angepasstem Fokus

- Aufgaben verlagern sich vom „Hinwirken" nach BDSG auf Beratungs- und Überwachungsauftrag
- Aufgaben werden teilweise (entsprechend „Accountability") auf den Verantwortlichen verlagert
- Aufgabenwahrnehmung des DSB ist geprägt von risikobasiertem Ansatz
- Aufgabenwahrnehmung muss Rechenschaftspflicht (des Verantwortlichen!) besonders berücksichtigen

3. DSB verantwortet kein Tagesgeschäft

- Verantwortung des DSB beinhaltet nicht die operative Umsetzung durch andere Stellen in der Organisation des Verantwortlichen (Fachseiten/Abteilungen)
- DSB berät/überwacht

Ich danke Ihnen für Ihre Aufmerksamkeit.

Barbara Thiel

Die Landesbeauftragte für den
Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120 4501
Telefax 0511 120 4599

barbara.thiel@lfd.niedersachsen.de

www.lfd.niedersachsen.de
www.datenschutz.de