

Was bedeuten die aktuellen Neuerungen im BDSG in der Praxis für den Logistikprozess ?



MERENTIS DataSec GmbH

Datenschutz und IT-Sicherheit

Gerhard Stampe
geschäftsführender Gesellschafter

3. IFIT Security Day
27. Januar 2010

- **Das personenbezogene Datum als logistischer Prozess**
- **Hinweise aus dem BDSG**
- **Aktuelle Änderungen des BDSG (Novelle II)**
 - **Beispiel: Die Auftragsdatenverarbeitung**



Daten sind Phänomene! Daten leben!

Daten werden geboren (irgendwann werden sie erhoben und zum Zweck einer späteren Nutzung gespeichert), Daten vermehren sich (Generationenprinzip), Daten müssen wieder sterben (d.h., sie sterben nicht von alleine, sondern sie müssen gelöscht bzw. vernichtet werden).



Das personenbezogene Datum als logistischer Prozess



Def

Personenbezogene Daten (pbDaten)

pbDaten sind Einzelangaben über **persönliche** oder **sachliche** Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Persönliche Verhältnisse

Name, Anschrift, Familienstand,
Geburtsdatum, Staatsangehörigkeit,
Beruf, Konfession, Krankheiten, ...

Sachliche Verhältnisse

Einkommen, Eigentumsverhältnisse,
KFZ-Typ, Steuern, Versicherungen,
...

Selbstkontrolle: Bestellung eines Datenschutzbeauftragten (DSB)



Manuelle Verarbeitung:

Wenn mindestens 20 Personen manuell pbDaten erheben, verarbeiten oder nutzen.

Automatisierte Datenverarbeitung:

- Wenn mindestens 10 Beschäftigte pbDaten erheben, verarbeiten oder nutzen oder
- wenn die Verarbeitung der Vorabkontrolle unterliegt.

Grundsätzlich gilt: **Verbot mit Erlaubnisvorbehalt**
für Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Def

Zulässigkeit

Die Erhebung, Verarbeitung und Nutzung von pbDaten ist nur zulässig, soweit

- das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder
- der Betroffene eingewilligt hat.

„Was bedeuten die aktuellen Neuerungen im BDSG für den Logistikprozess ?“

BDSG

- Werden personenbezogene Daten im Prozess verarbeitet ?
- Beachtung des BDSG und anderer Rechtsvorschriften !
 - Datenschutzbeauftragter
 - Prüfung der Zulässigkeit der Datenverarbeitung
 - Dokumentationspflichten
 - Rechte der Betroffenen
 - Technisch- organisatorische Maßnahmen (8 Gebote)

Aktuelle Änderungen des BDSG / seit 1.9.2009 in Kraft !

BDSG

BDSG-Novelle II

- Personalisierte Werbung
- Arbeitnehmerdatenschutz
- Informationspflicht über Datenpannen
- Kündigungsschutz für den DSB
- Erweiterte Anforderungen an die Auftragsdatenverarbeitung

Bußgeldbewährt (im Einzelfall 50 – 300 Tsd €)



Def



Auftragsdatenverarbeitung

Von Datenverarbeitung im Auftrag spricht man, wenn sich die verantwortliche Stelle einer Stelle bedient, die für diese im Auftrag pbDaten erhebt, verarbeitet oder nutzt (z.B. Rechenzentrumsdienstleistungen, IT-Wartung, oder Entsorgung).

Erhebung, Verarbeitung, Nutzung
im **Auftrag** ist zulässig:



Unternehmen als Auftraggeber

- sorgfältige Auswahl des Auftragnehmers
- schriftlicher Vertrag
- von der Einhaltung der Sicherheitsmaßnahmen überzeugen



Unternehmen als Auftragnehmer

- Arbeiten nach Weisung des Auftraggebers
- Bestellung eines Datenschutzbeauftragten



**Gilt auch bei Konzerngesellschaften und
für Wartung automatisierter Verfahren und DV-Anlagen**

Erweiterte Anforderungen an die Auftragsdatenverarbeitung !

BDSG

Gesetzestext

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

- (1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.....*
- (2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:*



Erweiterte Anforderungen an die Auftragsdatenverarbeitung !

BDSG

Vertragliche Inhalte nach §11 BDSG (Teil1)

- Gegenstand und Dauer des Auftrages

- Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

- Die nach §9 BDSG zu treffenden technischen und organisatorische Maßnahmen (IT-Sicherheit)

- Die Berichtigung, Löschung und Sperrung von Daten

- Die bestehenden Pflichten des AN, die von ihm vorzunehmenden Kontrollen



Erweiterte Anforderungen an die Auftragsdatenverarbeitung !

BDSG

Vertragliche Inhalte nach §11 BDSG (Teil2)

- Die Berechtigung von Unterauftragsverhältnissen
- Die Kontrollrechte des AG und die entsprechenden Duldungs- und Mitwirkungspflichten des AN
- Mitzuteilende Verstöße des AN oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz pbDaten oder gegen die im Auftrag getroffenen Festlegungen
- Der Umfang der Weisungsbefugnis, die sich der AG gegenüber dem AN vorbehält
- Die Rückgabe überlassener Datenträger und die Löschung der beim AN gespeicherten Daten nach Beendigung des Auftrags



Erweiterte Anforderungen an die Auftragsdatenverarbeitung !

- ▀ Vertragliche Inhalte nach §11 BDSG (Hinweis)
- ▀ Der Auftrag kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.
- ▀ Der Auftraggeber hat sich **vor Beginn der Datenverarbeitung und sodann regelmäßig** von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
- ▀ **Das Ergebnis ist zu dokumentieren.**



Erweiterte Anforderungen an die Auftragsdatenverarbeitung !

BDSG

Bußgeld gemäß § 43 Abs. 1 Nr. 2b BDSG (Neu)

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig :

■ einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder

■ sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen überzeugt

Geldbuße bis zu 50.000 Euro; zusätzlich sog. „Gewinnabschöpfung“ möglich




Prüfen Sie ihren Geschäftsprozess.....

*ob in der Logistik oder in anderen Geschäftsvorgängen personen-
bezogene Daten verarbeitet werden.*

Prüfen Sie die Notwendigkeit zur Bestellung eines betrieblichen
Datenschutzbeauftragten.

Machen Sie den Datenschutz zum Qualitätsmerkmal in ihrem
Unternehmen, um Bußgelder und Imageverlust von ihrem Unternehmen
fernzuhalten.

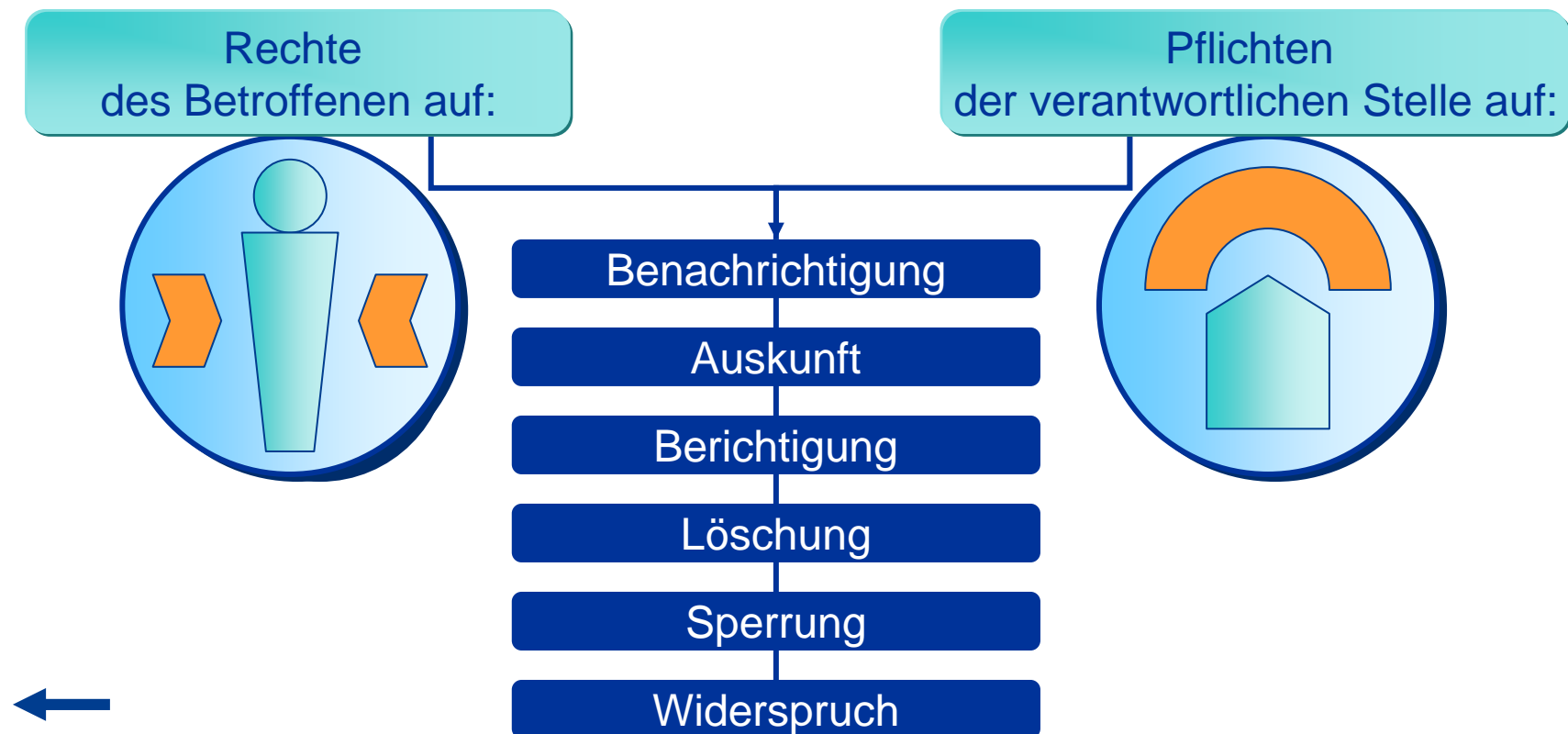




**Wir beraten und unterstützen
ihr Unternehmen gerne.....**

**Vielen Dank für Ihre
Aufmerksamkeit!**

Im BDSG werden dem Betroffenen unabdingbare Rechte gegeben, die damit zu Pflichten der verantwortlichen Stelle werden:



8 Gebote der Datensicherheit:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

