Compliance und Datenschutz

Unter Berücksichtigung der beabsichtigten gesetzlichen Änderungen

Beschäftigtendatenschutz § 32 BDSG

- § 32 Abs. 1 Satz 1 BDSG erlaubt wie bisher § 28 Abs. 1 Satz 1 Nr. 1 BDSG den Umgang mit personenbezogenen Daten eines Beschäftigten, wenn dies für Zwecke des Beschäftigungs-verhältnisses erforderlich ist oder nach Satz 2 zum Zweck der Aufdeckung von Straftaten, wenn
  - zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat,
  - dies zur Aufdeckung erforderlich ist und
  - das schutzwürdige Interesse des Beschäftigten nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Gilt auch bei Erhebung, Verarbeitung oder Nutzung ohne automatisierte Verarbeitung

Geplante Änderungen § 32 ... BDSG-E

Vor Begründung eines Beschäftigungsverhältnisses

§ 32 Datenerhebung

§ 32a Ärztliche Untersuchungen und Eignungstests

§ 32b Datenverarbeitung und -nutzung

Im Beschäftigungsverhältnis

§ 32c Datenerhebung

§ 32d Datenverarbeitung und -nutzung

§ 32e Datenerhebung ohne Kenntnis des Beschäftigten zur Aufdeckung und Verhinderung von Straftaten u. anderen schwerwiegenden Pflichtverletzungen

§ 32f Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen

§ 32g Ortungssysteme

§ 32h Biometrische Verfahren

§ 32i Nutzung von Telekommunikationsdiensten

§ 32j Unterrichtungspflichten

§ 32k Änderungen

§ 32l Einwilligung, Geltung für Dritte, Rechte der Interessenvertretungen, Beschwerderecht, Unabdingbarkeit

Autom. Verarbeitung nicht erforderlich
§ 27 (3) S.2 BDSG-E

Überwachungs- und Aufsichtspflichten

Aktiengesetz und GmbH-Gesetz

- § 91 AktG (2): Der Vorstand hat geeignete Maßnahmen zu treffen, insbes. ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

- § 93 AktG Schadensersatzzahlungen bei Pflichtverletzung

- § 43 GmbHG: Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden

Überwachungs- und Aufsichtspflichten

Ordnungswidrigkeitengesetz

§ 130 OWiG (1): Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern ..., handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. ...

Aufsicht bedeutet zweckmäßige Betriebsorganisation (Aufgaben definieren, übertragen auf geeignetes Personal mittels verständlicher Anleitung und angemessener Kontrolle der Prozesse und des Personals)

Überwachungs- und Aufsichtspflichten

Gewerbeordnung

- § 106 GewO Weisungsrecht des Arbeitgebers

- Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb.
- Grenzen:
  - Arbeitsvertrag
  - Betriebsvereinbarung
  - Tarifvertrag
  - gesetzliche Vorschriften

Überwachungs- und Aufsichtspflichten

Beispiele für Straftaten in Unternehmen

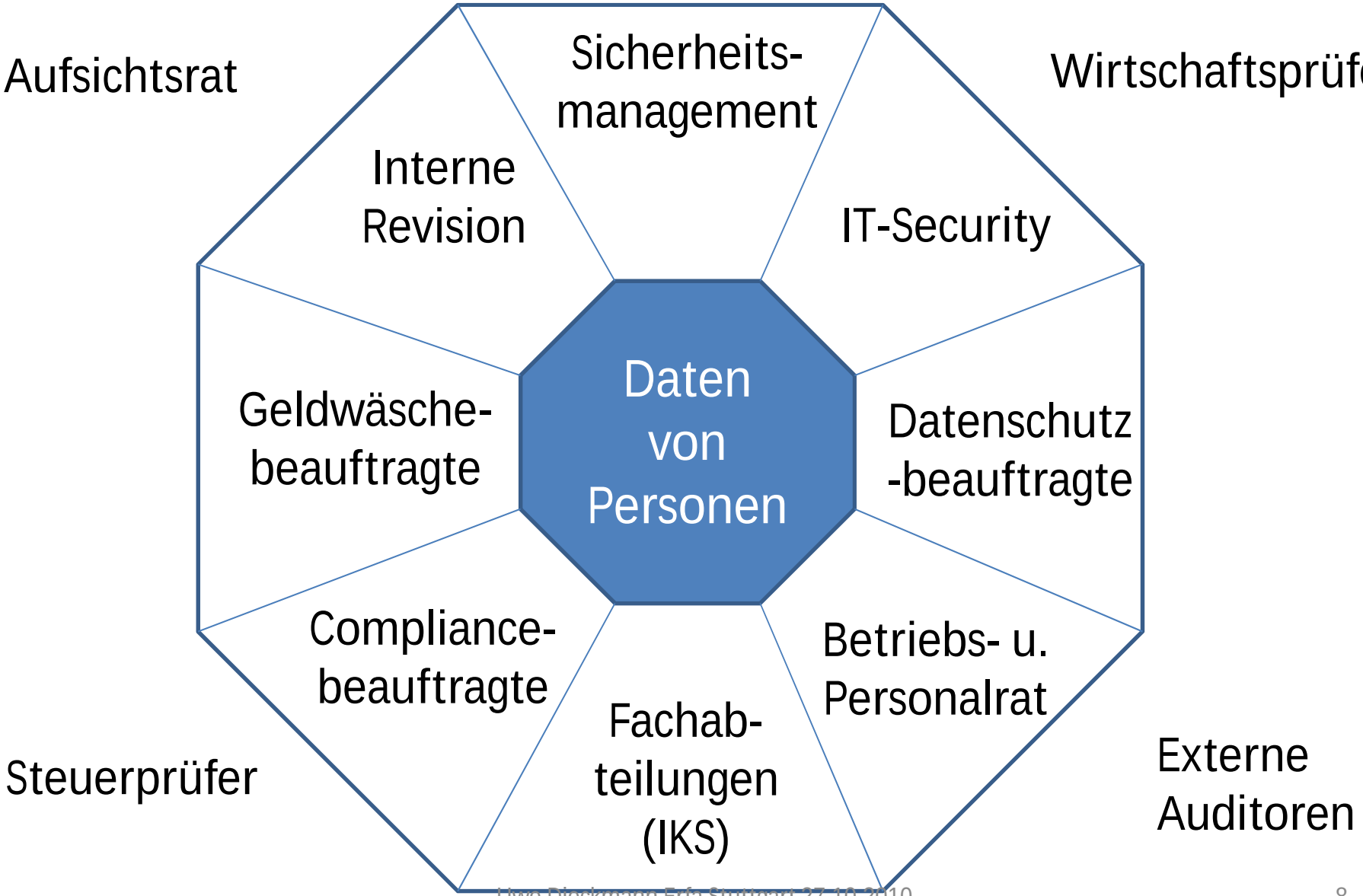
Hausfriedensbruch
Diebstahl und Unterschlagung
Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte
Betrug und Untreue, Urkundenfälschung
Verletzung der Buchführungspflicht
Bestechlichkeit und Bestechung im geschäftlichen Verkehr
Sachbeschädigung , Datenveränderung und Computersabotage
Herbeiführen einer Brandgefahr
Straftaten gegen die Umwelt

Weitere Straftaten (häufig mittels Intranet oder Internet):

Falsche Verdächtigung, Beleidigung
Straftaten gegen die sexuelle Selbstbestimmung
Verletzung des persönlichen Lebens- und Geheimbereichs
Nötigung , Bedrohung, Mobbing

Überwachungs- und Aufsichtspflichten

Organisation des Überwachungssystems



Überwachungs- und Aufsichtspflichten

Elemente des Internen Kontrollsystems

Präventive interne Kontrollen	Aufdeckende interne Kontrollen
Beispiele	Beispiele
Anweisungen 4-Augen-Prinzip Funktionstrennung Plausibilitäten (DV) Beschränkungen Zutritt Zugang Zugriff	Soll-Ist-Vergleiche ggf. 4-Augen-Prinzip Belegwesen Datenanalysen Protokollauswertung Kommt-Geht-Zeit An-/Abmeldung Zugriff auf Daten

Auch Zuverlässigkeitsüberprüfungen und die Abgabe von Verpflichtungserklärungen der Mitarbeiter stärken das IKS

Überwachungs- und Aufsichtspflichten

Datenschutz-Interessenkollision mit Compliancefunktionen

Trotz der gemeinsamen Compliance-Aufgabe wird eine Interessenkollision zum DSB vermutet bei folgenden Stellen

- Sicherheit, Revision
  - wegen Ermittlungen bei Straftaten und Pflichtverletzungen
- IT-Security
  - insbesondere bei Unterstellung unter die IT-Leitung
- Compliancebeauftragte in Kreditinstituten
  - wegen Nachforschungen bei Mitarbeitern im privaten Finanzbereich
- Geldwäschebeauftragte
  - wegen der Erforschung der Kundenumsätze anhand von Tools
  - DS-Aufsichtsbehörden sehen hier eine Interessenkollision

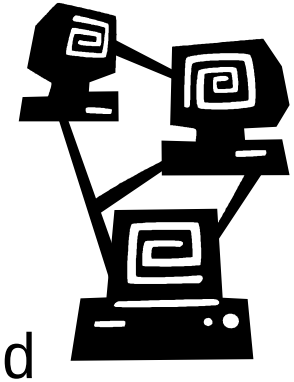
BVerfG-Urteile

- Informationelles Selbstbestimmungsrecht
  - Volkszählungsurteil BVerfG 15. Dezember 1983
- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
  - BVerfG 27. Februar 2008
- Datenabgleich
  - BVerfG 17. Februar 2009
- Vorratsdatenspeicherung
  - BVerfG 2.März 2010

BVerfG-Urteil

Datenabgleich 17. Februar 2009

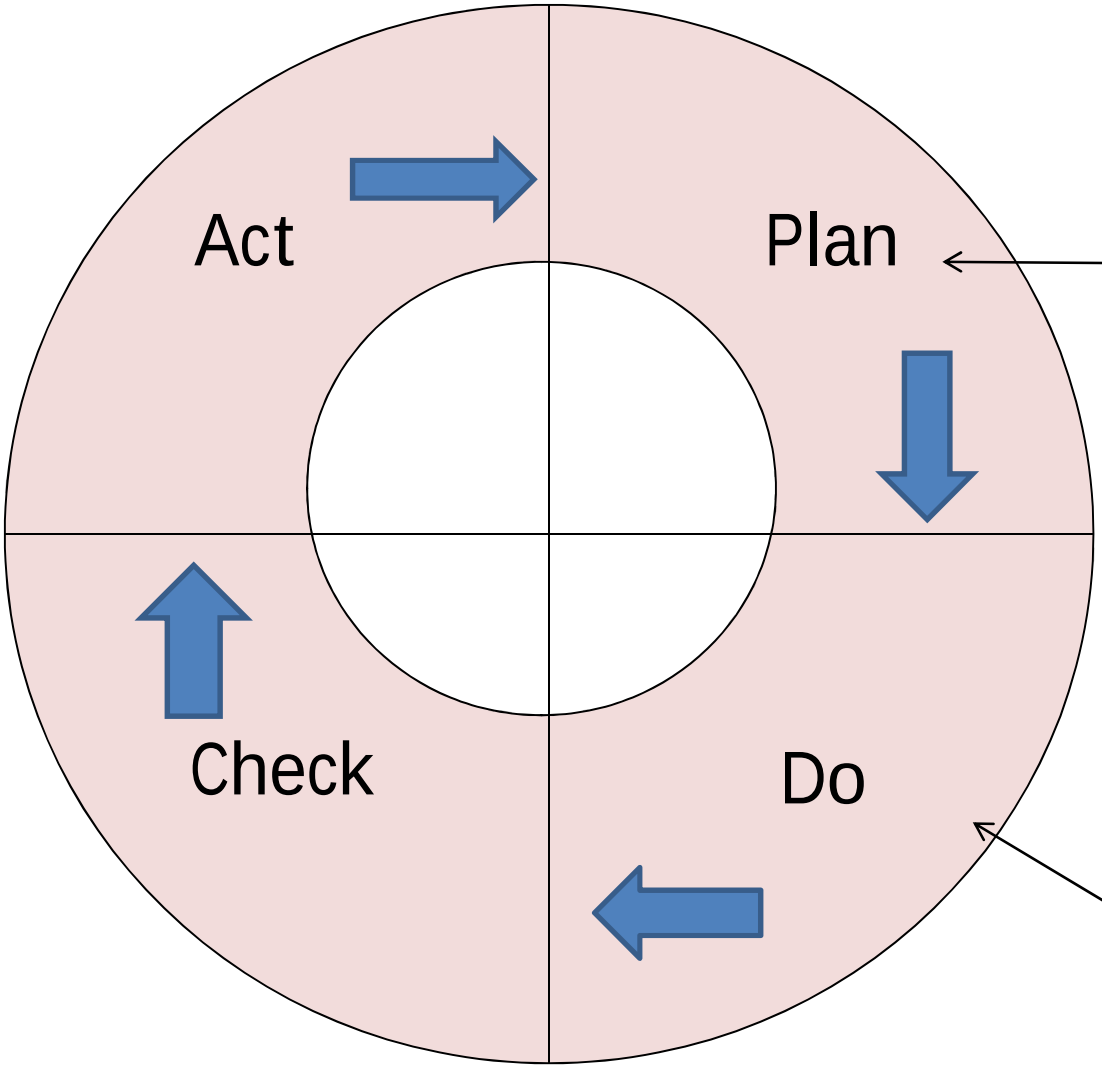
- Die maschinelle Einstellung der Kundendaten in einen Suchlauf, aus dem sie (mangels Treffer) anonym und spurenlos wieder ausscheiden, ist kein Eingriff in das informationelle Selbstbestimmungsrecht .



- Keine Rasterfahndung, da kein Abgleich zwischen den Datenbeständen verschiedener Speicherstellen stattfand
- Es wurde statt dessen gezielt nach Personen gesucht, die eine genau bezeichnete mit hinreichender Wahrscheinlichkeit strafbare Handlung vorgenommen haben.
- Die Datenerhebung war auf den Zweck der Tataufklärung begrenzt. Denn betroffen wurden dadurch regelmäßig nur Personen, die durch ihr Verhalten den hinreichenden Verdacht einer Straftat begründet hatten.

Sicherheitsmanagement

Ziele und Aufgaben



Sicherheitskonzept
- Schutzziele,
- Gefahrenanalyse
- potentieller Schaden
- Maßnahmenplanung
- Notfallplanung

Verletzung der betrieblichen Ordnung und internen und externen Normen durch Beschäftigte und externe Personen

Sicherheitsmanagement

Verhinderung von Verstößen

Zutrittskontrollen
Objektsicherung und Ortungssysteme
Beobachtung ggf. mit Kameraeinsatz
Biometrische Verfahren
Möglichkeit weitergehender Personenkontrollen

Sicherheitsmanagement

Zutrittskontrollen

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)

Gleiche Zielrichtung wie Sicherheitsmanagement

I.d.R. keine Probleme auch im Hinblick auf die Neuregelung des Beschäftigtendatenschutzes. Die Zutrittskontrolle ist ja auch aus Datenschutzgründen erforderlich. Auch offene Videobeobachtung ist möglich nach § 32f (1) Nr.1 BDSG-E.

Ist es erforderlich zu wissen, wo an welchem Ausweisleser jemand das Firmengelände betreten hat?

Sicherheitsmanagement

Objektsicherung und Ortungssysteme

Ortungssysteme sind Systeme, mit deren Hilfe der geographische Standort eines Beschäftigten bestimmt werden kann, z. B. GPS.

Nach § 32g BDSG-E nur zulässig, wenn schutzwürdige Interessen nicht überwiegen und es erforderlich ist aus betrieblichen Gründen

- zur Sicherheit des Beschäftigten oder
- zur Koordinierung seines Einsatzes.

Erlaubt nur während der Arbeits- oder Bereitschaftszeiten, d.h. nicht während der Freizeit oder im Urlaub.

Eine heimliche Ortung von Beschäftigten ist nicht zulässig. Einsatz und Nutzung eines Ortungssystems ist transparent zu gestalten. Strenge Zweckbindung!

Sicherheitsmanagement

Objektsicherung durch Ortungssysteme

§ 32g (2) BDSG-E:
Zulässig ist der Schutz der Arbeitsmittel und sonstiger beweglicher Sachen in der Obhut des Beschäftigten z. B. der Fracht

Keine Ortung zulässig während der ordnungsgemäßen Nutzung oder des ordnungsgemäßen Besitzes der Sache.

Typischer Anwendungsfall:
Diebstahlsschutz von Baumaschinen oder LKW.

Sicherheitsmanagement

Optisch-elektronische Einrichtungen

Videoüberwachung

§32f (1) BDSG-E:
Offene Beobachtung von Betriebsstätten nur zulässig,

1. zur Zutrittskontrolle,
2. zur Wahrnehmung des Hausrechts,
3. zum Schutz des Eigentums,
4. zur Sicherheit des Beschäftigten,
5. zur Sicherung von Anlagen oder
6. zur Abwehr von Gefahren für die Sicherheit des Betriebes
7. zur Qualitätskontrolle,

- soweit erforderlich wegen wichtiger betrieblicher Interessen und
- nach Art/Dauer keine überwiegenden schutzwürdige Interessen

Nicht zulässige Videobeoachtung

§ 32f (2) BDSG-E:
Zur Verfügung gestellte private Rückzugsräume, insbesondere Sanitär-, Umkleide- und Schlafräume.
Von vielen Beschäftigten genutztes Raucherzimmer ist kein individueller Rückzugsraum

Heimliche Videobeobachtung ist selbst dann, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre, nicht mehr möglich.

Die Beobachtung von Räumen und Gegenständen ist nur zulässig, wenn kein Personenbezug zu Beschäftigten hergestellt werden kann.

(Elektronische) Biometrische Verfahren

§ 32 h BDSG-E:

Erhebung, Verarbeitung, Nutzung biometrischer Merkmale zu Autorisierungs- und Authentifikationszwecken ist zulässig

Fingerabdruck (Fingerlinienbild),
Handgeometrie,
Iris (Regenbogenhaut des Auges),
Retina (Netzhaut),
Gesichtsgeometrie,
Stimmmerkmale

Zweckänderung erhobener Biometriedaten nur bei **Lichtbildern** und nur mit Einwilligung des Beschäftigten

Sicherheitsmanagement

Möglichkeit weitergehender Personenkontrollen

Taschenkontrollen und **Torkontrollen** stellen eine **Erhebung von Beschäftigtendaten** dar

Die Daten werden **mit Kenntnis** der Beschäftigten erhoben.

Präventionskontrollen

z. B. Stichproben bei Mitarbeitern des Rechenzentrums

Anlasskontrollen

z.B. bekanntgewordene Diebstähle in bestimmten Unternehmenseinheiten

Neben präventiven Zutritts-, Zugangs-, und Zugriffskontrollen ist die **Weitergabekontrolle** geeignet zur **Verhinderung der unbefugten Entfernung** von z. B. Notebooks und Datenträgern aller Art.

Interne Revision

Kernaufgaben sind risikoorientierte Prüfungen aller Prozesse und Aktivitäten – auch der ausgelagerten – im Hinblick auf die

- Wirksamkeit des Internen Kontrollsystems (IKS),
- Wirtschaftlichkeit *(Nutzung des Wettbewerbs, Beschaffungskosten)*
- Ordnungsmäßigkeit und Einhaltung der Normen
- (IT-)Sicherheit incl. Schutz vor Vermögensverlusten

(Korruptionsprävention)

Beschaffungsprozess

Planung/Bedarfsmeldung
Angebotseinholung + Angebotsbearbeitung
Lieferantenauswahl
Auftragserteilung/Vertragsmanagement
Auftragserledigung
Leistungsanerkennung
Rechnungsprüfung/-freigabe

Personenbezüge

Mitarbeiter der Auftraggeber und Lieferanten

Prüfung der Ordnungsmäßigkeit von Geschäftsvorfällen

- Die Prüfung von Geschäftsvorfällen ist grundsätzlich datenschutzrechtlich nicht zu beanstanden, wenn Prüfungsziel die Richtigkeit von Buchungen und /oder Zahlungen ist. Zahlungsströme haben regelmäßig eine Vertragsgrundlage mit den betroffenen Beschäftigten, Lieferanten oder Kunden, die die Voraussetzungen an die Zulässigkeit der Prüfung gemäß § 32 Abs. 1 Nr. 1 oder § 28 Abs. 1 Satz 1 BDSG erfüllt.
- Im Rahmen der vertraglichen Grundlage über die Höhe von Zahlungen ist auch die Überprüfung, ob an eine Person zu viel oder zu wenig gezahlt wurde, zulässig. Denkbar sind programmierte Abfragen über sämtliche Haupt- und Nebenbuchhaltungssysteme mit dem Ziel, die tatsächliche Höhe der Zahlungen an einen Betroffenen mit dem Soll zu vergleichen.

Interne Revision

Prüfung der Ordnungsmäßigkeit von Geschäftsvorfällen

- Alle ausgehenden und selbstverständlich eingehenden geschäftlichen Briefe können uneingeschränkt durch die Revision überprüft werden. Dazu zählen auch die Inhalte alle geschäftlichen Mails, die im Zusammenhang mit den gebuchten oder zu buchenden Geschäftsvorfällen oder Verträgen stehen.
- Erfolgen solche Überprüfungen ohne Kenntnis der Beschäftigten, ist in Zukunft aufgrund der geplanten Änderung des Beschäftigtendatenschutzes dies nur im Falle der Aufdeckung oder Verhinderung von Straftaten oder schwerwiegender Pflichtverletzungen möglich.

Interne Revision

Mögliche Hintergründe zu Lieferantenbeziehungen

Personenbezogene Indikatoren lt. Broschüre LKA NRW

- Private Beziehungen,
- Gemeinsame Vereinszugehörigkeit
- kostenlose Überlassung von Fahrzeugen, Geräten oder Urlaubsdomizilen
- mit dem Einkommen nicht erklärbarer Lebensstil
- persönliche Schwächen wie z.B. Spielsucht
- „Unabkömmlichkeit“ (Verzicht auf Urlaub, Anwesenheit bei Krankheit)
- Absonderung, Verschlossenheit des Mitarbeiters/der Mitarbeiter
- auffällige Mitnahme von Vorgängen nach Hause
- hochwertige „Werbegeschenke“ oder Spendentätigkeit des Auftragnehmers
- plötzlicher Meinungswandel in Bezug auf getroffene Entscheidungen
- plötzliches Interesse für andere Ressorts ohne eigene Zuständigkeit
- Sponsoring (für die Kaffeekasse oder Betriebsausflugskasse)
- Häufige Einladungen (Weinproben, Jagdausflüge, Golfturniere, Segeltörns)
- organisationsinterne Gerüchte

Aufdeckungsprüfungen ohne konkreten Anfangsverdacht 1

- Konventionelle Prüfvorgehensweise
  - Stichproben einer bestimmten Periode mittels (un-)bewusster Auswahl aus unbekannter Grundgesamtheit oder aus Teilen davon
  - Daten: Geschäftsvorfälle, Buchungen, Rechnungen, Verträge, Belege
  - Ggf. statistische Hochrechnung der Stichprobenergebnisse auf die Grundgesamtheit
- Massendatenunterstützte Prüfvorgehensweise
  - Abfragen über Vorgänge, die unplausibel sind oder auf Regelverstöße hindeuten, über den gesamten Datenbestand des zu überprüfenden Bereichs
  - Auch regelkonforme Einzelvorgänge können im Kontext mit anderen Einzelvorgängen unerwünscht sein (z. B. Betragsstückelungen).

Interne Revision

Aufdeckungsprüfungen ohne konkreten Anfangsverdacht 2

- Beispiel:
- Auszug aus ISA 240:
  - IT-gestützter Abgleich der Liste der Verkäufer mit einer Liste der Mitarbeiter zur Identifikation von Übereinstimmungen von Adressen und Telefonnummern
  - IT-gestützte Durchsuchungen der Aufzeichnungen für die Lohnbuchhaltung zur Identifikation doppelter Adressen, Personal- oder Steuernummern sowie Bankkonten

In Zukunft nach § 32d (3) BDSG-Entwurf wohl nur noch anonymisiert bzw. pseudonymisiert möglich

Aufdeckungsprüfungen ohne konkreten Anfangsverdacht 3

Dokumentation analog § 4 e BDSG
(ggf. im Prüfungsauftrag) vor Beginn der Datenanalyse über

- Zielsetzung der Datenanalyse
- Art und Ausmaß des vermuteten Risikos, gegen das die Analyse eingesetzt werden soll
- Datenschutzrechtliche Zulässigkeit des Prüfungsauftrags an sich

§ 4 e BDSG
verlangt Angaben zu Verfahren, u. a. über den Zweck, betroffene Personengruppen, Datenkategorien, Datenherkunft, Empfänger, Löschungsfristen, Datensicherheit

Dem Datenschutzbeauftragten sind die Verfahren nachzuweisen.

Aufdeckungsprüfungen ohne konkreten Anfangsverdacht 4

Fragen der Erforderlichkeit

- Einzubeziehende Datenfelder
  - Sind Datenfelder, die eine Identifizierung von Personen ermöglichen, nach dem Prüfungsziel überhaupt erforderlich?
- Einzubeziehende Datensätze
  - Müssen alle Datensätze der zu untersuchenden Datengesamtheit untersucht werden oder können Datensätze, die bestimmte Personen betreffen, herausgefiltert werden?
- Anonymisierung oder Pseudonymisierung notwendig?
  - Aus welchem Grund?
  - Wer nimmt diese vor?

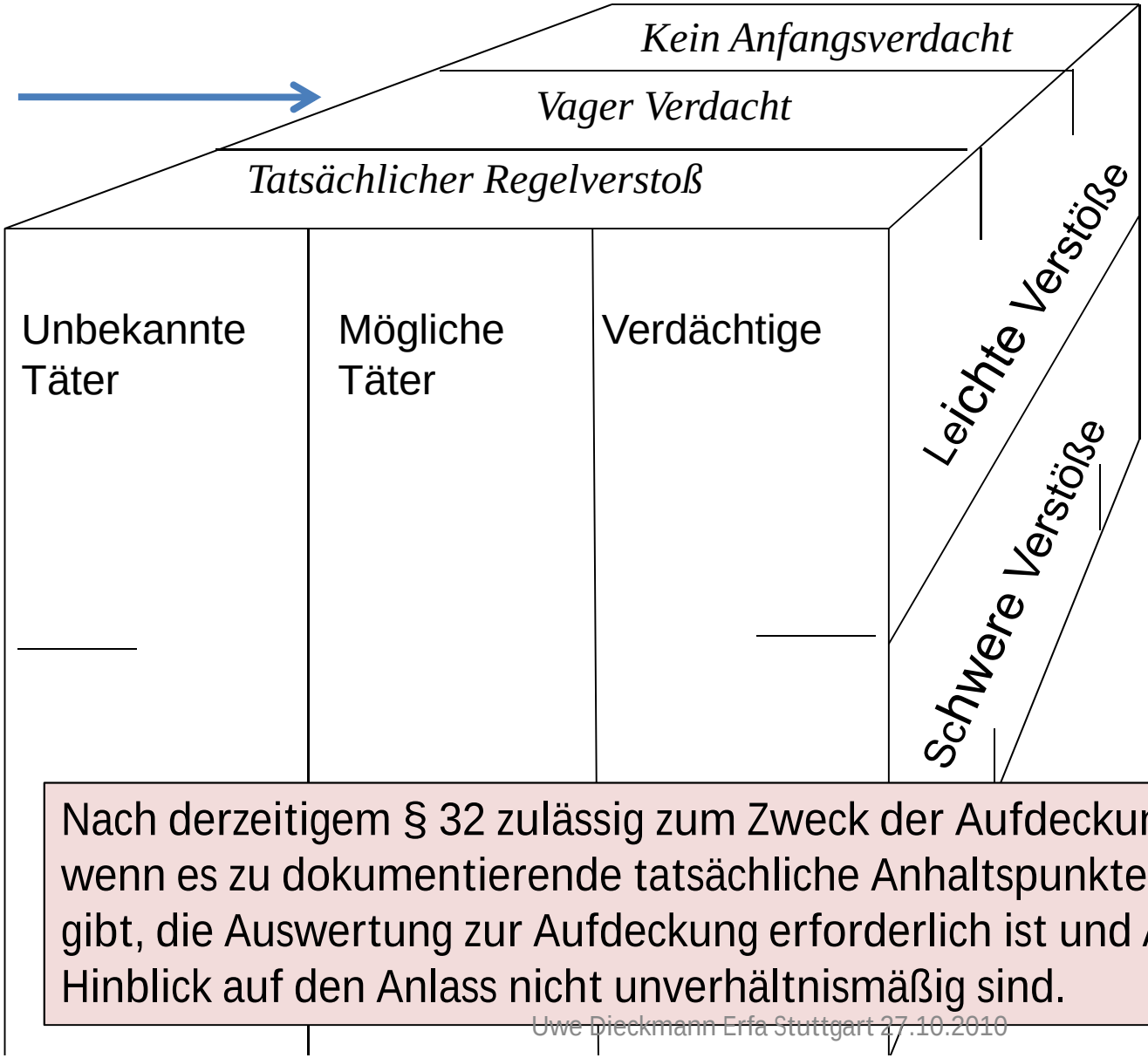
Aufdeckungsprüfungen ohne konkreten Anfangsverdacht 5

Fragen der Zweckbindung

- Sind die heranzuziehenden Datenfelder betroffener Personen zu einem Zweck erhoben und gespeichert, der mit dem Prüfungsziel vereinbar ist ?
- Beispiele:
  - Religionszugehörigkeit ist nur für den Zweck der Kirchensteuerabführung erhoben und gespeichert
  - Namen / Anschrift zu benachrichtigender Ehepartner oder anderer Personen sind nur für den Notfall erhoben
  - Bankverbindung eines Mitarbeiters nur für Zweck der Gehaltszahlung erhoben und gespeichert

Internen Revision

Ermittlungshandlungen bei Anfangsverdacht auf Unregelmäßigkeiten



Pflichtverletzungen

Ordnungswidrigkeiten

Straftaten

- Versuche
- Auf Antrag
- Vergehen
- Verbrechen

Nach derzeitigem § 32 zulässig zum Zweck der Aufdeckung von Straftaten, wenn es zu dokumentierende tatsächliche Anhaltspunkte für eine Straftat gibt, die Auswertung zur Aufdeckung erforderlich ist und Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Interne Revision

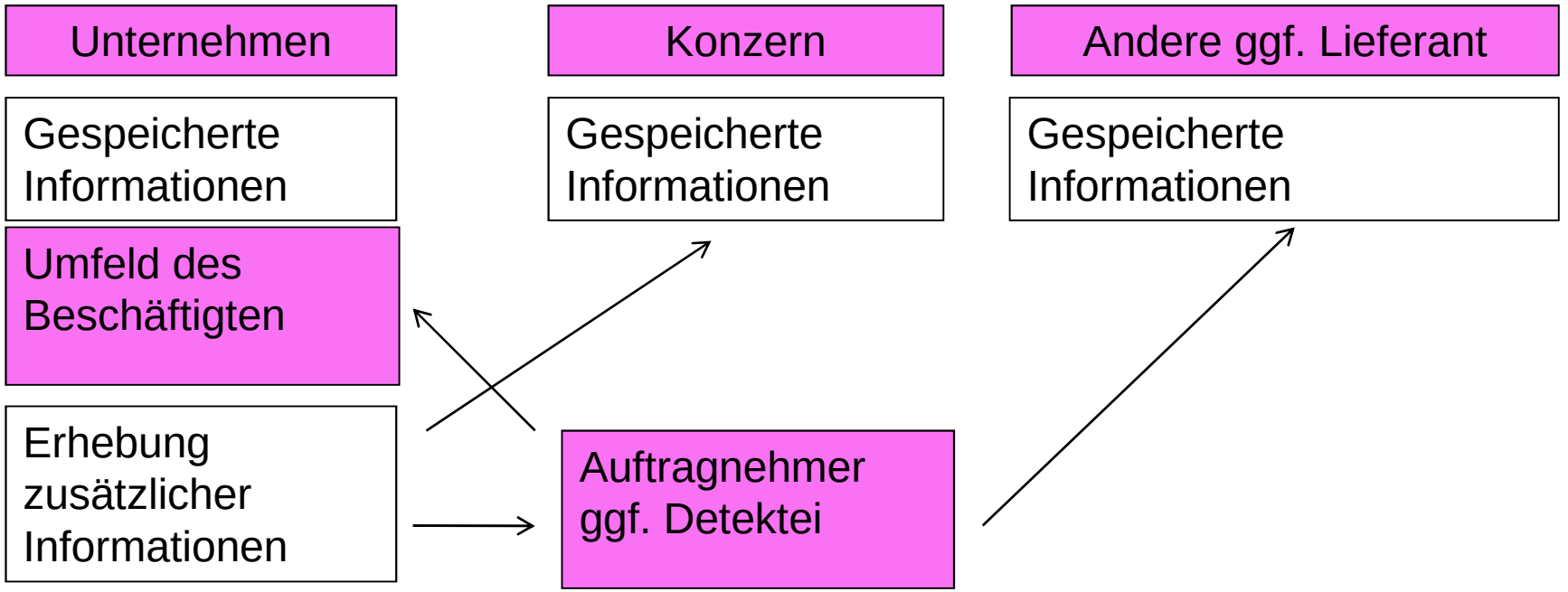
Ermittlungshandlungen bei Anfangsverdacht auf Unregelmäßigkeiten 2

Suche nach Informationen (was und wo?)

Stammdaten
- Beschäftigter
- Angehörige
- Gehalt
- Bankverbindung

Inhaltsdaten
Mail
Briefe
Dateien

Protokolldaten
Telefonverkehrsdaten
E-Mail-Verkehrsdaten
Aufgerufene Internetseiten
Ab-, Anwesenheitszeiten
System-An- und Abmeldung



Beschäftigtendatenschutz Entwurf

Geplante Erweiterungen des § 32 BDSG (hier § 32d)

§ 32d (3) BDSG-E:

- Automatisierter **anonymisierter oder pseudonymisierter** Abgleich von Daten der Beschäftigten ist zulässig zur Aufdeckung von Straftaten oder **anderen schwerwiegenden Pflichtverletzungen**
- Im Verdachtsfall dürfen die Daten personalisiert werden.
- Unterrichtungspflicht des Arbeitgebers

§ 32d (5) BDSG-E:

Zusammenführung einzelner Lebens- und Personaldaten zu einem Gesamtbild wesentlicher geistiger und charakterlicher Eigenschaften oder des Gesundheitszustandes des Beschäftigten **ist unzulässig**.

Beschäftigtendatenschutz Entwurf

Geplante Erweiterungen des § 32 BDSG (hier § 32e BDSG-E)

(2) Erhebung ohne Kenntnis des Beschäftigten ist nur zulässig, wenn Tatsachen den Verdacht einer Straftat oder einer anderen schwerwiegenden Pflichtverletzung begründen, die zu einer Kündigung aus wichtigem Grund berechtigen würde, und die Erhebung zur Aufdeckung oder Verhinderung weiterer Straftaten oder schwerwiegender Pflichtverletzungen erforderlich ist.

(3) Erhebung ist zeitlich auf das unumgängliche Maß zu beschränken.

(4) Beobachtung länger als 24 Stunden ohne Unterbrechung oder an mehr als 4 Tagen ebenso wie Ton- oder Videoaufnahmen unzulässig

(5) Vorabkontrolle des DSB
und Unterrichtungspflicht des Arbeitgebers

Beschäftigtendatenschutz Entwurf

Kontrollen der Telekommunikation

Die Gliederung des § 32h BDSG-E:

Abs. 1-3 Der andauernde Telekommunikationsvorgang

Abs. 1 Regelung zu Telekommunikationsdiensten allgemein

Abs. 2 Regelung zu Telefoniediensten

Abs. 3 Regelung zu anderen Telekommunikationsdiensten

Abs. 4 Der abgeschlossene Telekommunikationsvorgang

Beschäftigtendatenschutz Entwurf

Kontrollen der Telekommunikation (2)

§ 32i (1) Bei nur beruflich erlaubter Nutzung dürfen die Daten nur erhoben und verwendet werden, soweit dies erforderlich ist,

1. zur Gewährleistung des ordnungsgemäßen Betriebs einschließlich der Datensicherheit,
2 . zu Abrechnungszwecken oder
3. zu einer stichprobenartigen oder anlassbezogenen Leistungs- oder Verhaltenskontrolle

und keine schutzwürdige Interessen des Beschäftigten überwiegen.

Schutzwürdigen Interessen können sein z.B.

- unternehmensinterne psychologische Beratungen
- Kommunikation mit dem Betriebsrat
- Kommunikation mit erkennbar privaten Inhalten

Beschäftigtendatenschutz Entwurf

Kontrollen der Telekommunikation (3)

Aus der Begründung des § 32h (1) BDSG-E:

„Die Überprüfung der den Verkehrsdaten entsprechenden Daten kann auch ein taugliches Mittel für den Arbeitgeber sein, um Vertragsverletzungen zu seinen Lasten, Ordnungswidrigkeiten oder Straftaten zu verhindern oder aufzuklären.“

Bei Herstellung eines Personenbezugs ist der Beschäftigte über die Verarbeitung / Nutzung zu unterrichten, sobald der Zweck durch die Benachrichtigung nicht mehr gefährdet wird.

Beschäftigtendatenschutz Entwurf

Kontrollen der Telekommunikation – Telefondienste

§ 32h (2) BDSG-E Telefondienste:

Dienste für das Führen von Inlands- und Auslandsgesprächen einschließlich Sprachkommunikation (VoIP).

Inhalte einer beruflich erlaubten Nutzung von Telefondiensten dürfen nur bei berechtigtem Interesse des Arbeitgebers und nur mit der im Einzelfall vorher erteilten Einwilligung des Beschäftigten als auch seines Kommunikationspartners erfolgen.

Eine Einwilligung des Kommunikationspartners liegt vor, wenn er nach der Unterrichtung das Telefonat fortsetzt. Ein heimliches Mithören von Telefonaten ist dem Arbeitgeber damit untersagt.

Sonderregelung für Callcenter für Zwecke der Leistungskontrolle

Beschäftigtendatenschutz Entwurf

Kontrollen der Telekommunikation – E-Mail § 32i (3)

Inhalte anderer Telekommunikationsdienste (z.B. E-Mail) dürfen erhoben und verwendet werden, soweit erforderlich zur

- Durchführung des Beschäftigungsverhältnisses
- Gewährleistung der Ordnungsmäßigkeit (Betrieb, Datensicherheit)
- Abrechnung oder
- stichprobenartigen/anlassbezogenen Leistungs-/Verhaltenskontrolle

und keine schutzwürdigen Interesse des Beschäftigten überwiegen.

Dies gilt auch, soweit es für den ordnungsgemäßen Dienst- oder Geschäftsbetrieb des Arbeitgebers in den Fällen einer Versetzung, Abordnung oder Abwesenheit erforderlich ist. Ohne Kenntnis des Beschäftigten darf eine Erhebung nach Satz 1 in Verbindung mit der Leistungs- / Verhaltenskontrolle nur gemäß § 32e (2-7) erfolgen.

Beschäftigtendatenschutz Entwurf

Kontrollen nach Abschluss der Telekommunikation § 32i (4)

Nach Abschluss einer Telekommunikation gelten für die Erhebung, Verarbeitung und Nutzung der Daten und Inhalte die §§ 32c u. 32d.

Die Erhebung muss erforderlich sein für die Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses (z. B. bei Abwesenheitsvertretung), sofern es sich nicht um erkennbar private Inhalte handelt.

Die Verwendung privater Inhalte und Daten der abgeschlossenen Kommunikation eines Beschäftigten ist nur zulässig, wenn dies zur Durchführung des ordnungsgemäßen Geschäftsbetriebes unerlässlich ist (z.B. Weiterbearbeitung bei Krankheit).

Schriftlicher Hinweis an den Beschäftigten notwendig.

Beschäftigtendatenschutz Entwurf

Fazit

- Zulässigkeit der Verarbeitung von Arbeitnehmerdaten wird präzisiert
- Kontrolle des Einsatzes der IuK-Technik (Telefon, Internet, E-Mail) weitgehend unverändert
- Grundsatz der Direkterhebung beim Beschäftigten
- Einschränkung der verdeckten Datenerhebung.
- Datenerhebung bei Dritten, z.B. durch Befragung, nur unter strengen Voraussetzungen
- Generelles Verbot der heimlichen Videoüberwachung und Ortung
- Betriebsvereinbarungen könnten unwirksam werden.
- Wegen Konzernproblematik eingeschränkter Handlungsspielraum bei Konzernsicherheit und Konzernrevision

Ende der Präsentation

Vielen Dank

Noch Fragen ?