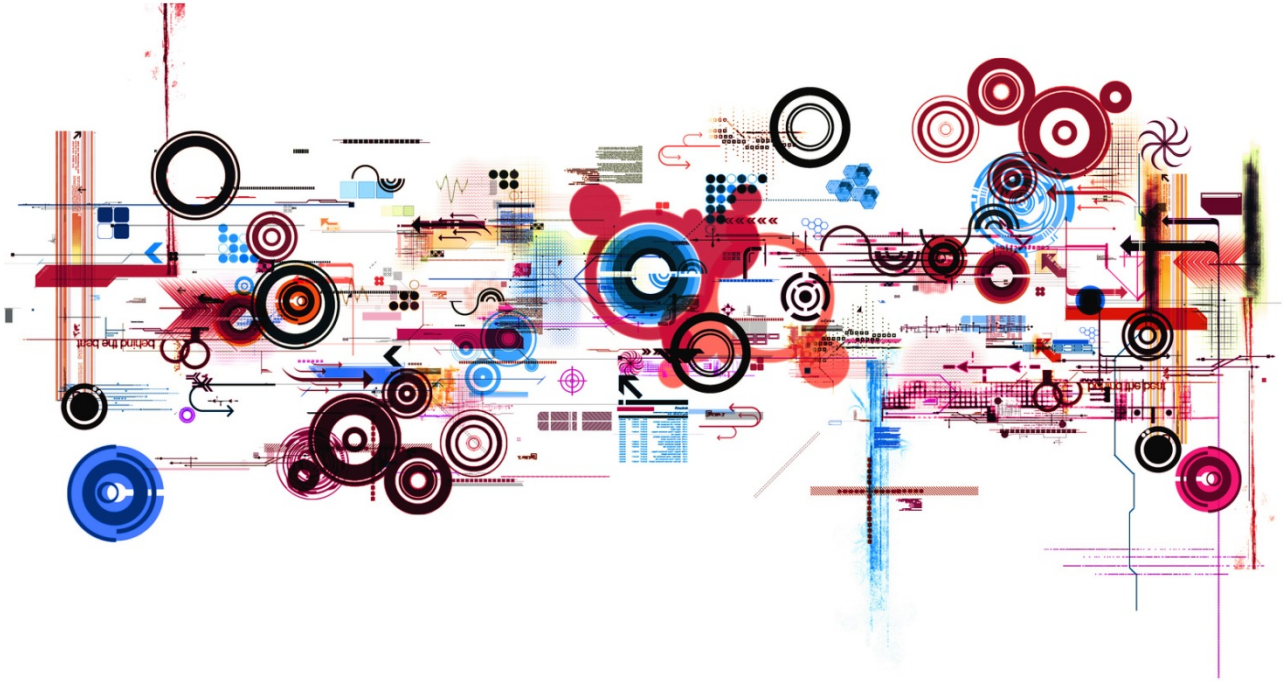
# Praxisreport der bayerischen Datenschutzaufsichtsbehörde

## Aktuelle Themen aus der Sicht der Datenschutzaufsicht



**Thomas Kranig**

Präsident des Bayer. Landesamtes für Datenschutzaufsicht

# Gliederung



1. Datenschutzaufsichts- und -kontrollbehörden
2. Themen des Düsseldorfer Kreises
   a. Videoüberwachung
   b. E-Mail und Internetnutzung am Arbeitsplatz
   c. Anonymisierung, Pseudonymisierung, Big Data
   d. Facebook - Zuständigkeit
   e. Internationaler Datenverkehr, Safe Harbour und NSA
3. Prüfpraxis des BayLDA
4. Diskussion um Datenschutz-Grundverordnung

# Gliederung



1. **Datenschutzaufsichts- und -kontrollbehörden**
2. Themen des Düsseldorfer Kreises
   a. Videoüberwachung
   b. E-Mail und Internetnutzung am Arbeitsplatz
   c. Anonymisierung, Pseudonymisierung, Big Data
   d. Facebook - Zuständigkeit
   e. Internationaler Datenverkehr, Safe Harbour und NSA
3. Prüfpraxis des BayLDA
4. Diskussion um Datenschutz-Grundverordnung

# 1. Datenschutzaufsichts- und -kontrollbehörden



LfD BW

LfD BY | BayLDA

Berliner BDI

LDA BDB

LfDI Bremen

BfDI HH

BD Hessen

LfD Meck-Pom.

Bundesbeauftragter für Datenschutz und Informationsfreiheit

**Datenschutz – Recht auf informationelle Selbstbestimmung**

ö-r- Rundfunk

priv. Rundfunk

kath. Kirche

ev. Kirche

LfD NDS

LfDI NRW

LfD Rh-Pf

LfD Saarland

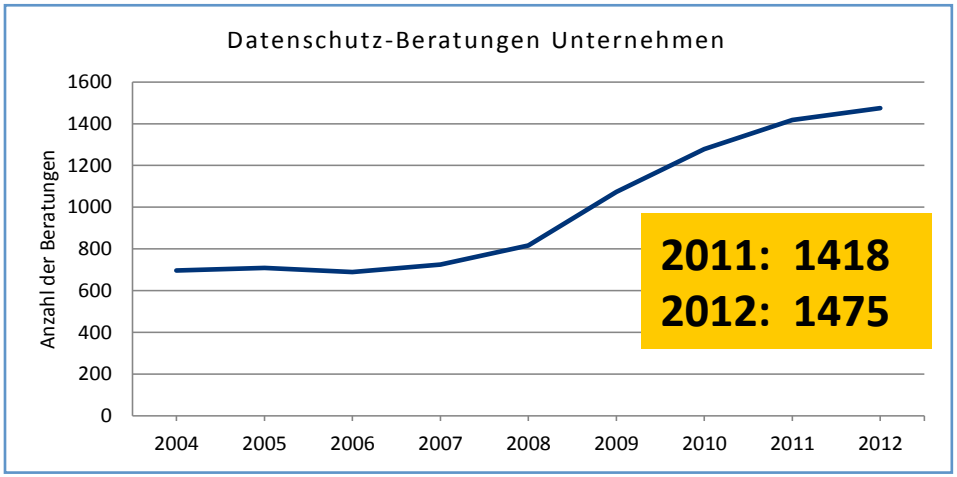
DB Sachsen

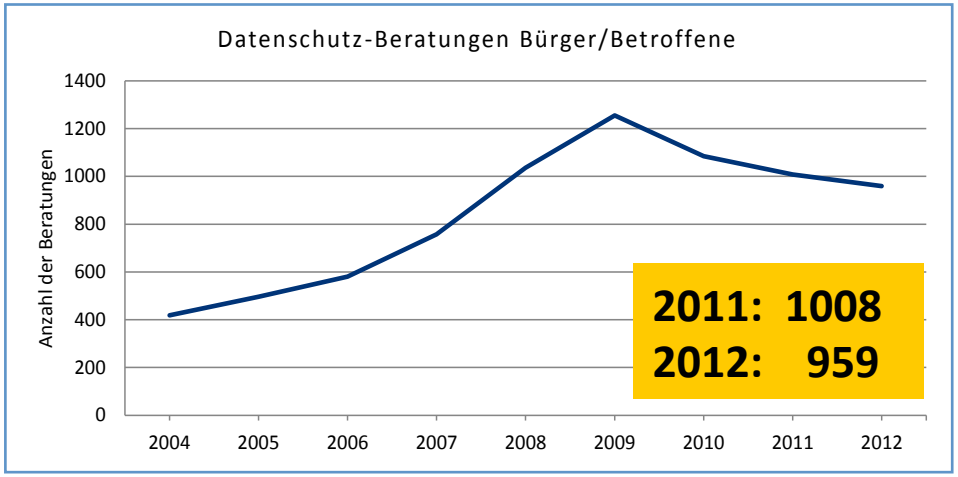
LfD Sa-Anh

ULD SH

LfD THÜ

## Beratung für Unternehmen

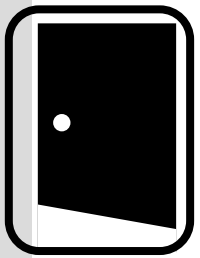


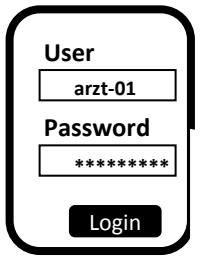

## Beratung für Privatleute

# 1. Datenschutzaufsichtsbehörden

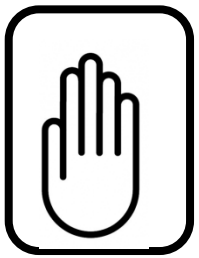




Zutritt

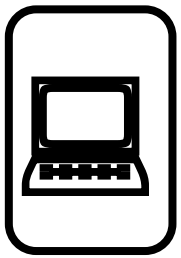



Zugang



Zugriff

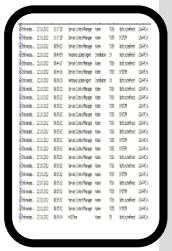
Weitergabe



Eingabe

Verfügbarkeit

Auftrag



Protokollierung

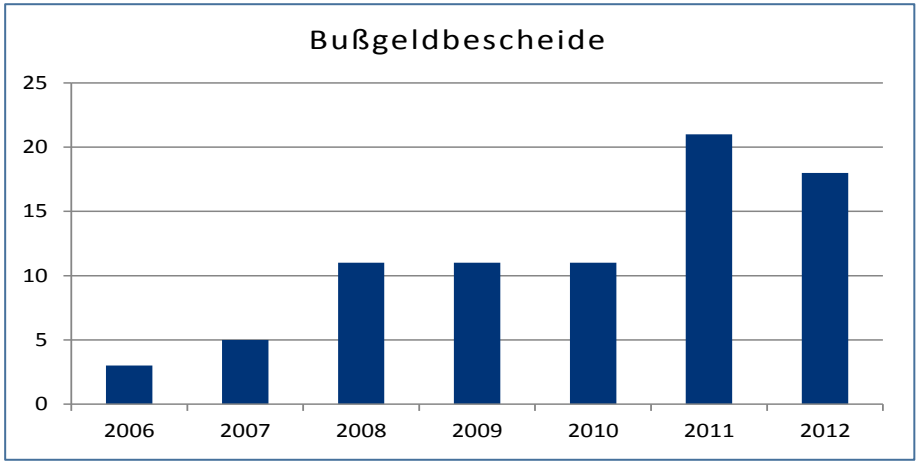
**Maßnahmen der Datensicherheit gemäß § 9 BDSG i.V.m. Anlage zu § 9**

- Tür, Schrank, Schloss
- Pass-wort, Sperre bei Ver-lassen
- Berech-tigungs-konzept, Entsor-gung
- Firewall, Ver-schlüs-selung
- Revisions-sicherheit; wer gibt ein
- Daten-siche-rung, USV - Strom
- Dienst-leister prüfen
- Doku-menta-tion von Zugriff

# 1. Datenschutzaufsichtsbehörden



## Bußgeldbescheide




- Insgesamt wurden 174 Ordnungswidrigkeits<u>verfahren</u> eröffnet (inklusive Onlineprüfung Google Analytics)
- Davon wurden **39 Bußgelder** verhängt
- Insgesamt 37.000 Euro

| Eingeleitete Verfahren mit Tatvorwurf | Anzahl | davon eingestellt | davon Bußgeld-bescheid | bestandskräftig ohne Rechtsmittel | Entscheidung AG |
|---|---|---|---|---|---|
| Fahrzeugortung mit GPS | 2 | | 2 | 2 | |
| Unsachgemäße Entsorgung von Unterlagen mit personenbezogenen Daten (insb. Papiermüll) | 1 | 1 | | | |
| Google Analytics: Übermittlung ungekürzter IP-Adressen an Google | 105 | 99 | 6 | 5 | Einspruch Rücknahme |
| Anfertigung von Nahaufnahmen (Fotos) von Demonstrationsteilnehmern | 2 | 2 | | | |
| Unternehmen, das in einem Internetportal negativ bewertet wurde, teilt den Namen des Bewertenden einem anderen Unternehmen mit, das von derselben Person bewertet wurde | 1 | | 1 | 1 | |
| Unternehmen verrät private E-Mail-Adresse eines ausgeschiedenen Mitarbeiters durch Nennung im „Abwesenheitsassistenten" des E-Mail-Programms (vereinbart war, dass Unternehmen eingehende E-Mails an den Mitarbeiter nachsendet) | 1 | 1 | | | |
| Weitergabe einer Vermögens- und Einkünfteübersicht zu einem Kunden durch Bank an ein verbundenes Unternehmen zwecks Verteidigung in einem Schadensersatzprozess | 1 | | 1 | 1 | |
| Ungeklärte Beschaffung einer Telefonnummer | 3 | 3 | | | |
| Werbender stellt nicht sicher, dass Beworbene Kenntnis über die Herkunft ihrer Daten erhalten können | 2 | 2 | | | |
| Weitergabe von Daten eines früheren Bankkunden an Dienstleister zwecks Beobachtung von Insolvenzbekanntmachungen | 1 | | 1 | 1 | |
| Unzulässige Speicherung, obwohl rechtskräftig gerichtlich geklärt ist, dass keine Geschäftsbeziehung besteht | 1 | | 1 | 1 | |
| Abruf von Daten zu Zahlungsvorgängen durch Mitarbeiter einer Zahlungsverkehrsdienstleistungfirma aus privater Neugier | 1 | 1 | | | |
| Hinzuspeicherung einer Telefonnummer (Hinzuspeicherung war zulässig) | 1 | 1 | | | |

# 1. Datenschutzaufsichtsbehörden



# Gliederung



1. Datenschutzaufsichts- und -kontrollbehörden
2. **Themen des Düsseldorfer Kreises**
   a. **Videoüberwachung**
   b. **E-Mail und Internetnutzung am Arbeitsplatz**
   c. **Anonymisierung, Pseudonymisierung, Big Data**
   d. **Facebook - Zuständigkeit**
   e. **Internationaler Datenverkehr, Safe Harbour und NSA**
3. Prüfpraxis des BayLDA
4. Diskussion um Datenschutz-Grundverordnung

## Rechtsgrundlage § 6b BDSG

**(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie**

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. **zur <u>Wahrnehmung</u> berechtigter Interessen für <u>konkret</u> <u>festgelegte</u> <u>Zwecke</u>**

**<u>erforderlich</u> ist und keine Anhaltspunkte bestehen, dass <u>schutzwürdige Interessen</u> der Betroffenen überwiegen.**


(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Verarbeitung oder Nutzung … ist zulässig, wenn …
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese …
(5) Die Daten sind unverzüglich zu löschen, wenn …

# 2. Themen des Düsseldorfer Kreises

## a. Videoüberwachung



- Darf ich das Haus meines Nachbarn überwachen?
- Darf ich Haus und Zufahrts-straße meines Nachbarn überwachen?
- Macht es einen Unterschied, ob man nur anschaut oder aufzeichnet?


- Was ist, wenn es sich „bei der Kamera“ nur um eine Attrappe handelt?

1. Techniktest mit Videokameras auf öffentlichen Straßen
   a. Begutachtung der Straßenqualität
   b. Überprüfung der Geeignetheit von Fahrradwegen
   c. Connected Drive - Fahrzeugtest
2. Videokamera im Privat-PKW („Dashboard-Kamera“)
3. Videoüberwachung aus der Luft (Drohnen)
4. Videoüberwachung in Taxis
5. Videoüberwachung in Schwimmbädern

- **<u>E-Mail und Internetnutzung im Unternehmen</u>**:
  - Wenn erlaubt, kann Arbeitgeber als Telekommunikationsanbieter angesehen werden, muss Fernmeldegeheimnis beachten, „Zugriffsproblem“ bei Urlaub, Krankheit o.ä.
  - Wenn verboten, Vollkontrolle der Mitarbeiter unzulässig
  - **<u>Empfehlung</u>**: Thema regeln insbes. Zugriffsmöglichkeiten – sonst verbieten

## c. Anonymisierung und Pseudonymisierung



**SGB V: § 300 Abrechnung der Apotheken und weiterer Stellen**

(2) Die Apotheken und weitere Anbieter von Leistungen nach § 31 können zur Erfüllung ihrer Verpflichtungen nach Absatz 1 Rechenzentren in Anspruch nehmen. Die Rechen-zentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke und ab dem 1. Januar 2003 nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; **anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.**

**Absolute Anonymisierung**

- Löschen aller Felder
- Berücksichtigung des potentiellen kriminellen Verhaltens

**SGB X: § 67 Begriffs-bestimmungen**

(8) **Anonymisieren ist** das Verändern von Sozialdaten der-art, dass die Einzelangaben über persönliche oder sachli-che Verhältnisse nicht mehr oder nur mit einem unverhält-nismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder be-stimmbaren natürlichen Person zugeordnet werden können.

**Faktische Anonymisierung**

- Verschlüsseln relevanter Felder
- Keine Berücksich-tigung des poten-tiellen kriminellen Verhaltens

## d. Facebook - Zuständigkeit



**BDSG: § 1 Abs. 5 Zweck und Anwendungsbereich des Gesetzes**

(5) Dieses Gesetz findet **keine Anwendung**, sofern eine in einem **anderen Mitgliedstaat** der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene **verantwortliche Stelle** personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. …

- **Facebook Inc. mit Sitz in USA**
- **Facebook Ltd. mit Sitz in Irland**

- **VG Schleswig:** Niederlassung in Irland, BDSG nicht anwendbar, sondern irisches (Datenschutz-)Recht, könnte wohl von deutschen Aufsichtsbehörden angewendet werden.

# 2. Themen des Düsseldorfer Kreises
## e. Internationaler Datenverkehr, Safe Harbour und NSA



**2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens„**

(1) Ungeachtet ihrer Befugnisse, …, können die zuständigen Behörden in den Mitgliedstaaten ihre bestehenden Befugnisse ausüben, … , wenn
a) …
b) **eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze verletzt werden**; wenn Grund zur Annahme besteht, dass die jeweilige Durchsetzungsinstanz nicht rechtzeitig angemes-sene Maßnahmen ergreift bzw. ergreifen wird, um den Fall zu lösen; …

- **Ist flächendeckende Überwachung durch Geheimdienst Verletzung der Grundsätze (welcher?)**
- **Was bedeutet es, dass Geheimdienstaktivitäten wohl nach US-Recht erlaubt sind?**
- **Untersagung von Datenübermittlungen in USA (auch nach England??)**
- **Prüfung läuft**

# Gliederung



1. Datenschutzaufsichts- und -kontrollbehörden
2. Themen des Düsseldorfer Kreises
   a. Videoüberwachung
   b. E-Mail und Internetnutzung am Arbeitsplatz
   c. Anonymisierung, Pseudonymisierung, Big Data
   d. Facebook - Zuständigkeit
   e. Internationaler Datenverkehr, Safe Harbour und NSA
3. **Prüfpraxis des BayLDA**
4. Diskussion um Datenschutz-Grundverordnung

# 3. Prüfpraxis des BayLDA



Kontrollen vom „grünen Tisch“ aus

Vor-Ort-Kontrollen

## Kontrollen

| | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|
| **Kontrollen ohne Vor-Ort-Besuch** | | | **50** | **13.404** |
| Banken, Finanzbereich | | | 42 | |
| Webseiten (Google Analytics) | | | | 13.404 |
| Videoüberwachung in Bäckerei-Filialen | | | 8 | |
| **Kontrollen mit Vor-Ort-Besuch** | **10** | **10** | **12** | **20** |
| Gesundheitsbereich | | | | 12 |
| Datenschutzorganisation und Technik | 3 | 3 | 3 | 3 |
| Auskunfteien | | 1 | 3 | 2 |
| Internetbezug | 4 | 4 | 3 | |
| Videoüberwachung | 2 | | 2 | 1 |
| Banken, Finanzbereich | 1 | 2 | 1 | 2 |

# Anlasslose und anlassbezogene Kontrollen

Kontrolle setzt keine Beschränkung auf einen Einzelfall oder einen Anlass voraus (Petri in Simitis, BDSG, Rdnr. 32 zu § 38 BDSG)

Kriterien für anlass**lose** Kontrolle

- Branchen
- Verarbeitungsarten
- Zufall (Fitnessstudios)
- Info über Realität (Ärzte)
- Sensible Daten
- …

Kriterien für anlass**bezogene** Kontrolle

- Gravierender Verstoß
- Früheres Verhalten
- Presseberichte
- Häufung von Beschwerden
- …
- …

# 3. Prüfpraxis des BayLDA



- **Videoüberwachung in Einkaufsläden**: 27 Läden im Münchener Fußgängerzone, Start: 26.04.2013, Ende: Oktober 2013
- **Allgemeine Unternehmens- und Bankenprüfung**: 150 Unternehmen, davon 50 Banken, Start: 21.01.2013, Ende: Oktober 2013
- **Arztpraxen**: 16 Ärzte, Start: April 2013, Ende: Oktober 2013
- **Zahnarzt/Labor**: 70 Zahnärzte, Start: 03.07.2013, Ende: Oktober 2013
- **App-Prüfung** (Internet Sweep Day): 30 App-Anbieter, Start: 14.06.2013, Ende: September 2013
- **Fitnessstudios**: 93 Fitnessstudios, Start: 31.05.2013, Ende: Oktober 2013
- **Adobe-Prüfung**: 46 Webseitenanbieter, Start: 14.06.2013, Ende: Oktober 2013
- **App-Prüfung** bayerischer Anbieter (permanent)

# 3. Prüfpraxis des BayLDA



- Jedes Referat soll regelmäßig anlasslos sog. „Großprüfung“ durchführen.
- Halbjährliche Planung der Prüfungen im BayLDA
- Vor der Prüfung Ziel festlegen.
- Zeitplan aufstellen.
- **Prüfungsschreiben** mit strukturiertem Antwortschreiben (ankreuzen) entwerfen; Fragen mit Freitextfeldern sind auf das notwendige Maß beschränken (**aber**: Vorlage von Unterlagen, § 11 Verträge, Daten-Sicherheitskonzept, Verfahrensverzeichnis, Videokonzept).
- **Standardisierte Excel-Tabelle für Auswertungsdatei** erstellen, Prüfalgorithmus hinterlegen

# Sachverhalt

Eine Mitarbeiterin eines Handelsunternehmens hat an Kunden eine E-Mail verschickt, die aus-gedruckt zehn Seiten umfasst, wobei neun-einhalb Seiten die E-Mail-Adressen ausma-chen und eine halbe Seite die Information be-inhaltete, dass man sich zeitnah um die An-liegen der Kunden kümmern werde.

# 3. Prüfpraxis des BayLDA (Bußgeld)



- E-Mail-Adressen sind personenbezogene Daten (thomas-kranig@t-online.de)
- Durch Sammel E-Mail werden personenbezogene Daten an alle Empfänger der Sammel-E-Mail bekannt gegeben (Verarbeitung in Form der Übermittlung nach § 3 Abs. 4 Satz 2 Nr. 3 BDSG).
- E-Mail-Adressen sind in der Regel keine allgemein zugänglichen Daten. Jeden-falls stellt die Information, dass der jeweilige E-Mail-Empfänger im Vorfeld mit dem Unternehmen in Verbindung stand, keine für jedermann zugängliche Information dar (§ 43 Abs. 2 Nr. 1 BDSG).
- Verbot mit Erlaubnisvorbehalt: Übermittlung nur zulässig, wenn Einwilligung vorliegt oder Rechtsvorschrift Übermittlung erlaubt oder anordnet; hier nicht gegeben (§ 4 Abs. 1 BDSG)

→ **Offener E-Mailverteiler ist OWi nach § 43 Abs. 2 Nr. 1 BDSG.**

# 3. Prüfpraxis des BayLDA (Bußgeld)



- **<u>Bußgeldrahmen</u>**: 5 bis 150.000,00 EUR (§ 43 Abs. 3 BDSG i.V.m. § 17 OWiG)
  - Bedeutung des Vorwurfs (Fahrlässigkeit)
  - Bedeutung des Verstoßes (Zahl der Personen, Gewichtung des einzelnen Verstoßes)
  - Wirtschaftliche Verhältnisse

- **<u>Warum gegen Mitarbeiterin?</u>**
  - Persönliche Verantwortung für Fehlverhalten
  - Kein Indiz für mangelnde Organisation in Unternehmen (sonst Unternehmensleitung wegen Organisationsverschulden haftbar)

# Gliederung



1. Datenschutzaufsichts- und -kontrollbehörden
2. Themen des Düsseldorfer Kreises
   a. Videoüberwachung
   b. E-Mail und Internetnutzung am Arbeitsplatz
   c. Anonymisierung, Pseudonymisierung, Big Data
   d. Facebook - Zuständigkeit
   e. Internationaler Datenverkehr, Safe Harbour und NSA
3. Prüfpraxis des BayLDA
4. **Diskussion um Datenschutz-Grundverordnung**

# 4. Diskussion um Datenschutz-Grundverordnung



- Am **25. Januar 2012** hat die EU-Kommission zur Fortschreibung der EU-Datenschutzrichtlinie vom 24. Oktober 1995 (RL 95/46/EG) den Entwurf einer „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (**Datenschutz-Grundverordnung**) vorgelegt.

- Diese Verordnung hat die **Vollharmonisierung** des Datenschutzrechts in Europa zum Ziel (d.h. Wegfall von Bundes- und Landesdatenschutzgesetzen und vieler sonstiger bereichsspezifischer Datenschutzregelungen.)


Quelle: ec.europa.eu

**Viviane Reding**

Vizepräsidentin

Kommissarin für Justiz, Grundrechte und Bürgerschaft

# 4. Diskussion um Datenschutz-Grundverordnung



- **<u>Diskussionspunkte aus Sicht des BayLDA</u>**:
  - Einwilligung
  - Datenschutzbeauftragter
  - Zuständigkeit Aufsichtsbehörde (one-stop-shop)
  - Vertretung im Europäischen Datenschutzausschuss
  - Kompetenz des Europäischen Datenschutzaus-schusses und der EU-Kommission
  - Einschränkung der delegierten Rechtsakte
  - …

# 4. Diskussion um Datenschutz-Grundverordnung



Beratung im **Europäischen Parlament**

Beratung im **Rat** (= Regierungschefs der Mitgliedstaaten der EU)

- Trilog-Verhandlungen zwischen Parlament, Rat und Kommission
- Beschlussfassung im Europäischen Parlament
- Beschlussfassung im Rat
- **Inkrafttreten gepl. in 2014, d.h. dann Beginn der zweijährigen Umsetzungsphase**

**Was auf Dauer wirklich gilt, ist mehr als offen.**

# Vielen Dank für Ihr Interesse

**Thomas Kranig**
Präsident des Bayerischen
Landesamtes für Datenschutzaufsicht