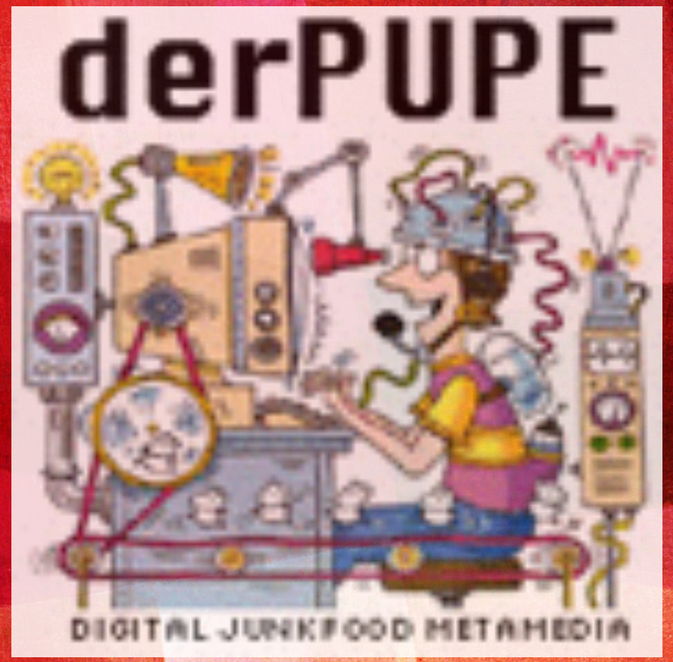
DIE EU DATENSCHUTZGRUNDREFORM

Rechte für Menschen - Pflichten für Firmen - Chancen für uns

derPUPE @ #33c3 - 30.12.2016



WHO AM I ...

- Lars Hohl - derPUPE <disclaimer>
- Humanoid - 43 Jahre
- Liebe IT in Ihrer ganzen Mannigfaltigkeit, Politik, Schach & meine Mitmenschen
- $irgendwas mit #HAL & #22c3

  zenga IFG & Datenschutz

- heute beruflich: Datenschutzbeauftragter und Information Security Manager

#DSGVO – WAS BISHER GESCHAH

- Ausgangslage: DS Richtlinie 95/46/EG & BDSG
- Gesetzlicherer Flickenteppich in 28 Staaten
- Reform-Prozess 2012 gestartet
- Ziele: Einheitliches DS Gesetz für gesamt Europa - Freier Datenverkehr in EU - Faire und transparenten Datenverarbeitung
- DSGVO verabschiedet: 05.2016

- Es gilt das Marktortprinzip
- Ein Abschwächen von Datenschutz gemäß DSGVO ist ausgeschlossen

#DSGVO – WAS NOCH KOMMT

- DSGVO enthält (leider) Öffnungsklauseln
- Bis zum 24.Mai 2018 haben die EU-Mitgliedstaaten Zeit, das nationale Recht – wo nötig und möglich – an das neue EU-Recht anzupassen.
- BMI: #DSAnpUG-EU - Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
- Datenschutz-Grundverordnung wird somit ein „Hybrid“ zwischen einer Richtlinie und Verordnung
- Die DSGVO ist dann ab dem 25.5.2018 in allen Ländern für alle Firmen bindend


EIN TALK ÜBER DATENSCHUTZ
WORAN DENKEN DIE MEISTEN?
imgflip.com

WELT ONLINE
WIRTSCHAFT

DATENSCHUTZ (11)

Bahn und Daimler geraten ins Visier der Behörden

VON NIKOLAUS DOLL 16. April 2009, 23:31 Uhr

Wegen Datenschutz-Pannen stehen gleich zwei deutsche Großko
Druck. Erstmals ermittelt die Staatsanwaltschaft gegen die Deuts
geht sie nach Informationen von WELT ONLINE in zwei Richtungen
Autobauer Daimler gibt es im Bremer Werk Unregelmäßigkeiten.

Schlamperei bei Hypo-Bank: Konto-Auszüge auf dem Müll

Von Dorita Plange

München – Eine Bank, ein Wort? Ein Hund hat bei der Bayerischen Hypotheken- und Wechselbank (Aktueller Werbeslogan: „Wir lassen uns was für Sie einfallen!") in Unterhaching einen Datenskandal ersten Ranges enthüllt. Auf der Jagd nach einer Katze sprang „Bingo" am Mittwochabend in einen Bau-Container vor der Hypo-Filiale an der Münchner Straße. Dabei platzte einer von mehreren blauen Müllsäcken. Heraus purzelten hundertfach Kundenkarten mit brisanten Inhalt: Kontostände, Wertpapier-Geschäfte, Kredite, handschriftliche Vermerke über Pläne und persönliche Nöte der Kunden – und das [illegible] Namen! Betroffen sind hunderte Unterhachinger B[illegible] men, Vere[illegible] namhafte Manage[illegible]

Hamburger Abendblatt

Abendblatt als Startseite | Aboservice | E-Paper www.abendblatt.de

Sie sind hier: Nachrichten > Aus aller Welt

AUS ALLER WELT

Versenden Ausdrucken

BUSSGELD

Datenskandal: Bahn droht Millionen-Strafe

20. Oktober 2009, 06:00 Uhr

Wegen des internen Datenskandals soll die Deutsche Bahn nach einem Bericht der "Süddeutschen Zeitung" ein Bußgeld in Höhe von 1,1 Millionen Euro zahlen.

BERLIN. Der Konzern habe einen entsprechenden Bescheid des Berliner Datenschutzbeauftragten Alexander Dix erhalten, bestätigte gestern ein [illegible] der Summe äußerte er sich jedoch nicht. Bei der Bahn [illegible] heimlich Daten von Mitarbeitern abgeglichen und [illegible] rrupte Angestellte aufzuspüren. Nach Bekanntwerden d[illegible] hartmut Mehdorn freiwillig. Die Bahn hat nun 14 Tag[illegible]

FOCUS MONEY ONLINE FINANZEN

« Home

Datenschutz

Neuer Skandal bei der Telekom

Deutsche Großunternehmen sind beim Sammeln sensibler Daten [illegible] noch schmerzfreier als bisher angenommen. [illegible] im Visier: die Deutsche Telekom.

[illegible] chen Bahn hat

N24 Login Registrierung

NACHRICHTEN BÖRSE VIDEOS WISSEN TIPPS & SERVICE BILDERSERIEN

Verstoß gegen Datenschutz

Lidl muss erneut Strafe zahlen

Lidl muss wegen Verstößen gegen den Datenschutz in Nordrhein-Westfalen erneut ein Bußgeld zahlen. Der Discounter hatte heimlich Krankendaten vieler Mitarbeiter gesammelt.

Der Discounter Lidl muss erneut wegen Verstößen gegen den Datenschutz zahlen: Nach einem Bußgeld von 1,5 Millionen Euro wegen Bespitzelung von Mitarbeitern im letzten Herbst fordert der nordrhein-westfälische Datenschutz jetzt 36.000 Euro von der Neckarsulmer Handels-Kette (Kreis Heilbronn). Grund: Die Regionalgesellschaft in dem Bundesland hatte unzulässigerweise Daten von Krankheiten der Mitarbeiter erhoben und gespeichert. Betroffen seien [illegible]


EIN TALK ÜBER DATENSCHUTZ
WO IST DIE DEFINITION?
imgflip.com

DATENSCHUTZ – WAS IST DAS?

- Schutz der **informationellen Selbstbestimmung** von Menschen
- Datenschutz will den „gläsernen Menschen“ verhindern.
- Jeder Mensch soll grundsätzlich selbst entscheiden, **wem wann welche seiner persönlichen Daten zugänglich** sind.

#DSGVO Ziel „**Faire und transparenten Datenverarbeitung**“ dafür unabdingbar

WARUM KÜMMERN SICH FIRMEN DARUM?

- juristisch / compliance:

  weil es gesetzlich vorgeschrieben

- Zum Image-Erhalt

  Vermeidung von Kosten zum erneuten Imageaufbau nach Datenschutzskandal

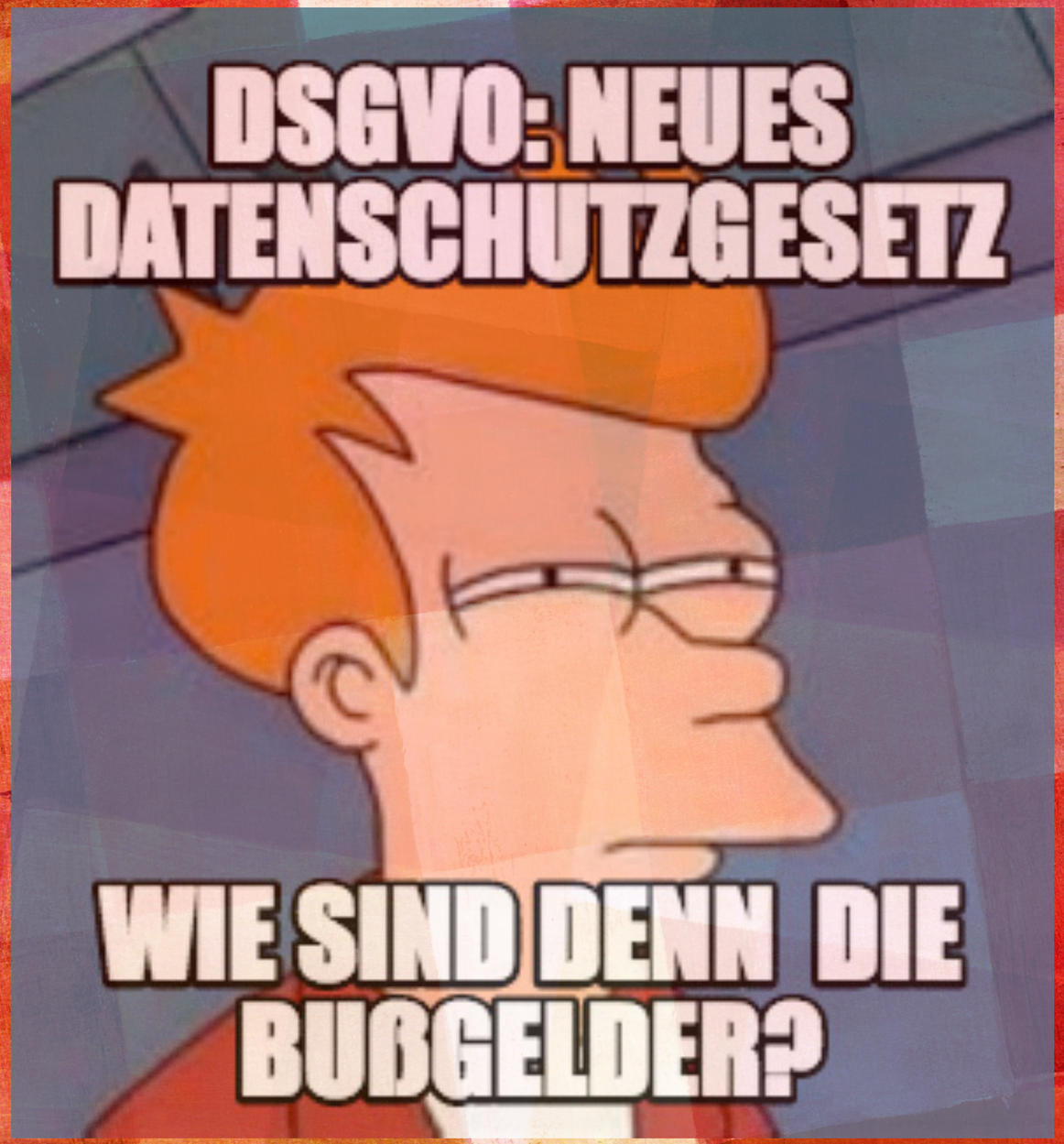
- Zur Busgeld-Prävention

  Vermeidung von Kosten durch Strafzahlungen

PLANUNGSANNAHMEN / THESEN

- Datenschutz ist in der Regel kein Primärziel von Firmen und Institutionen
- Firmen agieren in der Regel mit Gewinnerzielungsabsicht
- Datenschutz ist wie alles andere in Firmen eine Kostenstelle.
- Kostenstellenverantwortliche müßen jährlich Ihr Budget und FTE Bedarf verargumentieren
- In Geld quantifizierbare Risiken (zB mögliche Bußgelder) sind sehr nützlich und schaffen Managementawareness

RISIKO: DATENSCHUTZ BUßGELDER



SCHADENPOTENTIAL SANKTIONEN

- jeder Verstoß kann ein Bußgeld auslösen
- Maximale Strafe (a) bis zu 20.000.000 € oder (b) 4% des weltweiten Konzernumsatzes

  (Art. 83 Abs. 5 Buchst, b DSGVO)

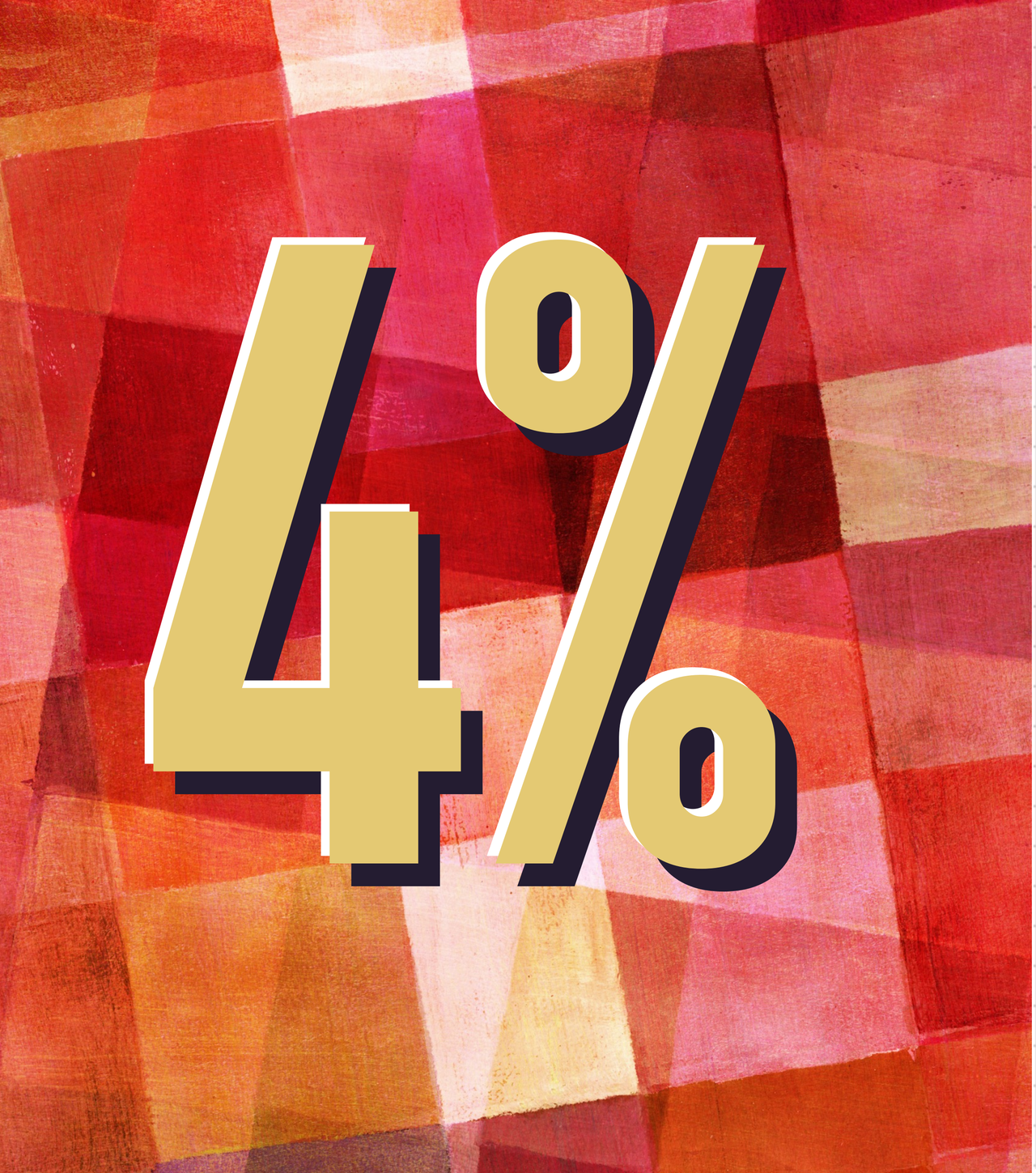
  Keine Deckelung: Der höhere Betrag (a) oder (b) ist Ausschlag gebend

BEKANNTE DATENSCHUTZFÄLLE

Deutsche Bahn Strafe 2009 1,1 Mio
=-Im neuen DSGVO Busgeldrahmen-=
Deutsche Bahn Umsatz 39,2 Mrd
=> DSGVO-Budgeld 4% => 1,568 Mrd.

LIDL - akkumulierte Strafe 1,5 Mio
=-Im neuen DSGVO Busgeldrahmen-=
LIDL-Umsatz ca. 59 Mrd
DSGVO-Busgeld 4% => 2,36 Mrd.

MÖGLICHE DSGVO BUSGELDER



Dax-Konzern:	Jahresumatz	max. Bußgelt
Volkswagen	213.292.000,00 €	8.531.680,00 €
Daimler	149.467.000,00 €	5.978.680,00 €
Allianz	125.190.000,00 €	5.007.600,00 €
E.ON	116.218.000,00 €	4.648.720,00 €
BMW	92.175.000,00 €	3.687.000,00 €
Siemens	75.636.000,00 €	3.025.440,00 €
BASF	70.449.000,00 €	2.817.960,00 €
Deutsche Telekom	69.228.000,00 €	2.769.120,00 €
Deutsche Post	59.230.000,00 €	2.369.200,00 €
Munich Re	50.400.000,00 €	2.016.000,00 €
RWE	48.599.000,00 €	1.943.960,00 €
Bayer	46.324.000,00 €	1.852.960,00 €
ThyssenKrupp	42.778.000,00 €	1.711.120,00 €
Continental	39.232.000,00 €	1.569.280,00 €
Deutsche Lufthansa	32.056.000,00 €	1.282.240,00 €
Fresenius	27.626.000,00 €	1.105.040,00 €
SAP	20.793.000,00 €	831.720,00 €
Henkel	18.089.000,00 €	723.560,00 €
Linde	17.944.000,00 €	717.760,00 €
Adidas	16.915.000,00 €	676.600,00 €
Fresenius Medical Care	16.738.000,00 €	669.520,00 €
HeidelbergCement	13.465.000,00 €	538.600,00 €
Merck	12.845.000,00 €	513.800,00 €
Beiersdorf	6.686.000,00 €	267.440,00 €
Infineon	5.795.000,00 €	231.800,00 €
K+S	4.176.000,00 €	167.040,00 €
Vonovia	3.506.000,00 €	140.240,00 €
Deutsche Börse	2.367.000,00 €	94.680,00 €

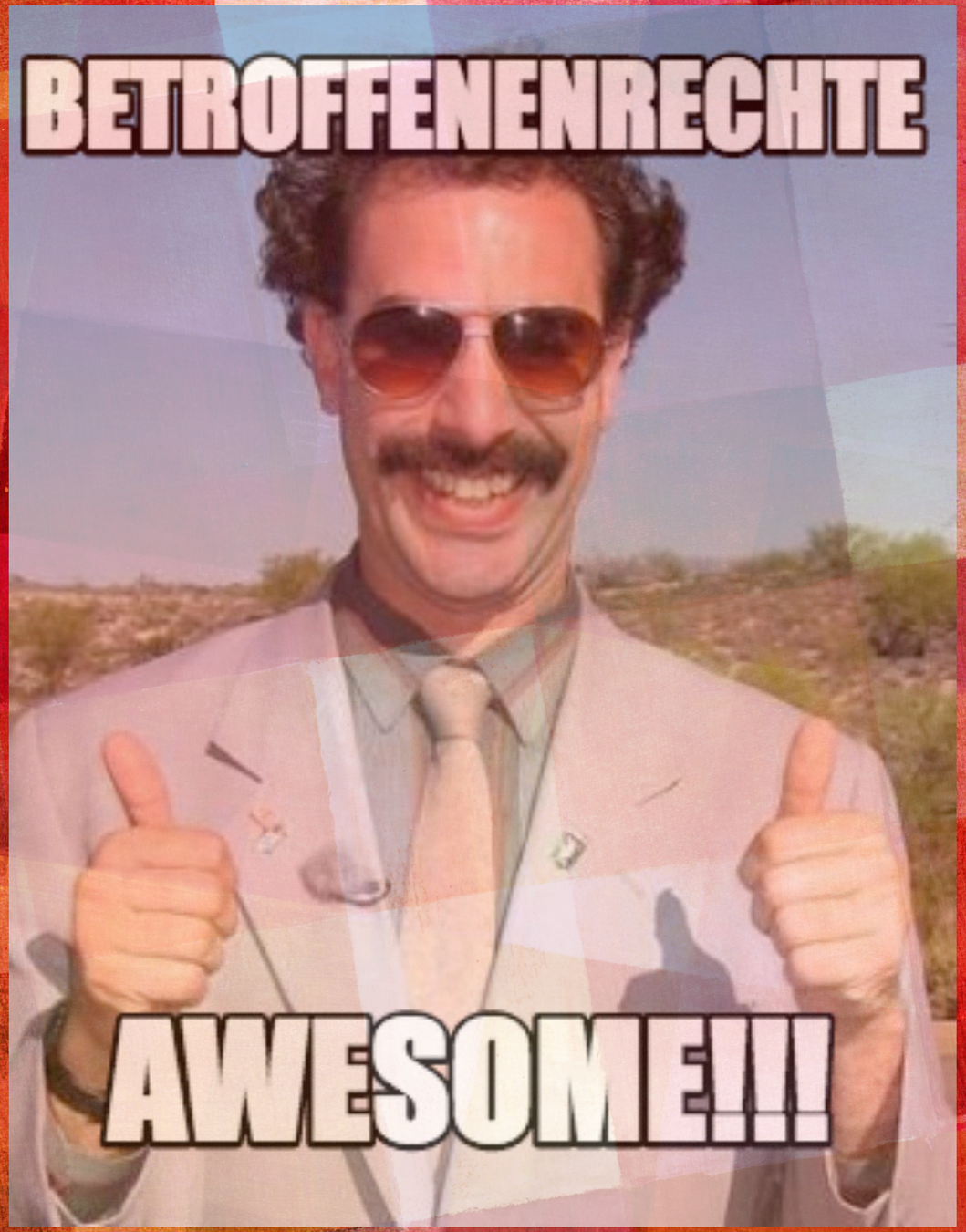

Was können wir jetzt damit machen?
Wo kommen wir jetzt ins Spiel?

RISIKO: DATENSCHUTZ BUßGELDER

BEISPIEL: BETROFFENEN RECHTE

- „Betroffenenrechte“ sind **Ansprüche** und **Gestaltungsmöglichkeiten**, die den **Berechtigten** aufgrund ihrer **Betroffeneneneigenschaft** zukommen und einen hinreichend konkreten, idealerweise **vollstreckungsfähigen** Inhalt besitzen.

- **Rechte** für **Betroffene** gehen mit **Pflichten** von **verantwortlichen Stellen** einher



ZIELRICHTUNGEN VON BETROFFENENRECHTEN

- (1) **Permissionsrechte** gestatten Datenverarbeitungen
- (2) **Interventionsrechte** vermögen bestimmte Datenverarbeitungen zu verhindern
- (3) **Informationsrechte** vermitteln ein Bild darüber, was mit den Daten geschieht
- (4) **Petitionsrechte** verbriefen Beschwerdemöglichkeiten
- (5) **Kompensationsrechte** gewähren Schadensersatz bzw. Entschädigung.

AUSKUNFTSRECHTE / AUSKUNFTSPFLICHTEN

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten,
- Empfänger oder Kategorien von Empfängern,
- die Speicherdauer oder Kriterien für die Festlegung derselben,
- umfassende Informationen über Betroffenenrechte,
- die verfügbaren Informationen über die Herkunft der Daten außerhalb der Direkterhebung
- das Bestehen einer automatisierten Entscheidungsfindung nebst aussagekräftiger Informationen über die verwendete Logik.
- Nach Art. 15 Abs. 2 DS-GVO besteht zudem ein Unterrichtungsrecht hinsichtlich geeigneter Datenschutzgarantien bei unsicheren Drittländern.
- Art. 19 S. 2 DS-GVO enthält an etwas versteckter Stelle noch einen weiteren Anspruch auf Information darüber, welchen Empfängern die Berichtigung, Löschung oder Einschränkung von Daten mitgeteilt wird. Diese Information muss allerdings durch den Betroffenen konkret angefragt werden.

DATENSCHUTZGRUNDVERORDNUNG EXTREM USE

ALL YOUR AUSKUNFTSRECHTE

BEISPIEL: INFORMATIONSPFLICHTEN GEMÄß ARTIKEL 13 ABS. 1 DSGVO

A. Verantwortliche Stelle (Namen und Kontaktdaten)

B. Datenschutzbeauftragte/er (Kontaktdaten)

C. Zweck der Datenverarbeitung und die Rechtgrundlagen (Erlaubnistatbestand)

D. Soweit die DV auf dem „berechtigten Interesse“beruht (gem. Art 6 Abs. 1 DSGVO) ausdrückliche Nennung dieser Interessen

E. Empfänger der Daten, soweit Daten übermittelt werden. Oder Kategorie, wenn konkrete Unternehmen noch nicht bezeichnet werden können.

F. Datenübermittlung in Drittländer

BEISPIEL: INFORMATIONSPFLICHTEN GEMÄß ARTIKEL 13 ABS. 2 DSGVO

A. Dauer der Speicherung - Wenn keine Löschfristen definiert sind, ist die Nennung der Kriterien möglich.

B. Rechte der Betroffenen - Die Betroffenen sind über ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung sowie Datenübertragbarkeit hinzuweisen

C. Widerrufbarkeit von Einwilligungen

D. Beschwerderecht bei der Aufsichtsbehörde

E. Verpflichtung zur Bereitstellung personenbezogener Daten

F. Automatisierte Entscheidungsfindung und Profiling

INFORMATIONSPFLICHTEN ARTIKEL 14 DSGVO

- Nach Art. 14 Abs. 2 f) DSGVO muss der Verantwortliche den Betroffenen jedoch darüber aufklären, aus welcher Quelle die personenbezogenen Daten stammen und ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

IN WELCHER FORM MÜSSEN DIE INFORMATIONEN BEREITGESTELLT WERDEN?

- Nach Art. 12 DSGVO sind die oben dargestellten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erteilen. Dabei können sie schriftlich oder in elektronischer Form an den Betroffenen übermittelt werden.
- Es wird explizit erwähnt, dass dafür auch sog. standardisierte Bildsymbolen verwendet werden können, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln
- Anders als im BDSG wird es in der Datenschutz-Grundverordnung besondere Anforderungen an die Verarbeitung personenbezogener Daten von Kindern geben. In diesem Falle sollten nach Erwägungsgrund 58 der DSGVO aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

WANN MUSS DER BETROFFENE INFORMIERT WERDEN?

- Bei der Direkterhebung muss der Betroffene nach Art. 13 Abs. 1 DSGVO zum Zeitpunkt der Erhebung informiert werden.
- Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen nach Art. 14 Abs. 3 DSGVO grundsätzlich innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilen.
- Werden die Daten allerdings zur Kommunikation mit dem Betroffenen verwendet oder sollen an einen Empfänger übermittelt werden, ist die Information zwingend zum Zeitpunkt der Kontaktaufnahme oder ersten Übermittlung vorzunehmen.

KANN DIE INFORMATIONSPFLICHT EINGESCHRÄNKT SEIN?

- Bei der Direkterhebung kann nach Art. 13 Abs. 4 DSGVO auf die Information des Betroffenen nur dann verzichtet werden, wenn dieser bereits informiert wurde.
- Soweit die Daten nicht beim Betroffenen erhoben werden, sind die Informationspflichten gemäß Art. 14 Abs. 5 DSGVO in drei weiteren Fällen entbehrlich:

A. Die Information ist unmöglich oder unverhältnismäßig aufwendig.

B. Die Erhebung oder Übermittlung ist gesetzlich vorgeschrieben

C. Es besteht ein Berufsgeheimnis oder eine sonstige satzungsmäßige Geheimhaltungspflicht.

DIE 5 ZIELRICHTUNGEN DER BETROFFENENRECHTE IM DATENSCHUTZ

Permission	Intervention	Information	Petition	Kompensation
Einwilligung	Widerruf der Einwilligung	Tranzparenzpflichten bei Direkterhebung	Datenschutz-beauftragter	Art. 82 DSGVO
Einwilligung von Kindern	Widerspruch	Transparenzpflichten außerhalb der Direkterhebung	Betriebsrat	§§ 280 ff. BGB
Werbeeinwilligung	Unterlassungsanspruch	Datenpannen	Datenschutzaufsicht	§§ 823 ff. BGB
Schweigepflicht-entbindung	Gegendarstellung	Auskunfts- und Einsichtsrechte	Vertretung	
Erlass	Löschung	Datenübertragbarkeit	Staatsanwaltschaft	
Löschwiderspruch	Vergessenwerden		Standesrechtliche Gremien	
	Einschränkung			
	Berichtigung			

WEITERFÜHRENDE QUELLEN:

- RDV Recht der Datenverarbeitung (2016/03)

„Dr. iur. Lorenz Franck - Das System der Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO)“ S.111 ff

Netzfundstück: http://filestore.to/?d=FT2Q1LDZD8

- Kommunikation und Recht (10/2016)

„Dr. Carlo Pilz: Die Datenschutzgrundverordnung - Teil 2 - Rechte der Betroffenen und korrespondierende Pflichten des Verantwortlichen“ S.629 ff

Netzfundstück: http://filestore.to/?d=FT2Q1LDZD8

- Kommunikation und Recht (11/2016)

„Dr. Carlo Pilz: Die Datenschutz grundverordnung - Teil 3 - Rechte und Pflichten des Verantwortlichen und Auftragsverarbeiters“ S.709 ff

Netzfundstück: http://filestore.to/?d=NVNHYNHO7C

MOTIVATION

KONTAKT

- Elektromail: derPUPE@datengala.de
- Schlüssel ID: F44A70DE
- Fingerprint: 1971 929A 0069 A006 7033 A985 2027 D636 F44A 70DE
- XMP/Jabber: derPUPE@jabber.ccc.de
- Twitter: @derPUPE