



Rheinischer Arbeitsrechtstag 2018 – Die Datenschutzgrundverordnung und das Arbeitsrecht

06. Juli 2018

Dr. Daniel Klösel
JUSTEM Rechtsanwälte
d.kloesel@justem.de

Inhalt

I. Einführung: Was ist neu?

II. Grundzüge einer GDPR-Compliance

1. Bestandsaufnahme
2. Wesentliche Bausteine
3. Insbesondere: „Paperwork“ (Einwilligung, BV, SLA etc.)

III. DSGVO und Arbeitsrecht

1. Datenschutz bei einzelnen HR-Prozessen
2. Datenschutz und Betriebsverfassung
3. Datenschutz im Konzern
4. Datenschutz bei Restrukturierungen und M&A-Transaktionen
5. Datenschutz bei Internal Investigations

IV. Ausblick: Kernthesen & Arbeiten 4.0

I. Was ist neu?

1. Neuer Rechtsrahmen

- **DSGVO** erlangte Geltung ab dem 25.05.2018 unmittelbar und verbindlich in allen 28 Mitgliedsstaaten der EU (Art. 99 Abs. 2 DSGVO)
 - Schaffung eines einheitlichen Rechtsrahmens
 - Aber: Art. 88 Abs. 1 DSGVO ermöglicht „spezifischere Vorschriften“ zum Beschäftigten-datenschutz („Öffnungsklausel“): **BDSG n.F.**

- Praktische Auswirkungen: Gleichlauf in multinationalen Unternehmensgruppen?
 - Grds.: Gleicher Rechtsrahmen in Deutschland und EU-Ausland
 - Aber:
 - Zusätzlich BDSG n.F. in Deutschland
 - Unterschiedliche nationale Entscheidungspraxis (Datenschutzbehörden, Gerichte etc.)

I. Was ist neu?

2. Neues Haftungsregime

- Altes Haftungsregime:
 - Bußgelder bis **EUR 50.000** und bis **EUR 300.000** (§ 43 Abs. 1 und 2 BDSG)
 - „Datenschutzskandale“ u.a. bei Daimler, Deutsche Bahn, Lidl, Telekom mit Bußen in Millionenhöhe bei massenhaften und intensiven Verstößen
 - Zuletzt: Adobe, Ponica, Unilever für Safe Harbor Verstöße mit Bußen von EUR 9.000
 - Schmerzensgeld von EUR 1.000 bei unzulässigem Detektiveinsatz (BAG vom 19.02.2015 – 8 AZR 1007/13)
- Neues (kartellrechtsähnliches) Haftungsregime:
 - Bis zu **EUR 20 Mio. oder 4 %** des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bei Unternehmen (Art. 83 DSGVO)
 - Ersatz materieller und immaterieller Schäden (Art. 82 DSGVO)
- Aber: Abmahnwelle (FAZ vom 21.06.2018: „Selbst Anwälte sind ratlos über die neuen Datenschutzregeln“)?

- I. Was ist neu?
- 3. Datenschutzrechtliches Grundkonzept

Verarbeitung personenbezogener Daten („pbd“)

- *Def.:* Jeder Vorgang bzgl. Informationen zu identifizierbarer natürlicher Person
- *Bsp.:* Erhalt bis Löschen von Bewerbungsunterlagen



<p>„Alt“: Rechtfertigungsgrundlage</p> <ul style="list-style-type: none"> • <u>1. Stufe:</u> Einwilligung, BV, gesetzliche Rechtfertigung • <u>2. Stufe:</u> Einwilligung, (kein) angemessenes Schutzniveau („Privacy Shield“ / EUMC, BCR) 	<p>„Neu“: Transparenz, d.h. Information zu</p> <ul style="list-style-type: none"> • Zweck • Kategorien von Daten etc. • Übermittlung an Drittstaaten? • Löschfristen • Sicherheitsmaßnahmen etc.
---	--

I. Was ist neu?

4. Voraussetzung („Alt & Neu“): Verarbeitung von pbD

- Verarbeitung... (Art. 4 Nr. 2 DSGVO)
 - Def.: „**Jeder Vorgang**“ im Zusammenhang mit pbD“
 - Bsp.: Erheben, Erfassen, Organisation, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Übermitteln, Abgleichen, Löschen, Vernichten
- ...personenbezogener Daten (Art. 4 Nr. 1 DSGVO)
 - Def.: **Alle Informationen**, die sich auf eine **zumindest identifizierbare** natürliche Person beziehen
 - Bsp.: Status- und Leistungsdaten von Arbeitnehmern, aber auch E-Mail, IP-Adressen, soweit hier regelmäßig auch eine personenbezogene Zuordnung möglich ist/wäre
- Sensitive Daten (Art. 9 DSGVO)
 - Def.: Rassistische/ethnische Herkunft, politische Meinungen, religiöse/weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, sexuelle Orientierung
 - Folge: Eingeschränktes Verbot, besonderer Rechtfertigungsbedarf

- I. Was ist neu?
- 5. Folge („Alt“): Rechtfertigungsbedarf (Drei Instrumente bleiben erhalten!)

1. Schritt	Grundlage	BDSG a.F.	DSGVO	BDSG n.F.
	Einwilligung	§§ 4, 4a	Art. 6 Abs. 1a, 7 ff.	§ 26 Abs. 2
	Betriebsvereinbarung	§ 4	Art. 88	§ 26 Abs. 4
	Erlaubnistatbestand	§§ 28, 32	Art. 6 Abs. 1	§ 26 Abs. 1
	<i>Auftragsdaten- verarbeitung</i>	§§ 9, 11	<i>Art. 28 DSGVO</i>	(§ 38)

2. Schritt „Outside EU“	Grundlage	BDSG a.F.	DSGVO	BDSG n.F.
	Einwilligung	§ 4c Abs. 1 Nr. 1	Art. 49 Abs. 1 a)	§ 26 Abs. 2
	Angemessenes Schutzniveau (Privacy Shield)	§ 4b	Art. 45	§ 78
	Kein angemessenes Schutzniveau (EUMC, BCR)	§ 4c	Art. 46 f.	§ 79

I. Was ist neu?

6. Folge („Neu“): Transparenzanforderungen

- Transparenz durch zahlreiche **parallele Bausteine** (Art. 12 ff. und 88 DSGVO):
 - „Institutionell“: Verarbeitungsverzeichnis, Betriebsvereinbarung, Datenschutzerklärung
 - Zudem in HR-Prozessen: Informationspflichten und individuelle Ansprüche, insbes. Auskunftsanspruch

- Inhaltliche Anforderungen – **Nahezu identische Kataloge** (bspw. Verarbeitungsverzeichnis):
 - Zwecke der Datenverarbeitung
 - Kategorien von Betroffenen, Daten und Datenempfängern
 - Übermittlung an Drittstaaten?
 - „wenn möglich“, Löschfristen
 - „wenn möglich“, Sicherheitsmaßnahmen

- I. Was ist neu?
- 7. **Transparenz am Beispiel eines ausgewählten HR-Prozesses**

Name	Elektronische Personalakte
Zweckdefinition	Effiziente Personaldatenverwaltung
Kategorien der erhobenen pbD	Statusdaten und Leistungsdaten (Name, Zeugnisse etc.)
Methode der Datenverarbeitung	Intern/Cloud
Ort der Datenverarbeitung	Inside/Outside EU/EWG, bei Outside Rechtsgrundlage!
Kategorien besonderer pbD	Keine/konkrete Benennung
Transfer pbD in der Unternehmensgruppe	Ja/Nein
Zugriffsberechtigungen	Zugriffskonzept, zumeist rollenbasiert
Speicherdauer/Löschkonzepte	Speicherdauer/Löschkonzept
Ggf. Maßnahmen zur Datensicherheit	Passwortgeschützt etc.

II. Grundzüge einer GDPR-Compliance

1. Bestandsaufnahme

a) Tatsächlich

- Ausgangspunkt: „altes“ Verzeichnisse, § 4d BDSG a.F.
- Regelmäßige Datenverarbeitungen im Beschäftigtenkontext (nicht nur elektronisch!)
 - **HRIS / HR-Managementsysteme** , d.h. (Elektronische) Personalakte & Co
 - **Arbeitsbegleitende EDV-Programme** (CRM, Office 365, IT-Security, Kommunikation)
- Weitere (einzelfallabhängige) Datenverarbeitungen
 - **Überwachung**, d.h. Tor-, Spind-, Videokontrollen
 - **Compliance / Internal Investigations**

b) Rechtsgrundlagen und Änderungsbedarf?

- Einwilligung
- Betriebsvereinbarung
- Allgemeiner gesetzlicher Erlaubnistatbestand
- Einbeziehung Dritter: ADV, SLAs & Co.
- Internationaler Datentransfer: EUMC, BCRs, Privacy Shield & Co.

II. Grundzüge einer GDPR-Compliance

2. Wesentliche Bausteine

- Institutionelle Bausteine
 - ggf. **Verarbeitungsverzeichnis** (Art. 30 DSGVO)
 - ggf. DPO (Art. 38 DSGVO, § 37 BDSG)
 - ggf. Datenschutzfolgeabschätzung (Art. 35 DSGVO)

- Rechtfertigungsgrundlagen
 - **Einwilligung** (Art. 7 DSGVO, § 26 Abs. 2 BDSG)
 - **Betriebsvereinbarung** (Art. 88 DSGVO, § 26 Abs. 4 BDSG)
 - SLAs / ADV
 - Drittstaatentransfer: EUMC, BCR & Co.

- Sonstiges: Interne Richtlinien zur Transparenz etc.

II. Grundzüge einer GDPR-Compliance

3. „Paperwork“ – Einwilligung, Art. 7 DSGVO, § 26 Abs. 2 BDSG n.F.

- Einwilligung bleibt **Erlaubnistatbestand** (vgl. BAG vom 19.02. 2015 – 8 AZR 1011/13; a.A. DSB)
- Schriftform**, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“ (§ 26 Abs. 2 S. 3 BDSG n.F., § 126 (a) BGB; Home-Office oder Online-Bewerbung?)
- Problem: Berücksichtigung der „im Beschäftigungsverhältnis bestehende[n] Abhängigkeit“ sowie der „Umstände, unter denen die Einwilligung erteilt worden ist“ (§ 26 Abs. 2 S. 1 BDSG n.F.)
 - Insbesondere möglich bei „*rechtlichem/wirtschaftlichem Vorteil*“ oder „*gleichgelagerten Interessen*“ (bspw. E-Mail Privatnutzung)
- Inhalt:
 - Praxishinweis: **Freiwilligkeit**
 - Einhaltung der **Transparenzanforderungen** (Art. 7 Abs. 2 DSGVO);
 - Zwecke, Datenkategorien, Datentransfer an Dritte, Betroffenenrechte etc.
 - **Hinweis auf Widerrufsrecht** in Textform (§ 26 Abs. 2 S. 4 BDSG n.F.).
 - Rückgriff auf andere Erlaubnistatbestände: „widersprüchliches Verhalten“?
- Praktisches Problem: jederzeitiger Widerruf möglich (Art. 7 Abs. 3 S. 1 DSGVO).

II. Grundzüge einer GDPR-Compliance

3. „Paperwork“ – Betriebsvereinbarung, Art. 88 DSGVO, § 26 Abs. 4 BDSG n.F.

- Doppelfunktion: **Erlaubnistatbestand** (h.L.) und **Transparenz**, § 77 Abs. 2 S. 3 BetrVG
- Art. 88 Abs. 1 DSGVO („spezifischere Regelungen“): Regelungsspielraum für Betriebsparteien?
 - Meinungsspektrum: **keinerlei Abweichung von Datenschutzstandards** auch nicht „nach oben“ zugunsten der Beschäftigten (*Maschmann*, DB 2016, 2480 ff.) bis zu möglichen Abweichungen auch „nach unten“ (*BeckOK/Riesenhuber*, DSGVO, Art. 88 Rn. 67 ff.)
 - Lösungsansatz, entwickelt aus Wortlaut und Sinn und Zweck von Art. 88 Abs. 1, 2 DSGVO und der insoweit eröffneten Interessenabwägung (*Klösel/Mahnhold*, NZA 2017, 1428):
 - gerichtlich nur eingeschränkt überprüfbarer **Ermessensspielraum für Betriebspartner**, z.B. auf erhebliche Widersprüche zu den Art. 5 ff. BDSG
- Art. 88 Abs. 2 DSGVO: **Notwendiger Inhalt** („angemessene Maßnahmen“)
 - Sachlich: Grundrechte der betroffenen Personen
 - Vor allem **„Transparenzkatalog“**, Art. 13 ff. DSGVO (Zweck, Datenkategorien, Empfänger etc.)
- **Praxis**: Kohärentes Konzept aus Rahmen-, Ergänzungs- und Einzel-BVs

II. Grundzüge einer GDPR-Compliance

3. „Paperwork“ – ADV, SLAs & Co., Art. 28 (26, 79, 82) DSGVO, § 38 BDSG n.F

- Privilegierungswirkung (str.), Art. 4 Nr. 10 DSGVO macht dies m.E. aber hinreichend klar
„Dritter ist eine natürliche oder juristische Person (...) außerhalb dem Verantwortlichen, dem Auftragsdatenverarbeiter (...)“
- **ADV vs. Funktionsübertragung** bleibt erhalten: Weisungsabhängigkeit / eigene Zwecke (Art. 28 Abs. 2 DSGVO)
 - In der Praxis: **„Global-HR-Systeme“** – SLAs und sonstige Intercompany-Agreements als privilegierte ADV?
- Anforderungen an ADV-Vertrag (auch Unteraufträge möglich, § 28 Abs. 2-9 DSGVO):
 - Verschärfte Vorgaben für Unteraufträge: Zustimmung/Widerspruch (Abs. 2 Alt. 1 und 2)
 - **Inhaltliche Anforderungen**: Dokumentierte Weisung, Vertraulichkeit, technische und organisatorische Schutzmaßnahmen etc. (Abs. 3 lit a-h)
 - Keine zwingendes Schriftformerfordernis, elektronische Form genügt (Abs. 8)

III. DSGVO und Arbeitsrecht

1. HR-Prozesse: Bewerbung/Recruiting

- Anknüpfungspunkt (pbD): Anschreiben, Statusdaten, Foto, CV, Leistungsnachweise etc.
- Beginn und Ende: Vom Eingang über die Erfassung und das Verschieben bis zur Löschung der Bewerberdaten
- Rechtlicher Rahmen: **Allgemeine Rechtfertigung** und **Transparenz**
- Relevante Einzelprozesse:
 - Einsatz von Personalberatern/-vermittlern
 - Backgroundchecks / Terrorlisten-Screening (BAG v. 16.12.2017 - 1 ABR 32/16)
 - Privacy Statement
 - Bearbeitung des Bewerbungsprozesses und Zugriff auf Bewerberdaten (bspw. CVs) bei HR, Vorgesetzten etc.
 - Löschung von Bewerberdaten
 - Recruiting Tools

III. DSGVO und Arbeitsrecht

1. HR-Prozesse: Laufendes Beschäftigungsverhältnis

- Anknüpfungspunkt (pbD): HR-Daten i.e.S. und sonstige pbD wie E-Mails, Browserverlauf etc.
- Allgemeiner rechtlicher Rahmen: **Betriebsvereinbarungen**, **Einwilligung**, **ggf. allgemeine Rechtfertigung** und **Transparenz**
- Relevante Einzelprozesse:
 - HR-Management (Elektronische Personalakte, HR-Training, Remuneration etc.)
 - Zugangskontrolle und Zeiterfassung
 - CRM-Systeme
 - IT-Tools
 - Gesundheits-/Fitness-Apps
 - Mitarbeiterbeurteilungen (BAG vom 13.12.2016 – 1 ABR 7/15, „Facebook“)
 - BYOD
- Vor allem **Auskunftsrecht**, Art. 15 DSGVO
 - Unverzüglich (= grds. 30 Tage) und in Textform
 - **Detailgrad** der Auskunft (Zwecke, Datenkategorien, Empfänger, Speicherdauer etc.)

III. DSGVO und Arbeitsrecht

1. HR-Prozesse: Beendigung des Beschäftigungsverhältnisses

- Anknüpfungspunkt (pbD): **Löschen** (= vgl. Art. 4 Nr. 1 DSGVO) aller zuvor verarbeiteten pbD
- Allgemeiner rechtlicher Rahmen: **Betriebsvereinbarungen**, **Einwilligung**, ggf. **allgemeine Rechtfertigung**
- Relevante Einzelprozesse:
 - Löschung von E-Mail-Accounts: Einwilligung über Löschen von privaten E-Mails und Festlegung von Standardprozessen (Beachte: § 667 BGB analog)
 - Löschfristen für pbD
 - Praktisches Probleme
 - Differenzierte Erforderlichkeit für Speicherdauer/Löschfristen für Daten aus Personalakte?
 - Abfindungsparameter bei ausgeschiedenen Mitarbeitern?

III. DSGVO und Arbeitsrecht

2. DSGVO und Betriebsverfassung

- (kein) Mitbestimmungsrecht aus § 75 Abs. 2 S. 1 und § 75 Abs. 1 BetrVG (BAG v. 28.05.2002 – 1 ABR 32/01)
- § 87 Abs. 1 Nr. 6 BetrVG: **technische Einrichtungen**, die dazu bestimmt sind, das **Verhalten und die Leistung der Arbeitnehmer zu überwachen**
- Kein ausdrücklicher Mitbestimmungstatbestand zum Datenschutz (BAG v. 19.12.2017 – 1 ABR 32/16)
 - Beschränkung der Mitbestimmung auf Verhaltens- und/oder Leistungskontrolle?
 - Mitbestimmung bzgl. Details der Datenverarbeitungen: Ort der Datenverarbeitung, (rollenbasierte) Zugriffskonzepte, Speicher-/Löschkonzepte, Beteiligung Externer etc.?
- Praxishinweise
 - Schwerpunkte: **Transparenzvorgaben**, Verhaltens- und Leistungskontrolle, Mitbestimmungsverfahren und Konfliktlösungsmodelle, detaillierte Datenschutzstandards
 - **„Abschichten“**: Rahmen-, Ergänzungs-, Muster-, Einzelbetriebsvereinbarungen
 - Erfahrungen aus Einigungsstellen: weiter Umfang der Mitbestimmung, in inhaltlicher Hinsicht aber weitestgehend Orientierung an Referenzrechtsprechung zu einzelnen Detailthemen

III. DSGVO und Arbeitsrecht

3. Datenschutz im Konzern

Konzerndatentransfer (bspw: einheitliches HR-Managementsystem)

- Allgemeine Rechtfertigung
 - Erneut kein ausdrückliches Konzernprivileg in der DSGVO
 - Aber „**Konzernprivileg light**“: Gem. *ErwGr 48* kann innerhalb einer Unternehmensgruppe berechtigtes Interesse zur Datenübermittlung zu Verwaltungszwecken bestehen
 - Konzernbezug des Arbeitsverhältnisses ausreichend?
- Betriebsvereinbarung** & Einwilligung: Kollektivvereinbarungen können Maßnahmen u.a. im Hinblick auf die Datenübermittlung in der Unternehmensgruppe treffen (vgl. Art. 88 Abs. 2 DSGVO)
- Transparenz

Matrix (bspw. Datentransfer zu fachlichem Matrixvorgesetztem)

- Allgemeine Rechtfertigung: „Matrixklausel“ im Arbeitsvertrag ausreichend?
- Betriebsvereinbarung, Einwilligung und Transparenz

Praxis: Konzernbezug, Betriebsvereinbarung, SLAs & (informierte) Einwilligung

III. DSGVO und Arbeitsrecht

4. Datenschutz bei Restrukturierung/Transaktion

- **Verarbeitung von pbD**: Anonymisierung, Re-Individualisierung und Führungskräfte
- Gesetzliche Rechtfertigung
 - Betriebsvereinbarung und Einwilligung? Allenfalls Einwilligung bei Führungskräften
 - **Allgemeine gesetzliche Rechtfertigung** nach Art. 6 Abs. 1 S. 1 lit. f. DSGVO (früher § 28 BDSG a.F. zentrale Vorschrift): Berechtigtes Interesse und Erforderlichkeit
 - Verschiedene Phasen bei M&A-Transaktionen: DD, Vertragsverhandlungen, Signing, Closing, Post -M&A-Integration
 - Unterschiede bei Share und Asset Deal
 - verschiedene Phasen der Restrukturierung: Information, Konsultation, Verhandlung, Einigungsstelle
 - Unterschiede bei Art der Betriebsänderung: Interessenausgleich/Sozialplan bei Personalabbau oder reiner Betriebsverlegung
- **Transparenz** und individuelle (Auskunfts-)Rechte der Arbeitnehmer

III. DSGVO und Arbeitsrecht

5. Datenschutz bei Internal Investigations

- Beispiele: Detektiv, Video, GPS, E-Mails und sonstige Dokumenten, Interviews, Drohnen etc.
- Hintergrund: **Beweis-/Sachvortragsverwertungsverbot**, Schmerzensgeld, Strafbarkeit
- **Wegfall des Gebots der Direkterhebung** (vgl. noch BAG vom 20.06.2013 - 2 AZR 546/12 – „Spindkontrolle“)
- Aber: **Verdeckte Ermittlungsmaßnahmen weiter zulässig?**
 - Problem: Transparenzvorschrift des Art. 14 DSGVO
 - Verbot als Verstoß gegen Gebot der Interessenabwägung im Einzelfall (*Byers*, NZA 2017, 1086)?
 - Art. 14 Abs. 5 lit. b/c DSGVO oder Art. 88 Abs. 1 DSGVO (*Franzen*, EuZA 2017, 313 und *Gola*, BB 2017, 1462)?
 - Nach BAG weiterhin grundsätzlich zulässig (z.B. BAG vom 22.09.2016, 2 AZR 848/15)
 - M.E.: Öffnungsklausel in Art. 14 Abs. 5 lit. c DSGVO durch § 26 BDSG genutzt, aber Compliance Betriebsvereinbarungen bzw. Klauseln als zusätzliche Lösung

III. DSGVO und Arbeitsrecht

5. Datenschutz bei Internal Investigations

- **DSGVO/BDSG vs. speziellere Vorschriften:** Arbeitgeber ist kein Dienstanbieter i.S.d. TKG, sodass E-Mail-Auswertung ausschließlich am Maßstab der DSGVO/BDSG zu bewerten ist (*noch immer str.*)
- Rechtlicher Rahmen (§ 26 Abs 1. Satz 1 und 2 BDSG)
 - Vgl. bereits § 32 Abs. 1 Satz 1 und 2 BDSG a.F.
 - (1) Zu dokumentierender („einfacher“) Verdacht einer Straftat (Satz 2)
 - Auch **Verdacht einer gravierenden Vertragspflichtverletzung** ausreichend (lange str., jetzt BAG vom 27.07.2017 – 2 AZR 681/16 – „Keylogger“)
 - Relevant v.a. bei Wettbewerbsverstößen (LAG BW vom 20.07.2016 - 4 Sa 61/15)
 - (2) Erforderlichkeit: **„Treppenmodell“**
 - Kenntnis von Überwachungsmöglichkeit wichtiger Abwägungsposten i.R.d. § 26 Abs. 1 BDSG n.F. (vgl. EGMR v. 05.09.2017 – 61496/08, *Barbulescu v. Romania*)
- Beteiligung des Betriebsrats
 - Gesetzliche Mitbestimmungsrechte: **Kein BVV** (BAG vom 03.12.2007 - 2 AZR 537/06)
 - Betriebsvereinbarung: ggf. Konsultationspflichten, Beweisverwertungsverbote etc.

III. DSGVO und Arbeitsrecht

5. Datenschutz bei Internal Investigations

- **Beispiel: Keylogger (BAG vom 27.07.2017 – 2 AZR 681/16)**
 - Keylogger = Hard- oder Software zur dauerhaften Protokollierung aller Tastatureingaben
 - Eingriffsintensität vergleichbar mit Videoüberwachung, damit (nur) in engen Grenzen zulässig
 - *Hier*: Unzulässig, weil weder § 32 Abs. 1 Satz 2 noch Satz 1 BDSG a.F. sowie bloßes Nicht-Widersprechen keine wirksame Einwilligung nach § 4a BDSG a.F.
 - Rspr. kann unter § 26 BDSG n.F. voraussichtlich fortgeschrieben werden

- **Beispiel: Videoüberwachung (BAG vom 22.09.2016 – 2 AZR 848/15 u.a.)**
 - § 32 BDSG a.F. als Konkretisierung von § 6b BDSG a.F.; bleibt in engen Grenzen möglich
 - Verwertung von Zufallsfunden kann in den Grenzen von § 32 Abs. 1 Satz 1 BDSG zulässig sein
 - Rspr. kann unter §§ 4, 26 BDSG n.F. voraussichtlich fortgeschrieben werden

- **Beispiel: Detektiv (BAG vom 19.02.2015 – 8 AZR 1007/13)**
 - § 32 BDSG auch bei Detektiveinsätzen und im Bereich der nicht elektronischen Datenverarbeitung anwendbar (vgl. § 32 Abs. 2 BDSG a.F.)
 - Hohe Anforderungen an Verdachtsschwelle (hohe Beweiskraft der AU-Bescheinigung)
 - Rspr. kann unter § 26 BDSG n.F. voraussichtlich fortgeschrieben werden

IV. Ausblick: Kernthesen & Arbeiten 4.0

- Datenschutz als ernstes Compliance-Thema („Kartellrechtsähnliche Strafen“)
- Aber: „Kirche im Dorf lassen“, **pragmatische Ansätze und praktikables Abschichten**
 - „Es gibt wohl kein Unternehmen, das hundertprozentig datenschutzkonform arbeitet.“ (Stefan Brink, Landesdatenschutzbeauftragter BW, FAZ vom 25.06.2018)
- Zentrale Aspekte: Transparenz der internen Datenflüsse und organisatorische Strukturen
- **Einbindung der Datenschutzbehörden**
 - Aus der *Praxis I* (Vorfeld): Beratungs- und Unterstützungstätigkeiten werden ernst genommen
 - „Die Aufsichtsbehörden **beraten und unterstützen** die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse.“ (vgl. § 40 BDSG n.F.)
 - Aus der *Praxis II* (Betriebsprüfung): Die (unterschiedliche) Behandlung von Kunden- vs. Beschäftigtendaten aus Sicht der zuständigen Datenschutzbehörden etc.
- Datenschutz in Unternehmenskultur verankern: **Einbindung der Betriebsräte** entscheidend
- **„Arbeiten 4.0“**: Digitalisierung und Entgrenzung der Arbeitsverhältnisse („globales Homeoffice“), Plattformökonomie, Crowdfunding, Scrum etc.

www.justem.de