Vorlesung FH Dortmund – Fachbereich Informatik –
Wintersemester 2023/24

IT-Recht Grundlagen für Informatiker
oder

was Geschäftsleitung, Vertrieb und Entwicklung schon immer wissen wollten, aber nicht zu fragen wagten!

Problem- und praxisorientierte Tipps für die Vertragsgestaltung

Rechtsanwalt Prof. Wolfgang Müller
Fachanwalt für Informationstechnologierecht
Fachanwalt für Bau- und Architektenrecht
Schlichter / Schiedsrichter nach SOBau
Honorarprofessor der Technischen Universität Dortmund
Lehrbeauftragter der Fachhochschule Dortmund

Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai

Die neue Datenschutz-Grundverordnung (DS-GVO), was man weiß, was man wissen sollte

oder

„Alles neu macht der Mai!“

bzw.

„Manches ist anders, manches genauso“

War da nicht noch irgendwas mit Datenschutz ???

Na dann schaun wir mal!
Dann sehn wir schon!

EU-Datenschutzrichtlinie

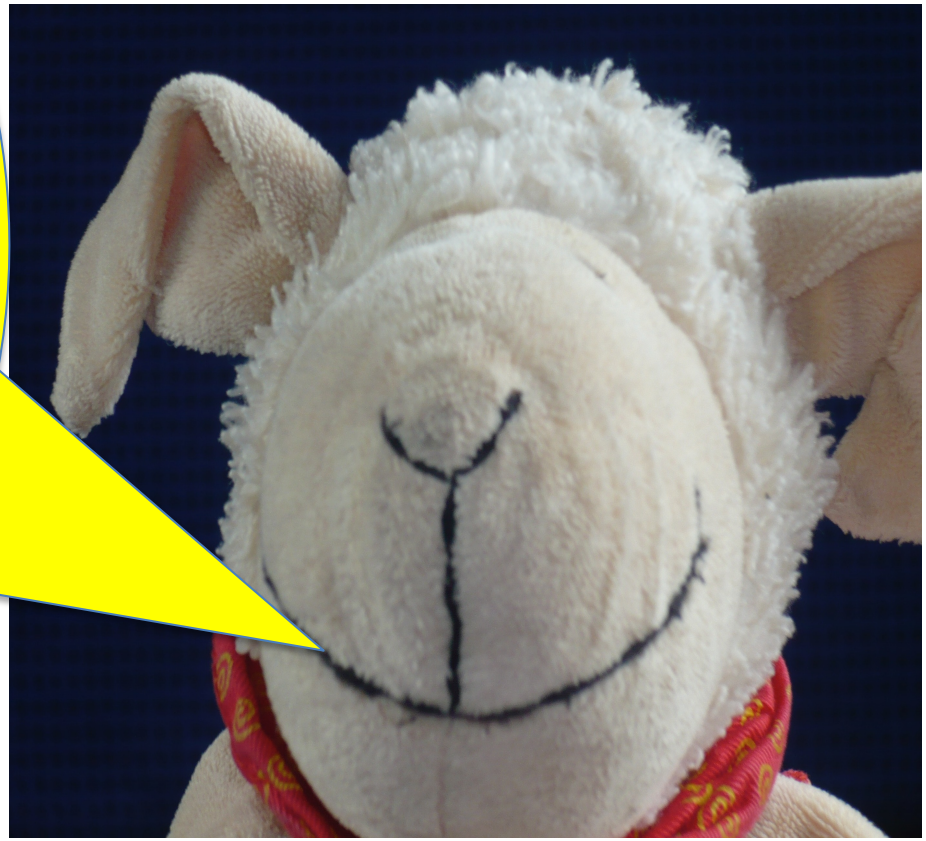
Mit der **Datenschutzrichtlinie** („**DSRL**“*) **sollte das Datenschutzrecht EU-weit harmonisiert werden**.

Die **DSRL** wurde in Deutschland durch das Bundesdatenschutzgesetz 2001 („**BDSG 2001**“) umgesetzt.

Die **DSRL** sollte einen **Rechtsrahmen für die Gewährleistung eines gleichwertigen Schutzes innerhalb der EU auf hohem Niveau schaffen**.

* Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsblatt der EG v. 23.11.1995, Nr. L. 281/31)

In der Vergangenheit hat sich allerdings gezeigt, dass eine einheitliche Umsetzung auf europaweiter Ebene **nicht** erreicht wurde, da die einzelnen Mitgliedsstaaten die Richtlinie doch mehr oder weniger **unterschiedlich** in nationales Recht umgesetzt haben **und** auch die Einhaltung entsprechender Vorschriften zum Teil nur recht halbherzig überwacht wurde!



Deshalb haben das
EUROPÄISCHE PARLAMENT
und der
RAT DER EUROPÄISCHEN UNION
eine Verordnung*
(*Datenschutz-Grundverordnung*)
zum Datenschutz beschlossen!

*VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTES UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. L EU L 119 vom 4.5.2016

Hää ?
Wo ist denn
da der
Unterschied
???

Bei einer **Richtlinie** hat jedes Mitgliedsland der EU Spielraum, wie sie den Inhalt der Richtlinie in nationales Recht umsetzt.
Eine **Verordnung** ist unmittelbar geltendes Recht auch auf nationaler Ebene, d.h. sie wird nur in die einzelnen Landessprachen übersetzt und gilt dann überall unverändert und gleich!

Nur soweit der europäische Gesetzgeber den Mitgliedsstaaten in der Verordnung selbst „*Spielräume*“ zur Ausgestaltung“ gewährt, können diese tätig werden und Regelungen treffen.

Das ist bei uns mit dem
Datenschutz-Anpassungs- und Umsetzungsgesetz EU
– DSAnpUG-EU –
insbesondere im Rahmen des schon bestehenden
Bundesdatenschutzgesetz
- BDSG -
erfolgt!

Hierzu aber an anderer Stelle
oder gar nicht!!!

*Gesetz zur Anpassung des Datenschutzes an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30. Juni 2017, BGBl. 2017 Teil 1 Nr. 44

Hää ???

Okay!
Soweit „*Allgemeine*“ Datenschutzvorschriften betroffen sind, in diesem Zusammenhang an anderer Stelle!
Soweit arbeitsrechtliche Problematiken betroffen sind, hier gar nicht!!!
Wir wollen ja auch noch nach Hause kommen!

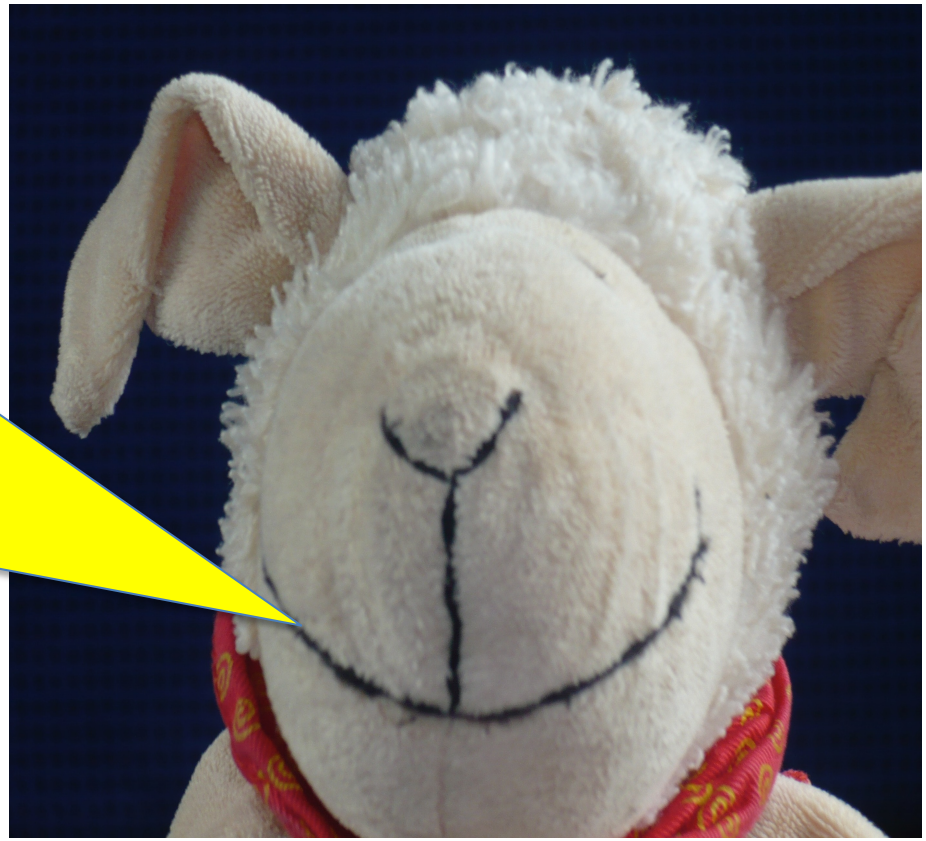
Und wie sieht das Ganze jetzt aus???

Mächtig heftig!

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 27. April 2016
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

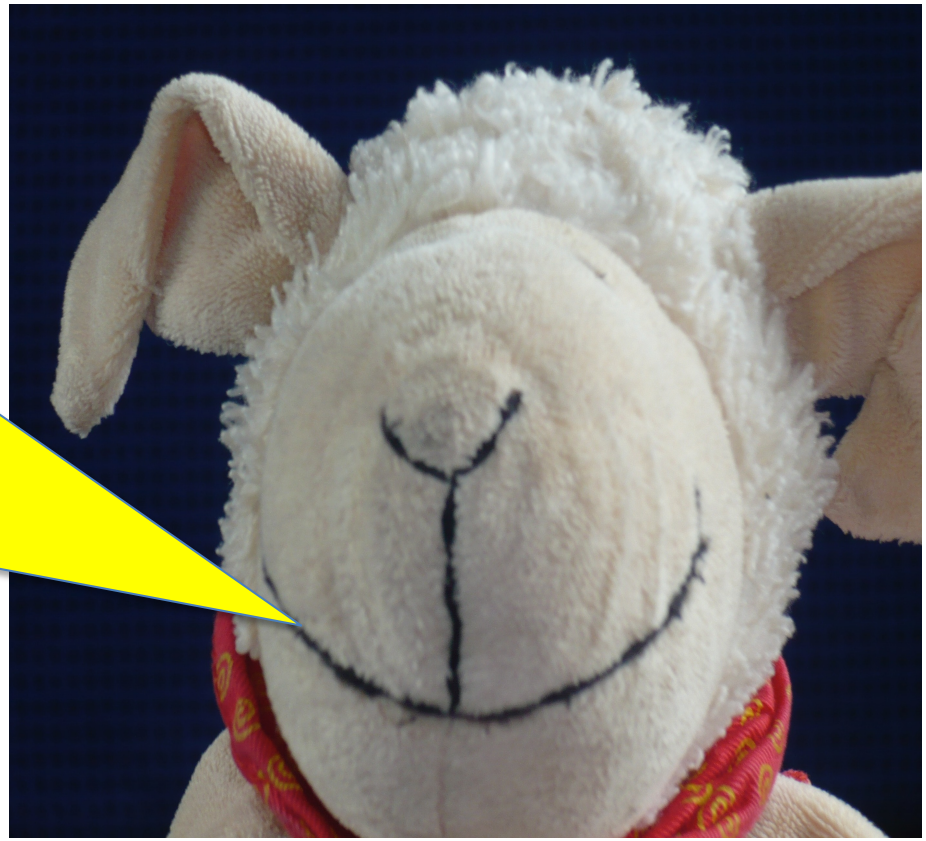
Puuh!!!
Und das
muss uns
nun alles
interessieren
???

Nein, natürlich nur ein Teil!!!



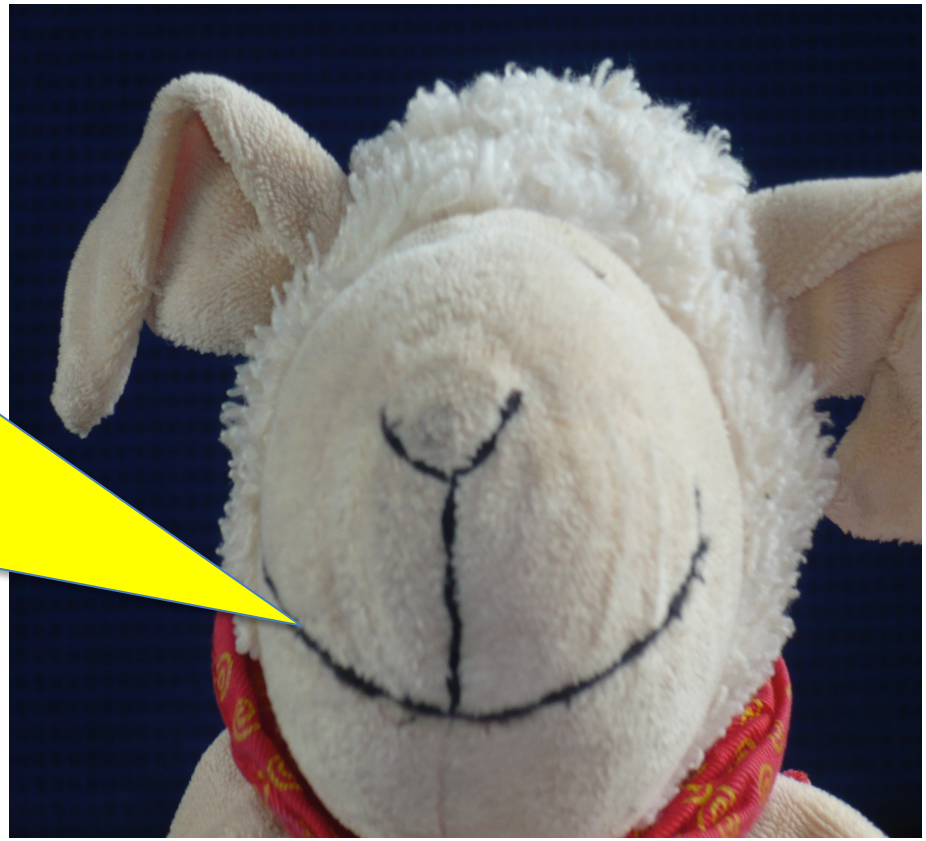
Ab wann gildet das ganze Zeugs denn überhaupt???

Ab dem
25. Mai 2018!



Dann mal los!

Im Einzelnen:



Gegenstand

der EU-Datenschutz-Grundverordnung (DS-GVO) ist nach Artikel 1:

der Schutz

natürlicher Personen bei der Verarbeitung personen-bezogener Daten

und

des freien Verkehrs solcher Daten.

Ziel

der EU-Datenschutz-Grundverordnung (DS-GVO) ist nach Artikel 1:

der Schutz

↓

der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

sachlicher Anwendungsbereich

Die EU-Datenschutz-Grundverordnung gilt nach Artikel 2 für:

die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten

die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen

sachlicher Anwendungsbereich

Die EU-Datenschutz-Grundverordnung gilt nach Artikel 2 für:

die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten

die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen

???

sachlicher Anwendungsbereich

Die EU-Datenschutz-Grundverordnung gilt nach Artikel 2 für:

die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten

die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen

Eine **nicht-automatisierte** Datenverarbeitung liegt vor, wenn die Daten „***manuell***“, d.h. **handschriftlich** oder **maschinenschriftlich** **ohne automatisierte Auswertungsmöglichkeit** verarbeitet werden. Die **DS-GVO** regelt, um eine Gesetzesumgehung zu vermeiden, den Schutz natürlicher Personen **technologieneutral** und erfasst auch die **manuelle Verarbeitung**, **wenn die Daten in einem Dateisystem gespeichert werden sollen**.*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 2 Rdn. 4

sachlicher Anwendungsbereich

Die EU-Datenschutz-Grundverordnung gilt nach Artikel 2 nicht für:

die **Verarbeitung personenbezogener Daten**

- im Rahmen einer Tätigkeit die **nicht** in **den Anwendungsbereich des Unionsrechts** fällt,
- durch die **Mitgliedsstaaten** im Rahmen von Tätigkeiten, die in den Anwendungsbereich von **Titel V Kapitel 2*** fallen,
- durch natürliche Personen zur Ausübung **ausschließlich persönlicher** oder **familiärer** Tätigkeiten,
- durch die zuständigen Behörden zum Zwecke der **Verhütung**, **Ermittlung**, **Aufdeckung** oder **Verfolgung** von **Straftaten** oder der **Strafvollstreckung**, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

*Vertrag über die EUROPÄISCHE UNION (EUV) v. 7.2.1992 (Maastricht) i.d.F. v. 13.12.2007 (Lissabon) Titel V Kapitel 2 „*Besondere Bestimmungen über die gemeinsame Außen- und Sicherheitspolitik*“

räumlicher Anwendungsbereich

Die EU-Datenschutz-Grundverordnung gilt nach Artikel 3 für:

↓

die Verarbeitung personenbezogener Daten

- soweit diese im **Rahmen der Tätigkeiten** einer **Niederlassung eines Verantwortlichen** oder eines **Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung selbst in der Union stattfindet**;
- von betroffenen Personen, die sich **in der Union befinden**, durch einen **nicht in der Union niedergelassenen Verantwortlichen** oder **Auftragsverarbeiter**, wenn die Datenverarbeitung im Zusammenhang damit steht
  - betroffenen Personen **in** der Union **Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist**;
  - **das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt**.
- durch einen **nicht in der Union niedergelassenen Verantwortlichen** an einem Ort, **der aufgrund Völkerrechts dem Recht eines Mitgliedstaates unterliegt**;

- soweit diese im **Rahmen der Tätigkeiten** einer **Niederlassung eines Verantwortlichen** oder eines **Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet**;*

Der Begriff der „***Niederlassung***“ ist hierbei äußerst weit auszulegen. Es genügt bereits für das Vorliegen der Voraussetzungen **eine effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung**. Nach einem Urteil des **EuGH** (**EuGH Urteil v. 01.10.2015 - C 230/14, wiedergegeben in PinG 2016, 21, 22**) ist dieses dahingehend zu interpretieren, **dass bereits jede tatsächliche, wenn auch geringfügige Tätigkeit zum Vorliegen einer Niederlassung führen kann** (im zu beurteilenden Fall konnten der **Vertreter**, das **Postfach** und das **Bankkonto** bereits genügen).*

Das Urteil liegt – worauf Schaffland/Holthaus an gleicher Stelle verweisen – auf einer Linie des Google-Spain-Urteils (**EuGH, Urteil v. 13.05.2014 – C 131/12**). **Es genügt mithin eine inhaltliche Verknüpfung zwischen der Tätigkeit (im Inland) und der eigentlichen Datenverarbeitung in einem anderen Land. Diese ist auch gegeben**, wenn ein Auftragsverarbeiter mit Sitz in einem Drittstaat Daten **im Inland durch eine Person erheben lässt, die ihren Wohnsitz im Inland hat** und **die eigentliche Verarbeitung der personenbezogenen Daten im Ausland, z.B. *Indien* durchführt. Ausreichend ist insoweit bereits schon eine minimale Präsenz!***

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 3 Rdn. 4

- von betroffenen Personen, die sich **in der Union befinden**, durch einen **nicht in der Union niedergelassenen Verantwortlichen** oder **Auftragsverarbeiter**, wenn die Datenverarbeitung im Zusammenhang damit steht
  - betroffenen Personen **in** der Union **Waren oder Dienstleistungen anzubieten**, **unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist**;
  - **das Verhalten betroffener Personen zu beobachten**, **soweit ihr Verhalten in der Union erfolgt**.**

Mit der **1. Alternative** dürften, da es nicht auf Entgeltlichkeit ankommt, wohl insbesondere **auch** die **internationalen Internetkonzerne** erfasst werden können. Insbesondere bedeutet der Begriff „befinden“ nicht, dass der Betroffene seinen **Wohnsitz** in der Union haben muss, es genügt wenn er sich **in der Union aufhält**.*

Mit der **2. Alternative** soll jede Form von **Web Analytics** erfasst werden. Dabei ist es unerheblich, ob die Ergebnisse **wirtschaftlich** (z.B. für Werbung, Markforschung), **wissenschaftlich** oder **zu anderen Zwecken** genutzt werden sollen.**

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 3 Rdn. 6

**Schaffland/Holthaus DS-GVO – Kommentar, Art. 3 Rdn. 6, mwN

EU-Datenschutz-Grundverordnung

Im Rahmen der **DS-GVO** wurden ferner insbesondere die folgenden **Begriffe/ Begriffsbestimmungen** einheitlich festgelegt:

1. „**personenbezogene Daten**“, Art. 4 Nr. 1 DS-GVO
2. „**Verarbeitung**“, Art. Nr. 2 DS-GVO
3. „**Einschränkung der Verarbeitung**“, Art. 4 Nr. 3 DS-GVO
4. „**Profiling**“, Art. 4 Nr. 4 DC-GVO
5. „**Pseudonymisierung**“, Art. 4 Nr. 5 DS-GVO
6. „**Dateisystem**“, Art. 4 Nr. 6 DS-GVO
7. „**Verantwortlicher**“, Art. 4 Nr. 7 DS-GVO
8. „**Auftragsverarbeiter**“, Art. 4 Nr. 8 DS-GVO
9. „**Empfänger**“, Art. 4 Nr. 9 DS-GVO
10. „**Dritter**“, Art. 4 Nr. 10 DS-GVO
11. „**Einwilligung**“, Art. 4 Nr. 11 DS-GVO
12. „**Verletzung des Schutzes personenbezogener Daten**“, Art. 4 Nr. 12 DS-GVO
13. „**genetische Daten**“, Art. 4 Nr. 13 DS-GVO
14. „**biometrische Daten**“, Art. 4 Nr. 14 DS-GVO
15. „**Gesundheitsdaten**“, Art. 4 Nr. 15 DS-GVO

EU-Datenschutz-Grundverordnung

Im Rahmen der **DS-GVO** wurden ferner insbesondere die folgenden **Begriffe/ Begriffsbestimmungen** einheitlich festgelegt:

16. „**Hauptniederlassung**“, Art. 4 Nr. 16 DS-GVO
17. „**Vertreter**“, Art. Nr. 17 DS-GVO
18. „**Unternehmen**“, Art. 4 Nr. 18 DS-GVO
19. „**Unternehmensgruppe**“, Art. 4 Nr. 19 DS-GVO
20. „**verbindliche interne Datenschutzvorschriften**“, Art. 4 Nr. 20 DS-GVO
21. „**Aufsichtsbehörde**“, Art. 4 Nr. 21 DS-GVO
22. „**betroffene Aufsichtsbehörde**“, Art. 4 Nr. 22 DS-GVO
23. „**grenzüberschreitende Verarbeitung**“, Art. 4 Nr. 23 DS-GVO
24. „**maßgeblicher und begründeter Einspruch**“, Art. 4 Nr. 24 DS-GVO
25. „**Dienst der Informationsgesellschaft**“, Art. 4 Nr. 25 DS-GVO
26. „**Internationale Organisation**“, Art. 4 Nr. 26 DS-GVO*

„personenbezogene Daten“, Art. 4 **Nr. 1** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„***personenbezogene Daten***“ alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** **natürliche Person** (im Folgenden „**betroffene Person**“) beziehen;
als **identifizierbar** wird eine natürliche Person angesehen, **die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann**.

„personenbezogene Daten“, Art. 4 **Nr. 1** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„***personenbezogene Daten***“ alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** **natürliche Person** (im Folgenden „**betroffene Person**“) beziehen;
als **identifizierbar** wird eine natürliche Person angesehen, **die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann**.

Wie *Härting** bereits zutreffend ausführt hat, konkretisierte bereits **Art. 2 lit. a** der EG-Datenschutzrichtlinie diese Definition dahingehend, dass alle **die Informationen** über eine **bestimmte** oder **bestimmbare** natürliche Person personenbezogene Daten sind, die Ausdruck ihrer **physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität** sind.
Dabei wird eine Person als **bestimmbar** angesehen, die direkt oder indirekt, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen identifiziert werden kann.

*Härting, Nico – Datenschutz zwischen Transparenz und Einwilligung, Datenschutzbestimmungen bei Facebook, Apple und Google, CR 2011, 169 (170)

Eine Person ist **identifiziert** (nach **BDSG 2003**: „***bestimmt***“), wenn die **gespeicherten Daten mit der Bezeichnung der Person, in der Regel mit ihrem Namen, verknüpft sind** oder **sich aus dem Inhalt oder dem Zusammenhang der Daten der Bezug unmittelbar erstellen lässt**.

Zur Frage, ob ein Datum **identifizierbar** (nach **BDSG 2003**: „***bestimmbar***“) ist, muss mit der Definition des **Anonymisierens** abgeglichen werden.
Eine Person **ist identifizierbar**, **wenn der Aufwand für die (Re-)Identifizierung** für die speichernde Stelle oder einen Dritten **verhältnismäßig** ist.
Ist der Aufwand **unverhältnismäßig**, ist das Datum **anonymisiert**.*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 5 mwN.

„*Verarbeitung*“, Art. 4 **Nr. 2** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Verarbeitung*“ **jeden** **mit** oder **ohne** **Hilfe automatisierter Verfahren** ausgeführten **Vorgang** oder **jede solche Vorgangsreihe** im Zusammenhang mit **personenbezogenen Daten** wie das **Erheben**, das **Erfassen**, die **Organisation**, das **Ordnen**, die **Speicherung**, die **Anpassung** oder **Veränderung**, das **Auslesen**, das **Abfragen**, die **Verwendung**, die **Offenlegung durch Übermittlung**, **Verbreitung** oder eine **andere Form der Bereitstellung**, den **Abgleich** oder die **Verknüpfung**, die **Einschränkung**, das **Löschen** oder die **Vernichtung**.

„*Einschränkung der Verarbeitung*“, Art. 4 **Nr. 3** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Einschränkung der Verarbeitung*“ die **Markierung** gespeicherter **personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken**.

„*Profiling*“, Art. 4 **Nr. 4** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Profiling*“ **jede Art der automatisierten Verarbeitung personenbezogener Daten**, die darin besteht, dass diese personenbezogenen Daten verwendet werden, **um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen**, **zu bewerten**, insbesondere um Aspekte bezüglich **Arbeitsleistung**, **wirtschaftliche Lage**, **Gesundheit**, **persönliche Vorlieben**, **Interessen**, **Zuverlässigkeit**, **Verhalten**, **Aufenthaltsort** oder **Ortswechsel** dieser natürlichen Person **zu analysieren** oder **vorherzusagen**.

„*Pseudonymisierung*“, Art. 4 **Nr. 5** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Pseudonymisierung*" die Verarbeitung **personenbezogener Daten** in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**, sofern diese zusätzlichen Informationen **gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden**.

Einzelangaben bleiben auch dann personenbezogene Daten, wenn sie kodiert sind.
Solche **Pseudonymisierungen** von Daten werden oft vorgenommen, wenn der Inhalt bestimmter Daten

- nur **bestimmten Personen bekannt sein soll** oder
- die Daten „**automationsgerechter**“ verarbeitet werden sollen.

So handelt es sich z.B. bei den Daten, die von der Versicherungswirtschaft an das von einer Drittfirma betriebene Hinweis- und Informationssystem („***HIS***“) gemeldet werden, um **pseudonymisierte Daten**, weil sich aus den Fahrzeugdaten in Kombination mit dem Datum des Versicherungsfalls Rückschlüsse ziehen lassen, wer zum Zeitpunkt des Unfalls Eigentümer des Fahrzeugs war und wie der Schaden reguliert wurde.*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 27, 29.

„*Dateisystem*“, Art. 4 **Nr. 6** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Dateisystem*“ **jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind**, unabhängig davon, ob diese Sammlung **zentral**, **dezentral** oder **nach funktionalen** oder **geografischen Gesichtspunkten** geordnet geführt wird.

„*Verantwortlicher*“, Art. 4 **Nr. 7** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Verantwortlicher*“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet**; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

„*Auftragsverarbeiter*“, Art. 4 **Nr. 8** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Auftragsverarbeiter*“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die **personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet**;

„*Empfänger*“, Art. 4 **Nr. 9** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Empfänger*" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **der personenbezogene Daten offengelegt werden**, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.
Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

„*Dritter*“, Art. 4 **Nr. 10** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Dritter*" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **außer** der **betroffenen Person**, dem **Verantwortlichen**, dem **Auftragsverarbeiter** und den **Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten**.

„*Einwilligung*“, Art. 4 **Nr. 11** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Einwilligung*" der betroffenen Person **jede**

- **freiwillig für den bestimmten Fall,**
- **in informierter Weise und**
- **unmissverständlich**

abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, **dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist**.

„*Verletzung des Schutzes personenbezogener Daten*“, Art. 4 **Nr. 12** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Verletzung des Schutzes personenbezogener Daten*“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig,

- zur **Vernichtung**,
- zum **Verlust**, zur **Veränderung**, oder
- zur **unbefugten Offenlegung von** beziehungsweise zum **unbefugten Zugang zu**

personenbezogenen Daten führt, die **übermittelt**, **gespeichert** oder **auf sonstige Weise verarbeitet** wurden.

„*genetische Daten*“, Art. 4 **Nr. 13** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*genetische Daten*“ **personenbezogene Daten** zu den **ererbten** oder **erworbenen genetischen Eigenschaften** einer natürlichen Person, die **eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern** und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

„*biometrische Daten*“, Art. 4 **Nr. 14** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*biometrische Daten*“ mit speziellen technischen Verfahren gewonnene **personenbezogene Daten** zu den **physischen**, **physiologischen** oder **verhaltenstypischen Merkmalen** einer natürlichen Person, die **die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten**.

„*Gesundheitsdaten*“, Art. 4 **Nr. 15** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Gesundheitsdaten*“ **personenbezogene Daten**, die **sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen** und **aus denen Informationen über deren Gesundheitszustand hervorgehen**.

„*Hauptniederlassung*“, Art. 4 **Nr. 16** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Hauptniederlassung*“

a) im Falle eines **Verantwortlichen** mit Niederlassungen in mehr als einem Mitgliedstaat **den Ort seiner Hauptverwaltung in der Union**, **es sei denn**, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten **werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen** und **diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen**; in diesem Fall **gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung**;

b) im Falle eines **Auftragsverarbeiters** mit Niederlassungen in mehr als einem Mitgliedstaat **den Ort seiner Hauptverwaltung in der Union** oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, **die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden**, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt.

„*Vertreter*“, Art. 4 **Nr. 17** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Vertreter*“ **eine in der Union niedergelassene natürliche oder juristische Person**, die von dem **Verantwortlichen** oder **Auftragsverarbeiter** schriftlich gemäß **Artikel 27** bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter **in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt**.

„*Unternehmen*“, Art. 4 **Nr. 18** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Unternehmen*" **eine natürliche und juristische Person**, **die eine wirtschaftliche Tätigkeit ausübt**, unabhängig von ihrer **Rechtsform**, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

„*Unternehmensgruppe*“, Art. 4 **Nr. 19** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Unternehmensgruppe*" eine **Gruppe**, die aus einem **herrschenden Unternehmen** und den von diesem **abhängigen Unternehmen** besteht.

„*verbindliche interne Datenschutzvorschriften*“, Art. 4 **Nr. 20** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*verbindliche interne Datenschutzvorschriften*" **Maßnahmen zum Schutz personenbezogener Daten**, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener **Verantwortlicher** oder **Auftragsverarbeiter verpflichtet**, im Hinblick auf **Datenübermittlungen** oder eine **Kategorie von Datenübermittlungen personenbezogener Daten** an einen **Verantwortlichen** oder **Auftragsverarbeiter derselben Unternehmensgruppe** oder **derselben Gruppe von Unternehmen**, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.

„*Aufsichtsbehörde*“, Art. 4 **Nr. 21** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Aufsichtsbehörde*“ eine von einem Mitgliedstaat gemäß **Artikel 51** eingerichtete **unabhängige staatliche Stelle**.

„*betroffene Aufsichtsbehörde*“, Art. 4 **Nr. 22** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„**betroffene Aufsichtsbehörde**" eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

a) der **Verantwortliche** oder der **Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist**, (oder)

b) diese **Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann** oder

c) eine **Beschwerde bei dieser Aufsichtsbehörde** eingereicht wurde.

Die Zuständigkeit einer **weiteren Aufsichtsbehörde** kann sich auch daraus ergeben (Buchst. **b**), dass in ihrem räumlichen Zuständigkeitsbereich Betroffene ihren Wohnsitz haben, wenn die Verarbeitung ihrer Daten durch einen **hier nicht ansässsigen Verantwortlichen erhebliche Auswirkungen** hat (z.B. **Facebook**)*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 218.

„*grenzüberschreitende Verarbeitung*“, Art. 4 **Nr. 23** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*grenzüberschreitende Verarbeitung*“ entweder

a) eine Verarbeitung **personenbezogener Daten**, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union **in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist**, oder

b) eine Verarbeitung **personenbezogener Daten**, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, **die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann**.

Buchstabe **b)** definiert **als grenzüberschreitende Verarbeitung** **auch**, wenn eine einzelne Niederlassung des **Verantwortlichen** oder **Auftragsverarbeiters Daten verarbeitet** und **dies erhebliche Auswirkungen auf betroffene Personen in mehr als in einem Land des EU-Binnenmarktes** hat. Hier orientiert sich die grenzüberschreitende Verarbeitung an den Wohnsitzen der betroffenen Personen und damit an den Orten des jeweiligen Leistungsangebotes (sog. „***Marktortprinzip***“)*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 219.

„*maßgeblicher und begründeter Einspruch*“, Art. 4 **Nr. 24** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*maßgeblicher und begründeter Einspruch*“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein **Verstoß gegen diese Verordnung vorliegt** oder ob **beabsichtigte Maßnahmen** gegen den **Verantwortlichen** oder den **Auftragsverarbeiter im Einklang mit dieser Verordnung stehen**, wobei aus diesem **Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen**.

„*Dienst der Informationsgesellschaft*“, Art. 4 **Nr. 25** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

„*Dienst der Informationsgesellschaft*“ eine **Dienstleistung** im Sinne des **Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates***.

***Richtlinie (EU) 201 5/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABI. L 241 vom 17.9.2015, S. 1)**

Mit der Bezugnahme auf die **EU-Richtlinie** werden die Dienstleistungen erfasst, **die in der Regel gegen Entgelt im Fernabsatz mittels Geräten für die elektronische Verarbeitung von Daten auf individuellen Abruf eines Empfängers erbracht werden**. Ausgegrenzt werden durch den Fernabsatz

- die **elektronische Dienstleistung bei gleichzeitiger Anwesenheit** der Vertragsparteien (**z.B. elektronische Spiele in der Spielhalle**),
- die **nichtelektronischen Dienstleistungen**, die **mithilfe elektronischer Geräte** erbracht werden (**Geldausgabeautomat, Fahrkartenautomat**) und
- der **nicht individuelle Abruf** elektronisch bereitgestellter Dienste (**Fernsehen, Rundfunk**)*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 220.

„*internationale Organisation*“, Art. 4 **Nr. 26** DS-GVO

Im Sinne der Verordnung bezeichnet der **Ausdruck**

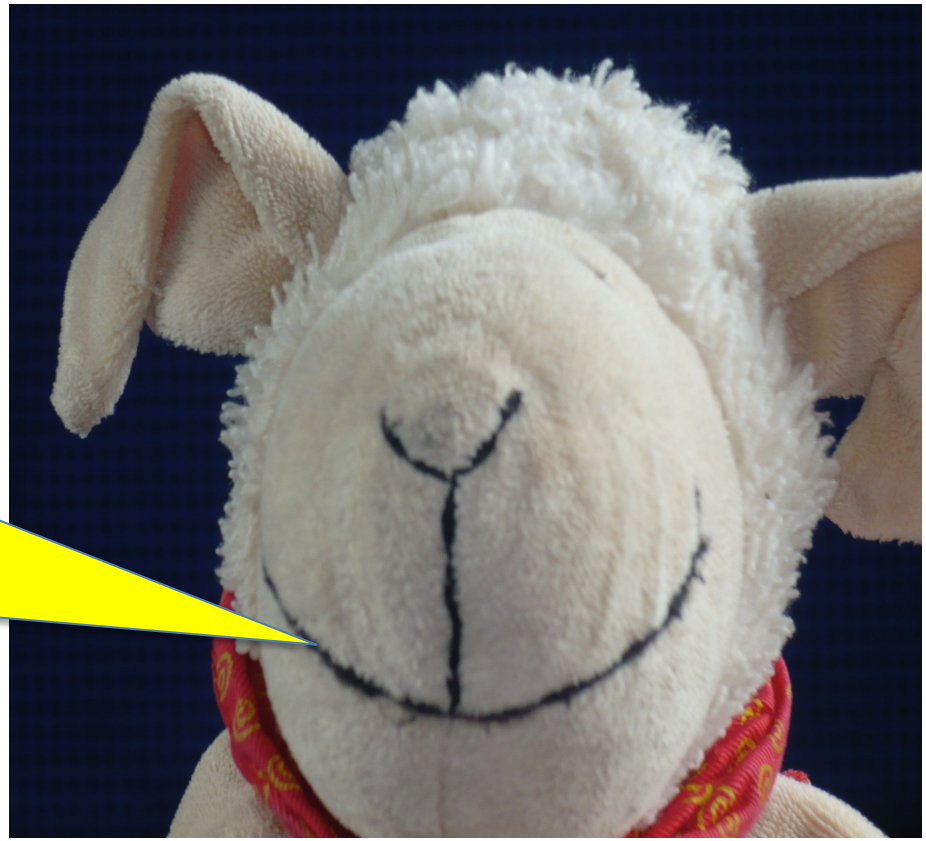
„*internationale Organisation*“ eine **völkerrechtliche Organisation** und **ihre nachgeordneten Stellen** oder **jede sonstige Einrichtung**, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

z.B.:

UNO und ihre Unterorganisationen, NATO, WHO, IWF, Internationale Schiedsgerichte im Rahmen von CETA und TTIP*

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 4 Rdn. 221.

Weiter geht´s!



Soweit ein Unternehmen **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

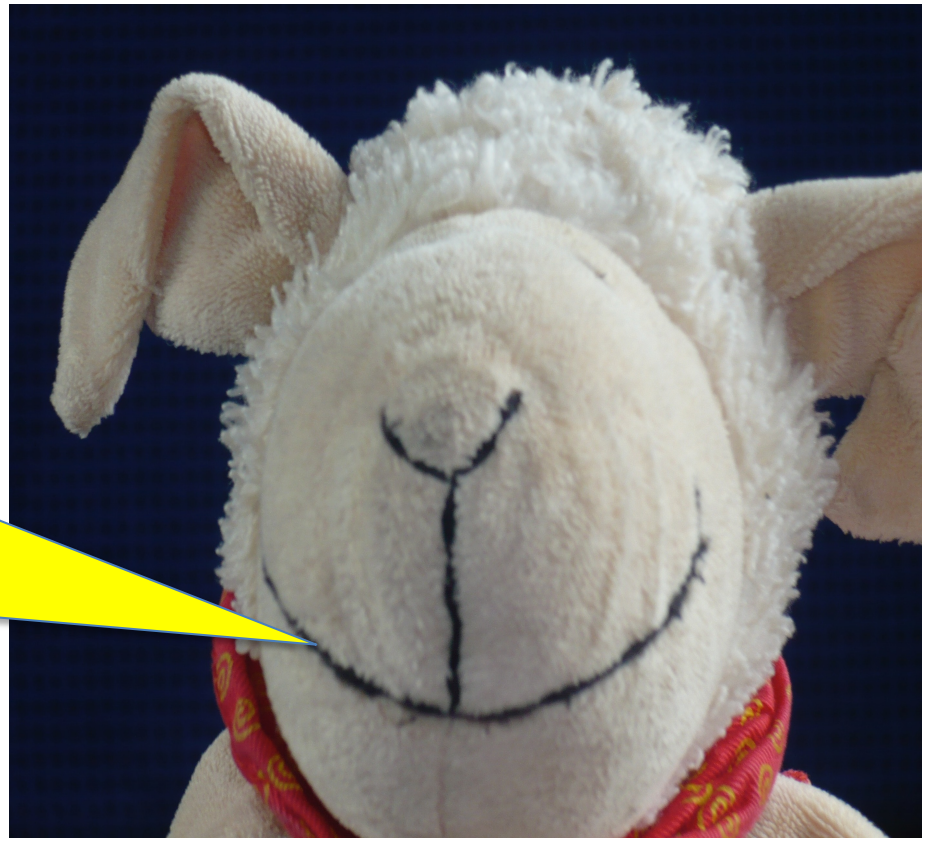
im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

Auf jeden Fall ist es „Verantwortlicher“, i.S.d. Art. 4 Nr. 7 DS-GVO

Sie erinnern sich!?



„***Verantwortlicher***“ im Sinne des **Art. 4 Nr. 7 DS-GVO** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet!**

Also zwar nicht der
„Herr der Ringe“
aber der
„Herr der Daten“!!!

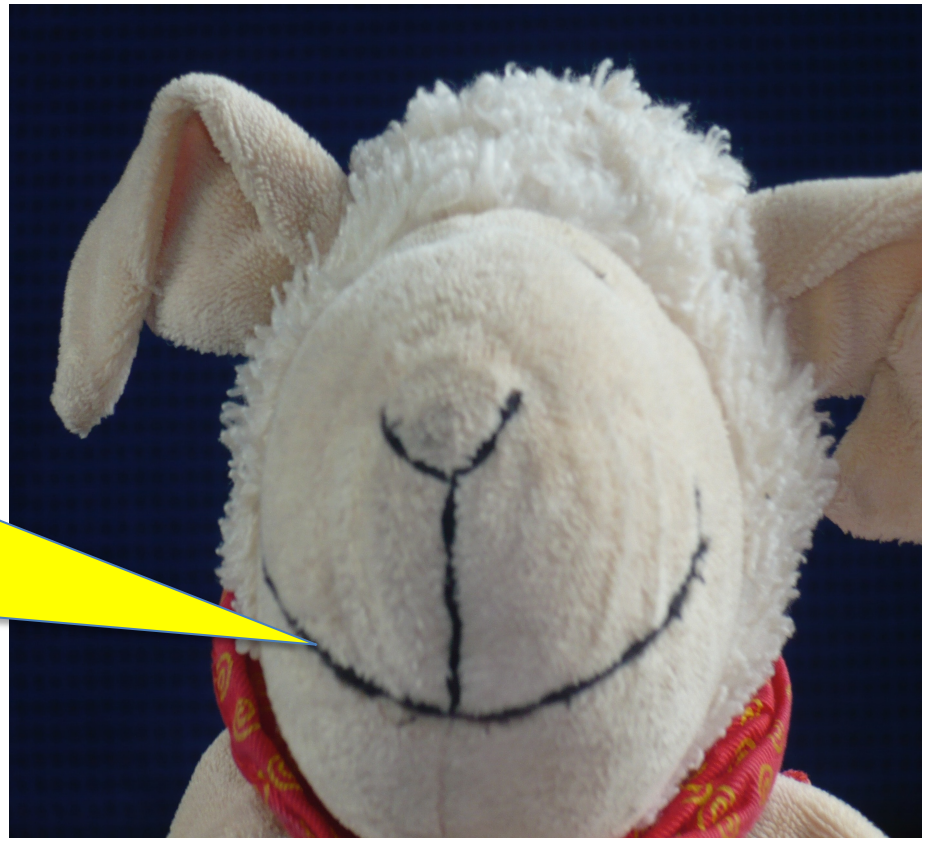
Die sog. „***Auftragsverarbeitung***“ liegt (nur) vor, wenn die personenbezogenen Daten **im Auftrag und auf Weisung** erhoben, verarbeitet oder genutzt werden.

Dies ergibt sich aus **Art. 4 Nr. 8 DS-GVO**, wonach „**Auftragsverarbeiter**“ **eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ist, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet**.

Hierzu gehört insbesondere z.B. der Betrieb eines **Rechenzentrums** in dem Daten für einen Anderen im Auftrag verarbeitet werden.

Hierzu gehören aber wohl auch nach neuem Recht auch **Pflege- und Wartungsarbeiten (§ 11 Abs. 5 BDSG (alt))**

Dazu aber später!



Soweit ein Unternehmen **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

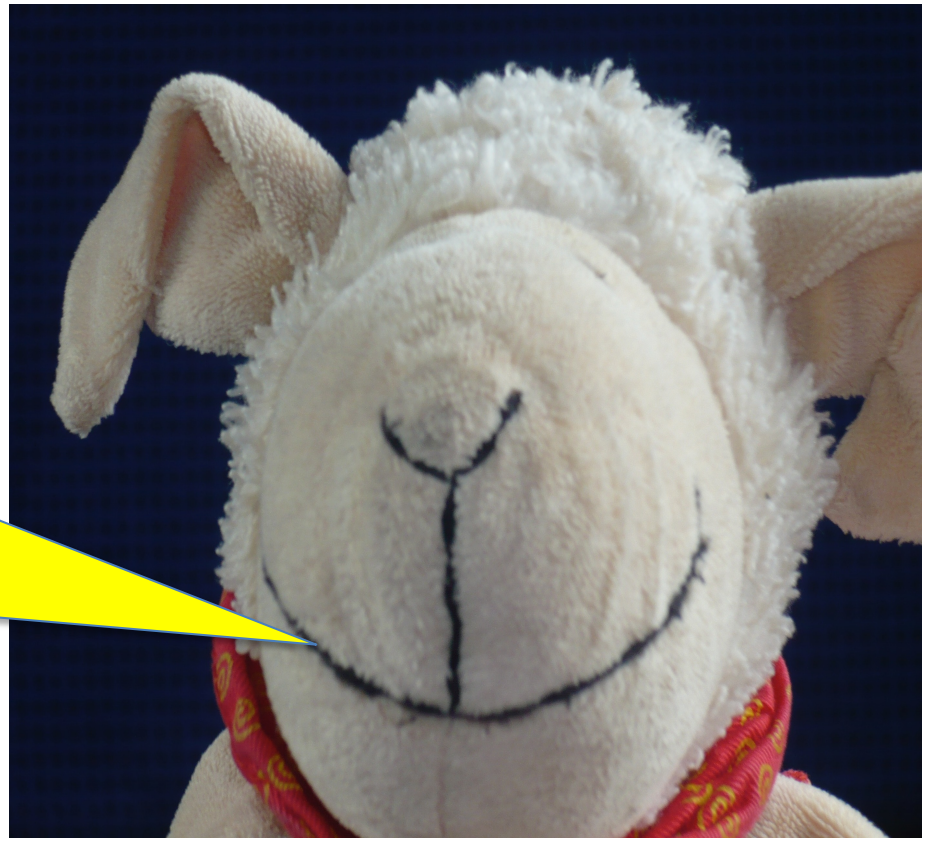
Zu berücksichtigen ist ferner noch ob eine Übermittlung/Verarbeitung in

EU bzw. EWR

„Drittländer“ oder internationale Organisationen

stattfindet

Auch hierzu noch später!



Soweit **spezialgesetzliche Regelungen** in Betracht kommen, sind diese, soweit sie im Einklang mit der Datenschutz-Grundverordnung (**DS-GVO**) stehen, vorrangig vor der **DS-GVO** heranzuziehen. In Betracht kommen hier Vorschriften aus:

dem **Telemediengesetz** (**TMG**)

dem **Telekommunikationsgesetz** (**TKG**)

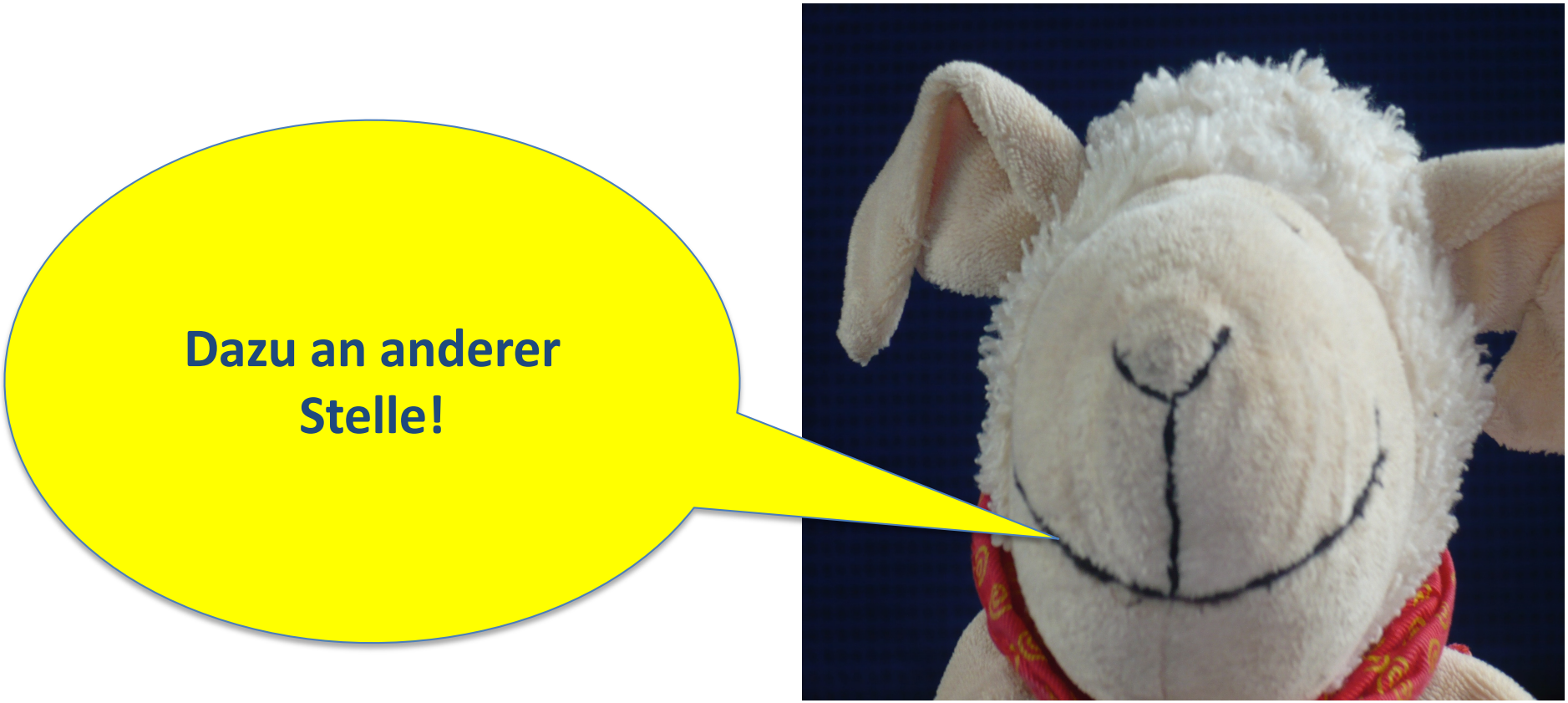
Soweit **spezialgesetzliche Regelungen** in Betracht kommen, sind diese, soweit sie im Einklang mit der Datenschutz-Grundverordnung (**DS-GVO**) stehen, vorrangig vor der **DS-GVO** heranzuziehen. In Betracht kommen hier Vorschriften aus:

dem **Telemediengesetz** (**TMG**)

dem **Telekommunikationsgesetz** (**TKG**)

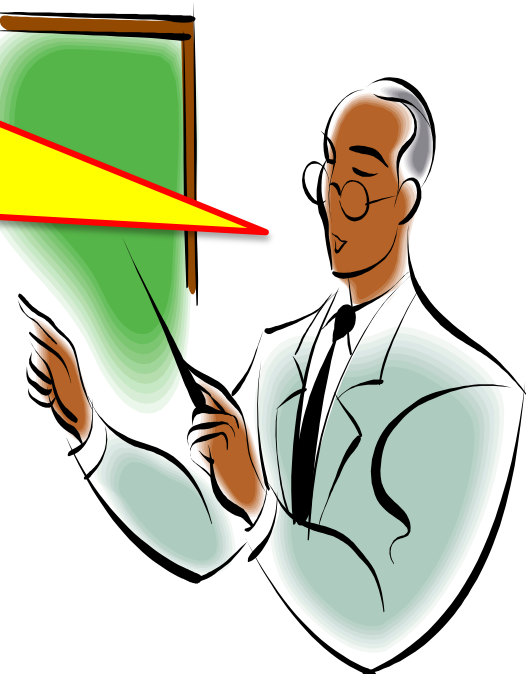
Oder seit dem 01.12.2021 jetzt neu im „*TTDSG*“

Telekommunikations- und Telemedien-Datenschutzgesetz


Dazu an anderer Stelle!

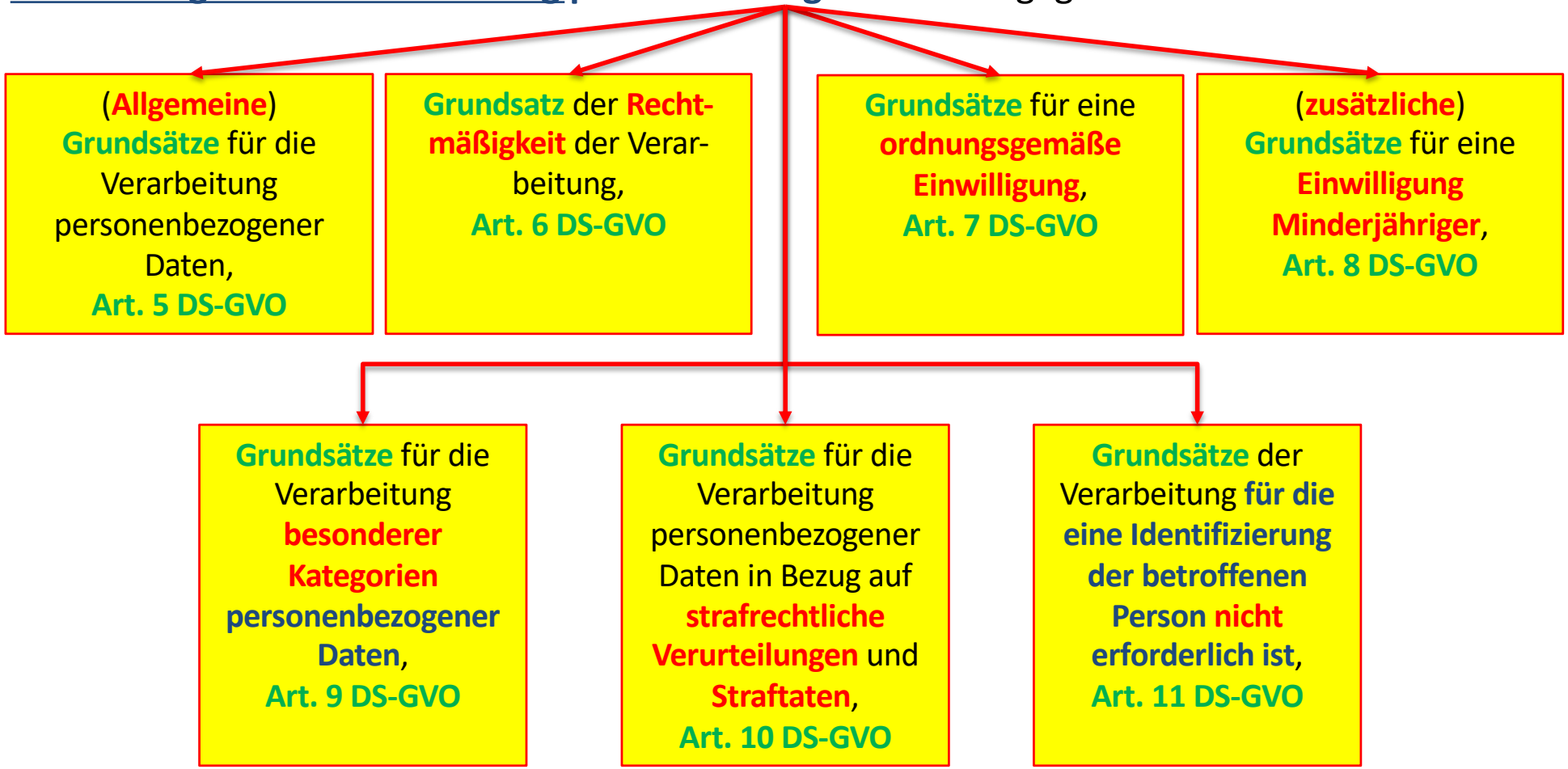
Grundsätze bei der Verarbeitung personenbezogener Daten

Die **DS-GVO** stellt hinsichtlich **personenbezogener Daten**, ähnlich wie bisher bereits auch in der **Richtlinie** und dem **BDSG** enthalten, bestimmte **Grundsätze** auf, **die für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gegeben sein müssen**:

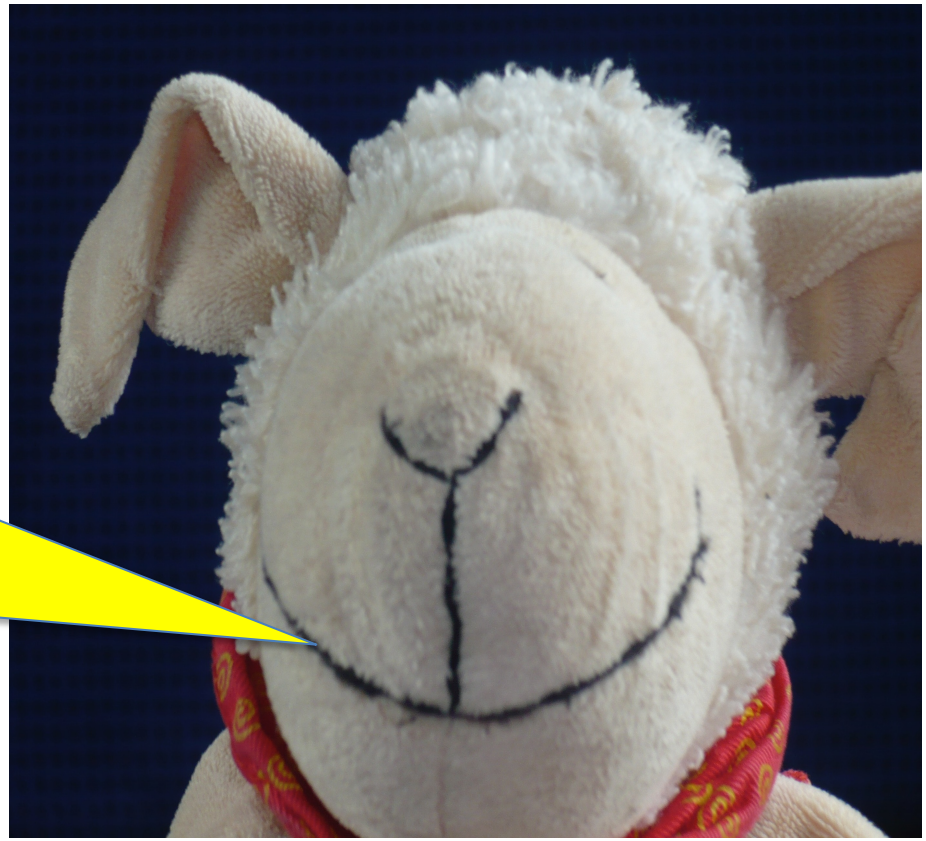


Grundsätze bei der Verarbeitung personenbezogener Daten

Die **DS-GVO** selbst stellt hinsichtlich personenbezogener Daten, ähnlich wie bisher bereits auch in der **Richtlinie** und dem **BDSG** enthalten, bestimmte **Grundsätze** auf, die für eine **Rechtmäßigkeit der Verarbeitung personenbezogener Daten** gegeben sein müssen:



Dann dazu mal im Einzelnen!

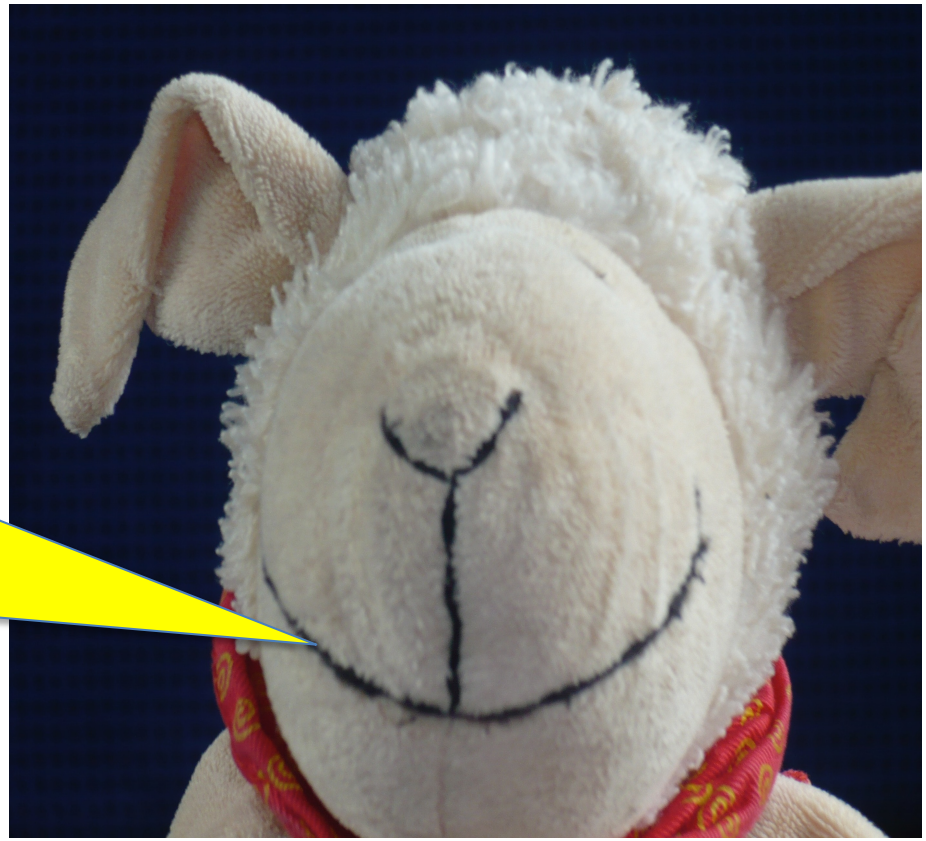


Die (Allgemeinen) Grundsätze sind in der DS-GVO in Art. 5 umgesetzt worden.
Folgende allgemeine Grundsätze sind zu beachten:

Grundsatz der rechtmäßigen, transparenten Verarbeitung unter Beachtung von Treu und Glauben

- Grundsatz der Zweckbindung
- Grundsatz der Datenminimierung
- Grundsatz der Richtigkeit
- Grundsatz der Speicherbegrenzung
- Grundsatz der Integrität und Vertraulichkeit
- Grundsatz der Rechenschaftspflicht

Weiter geht´s!



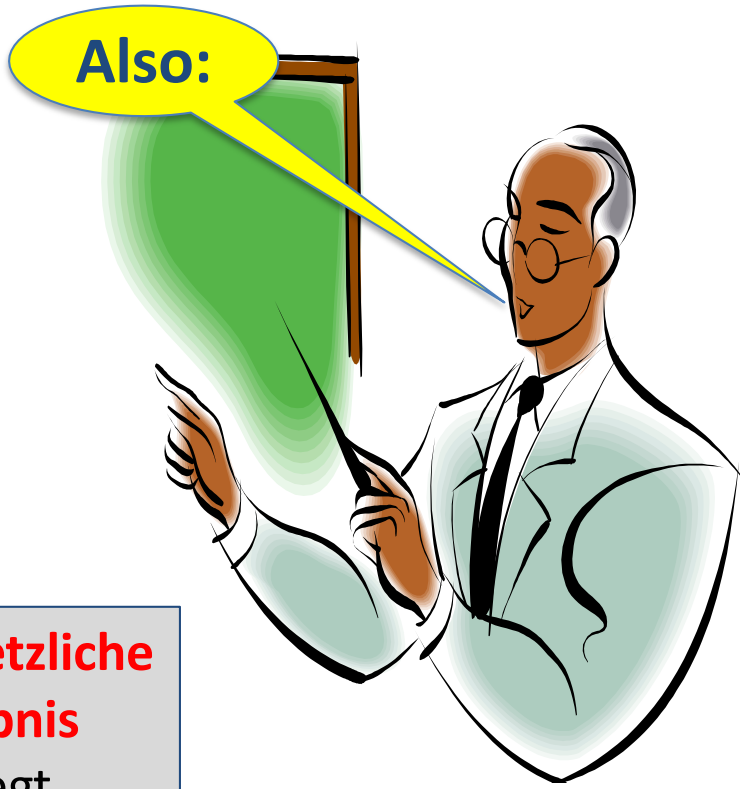
Grundsatz der **Rechtmäßigkeit** der Verarbeitung personenbezogener Daten ist in **Art. 6 DS-GVO** umgesetzt worden.

Das europäische Datenschutzrecht beruht, wie auch das (bisherige) deutsche Datenschutzrecht, auf dem sog.

„**Verbotsprinzip mit Erlaubnisvorbehalt**“,

d.h. es ist grundsätzlich jegliche Verarbeitung personenbezogener Daten **verboten**, wenn sie **nicht** – durch **Gesetz** oder **Einwilligung** bzw. auf Grund wirksamer vertraglicher Vereinbarung – **ausdrücklich erlaubt ist**.

*Das **Erheben**, **Verarbeiten** und **Nutzen** von **personenbezogener Daten** (**Art. 4 Nr. 1 DS-GVO**) für eigene Geschäftszwecke **ist damit grundsätzlich (nur) zulässig**:*

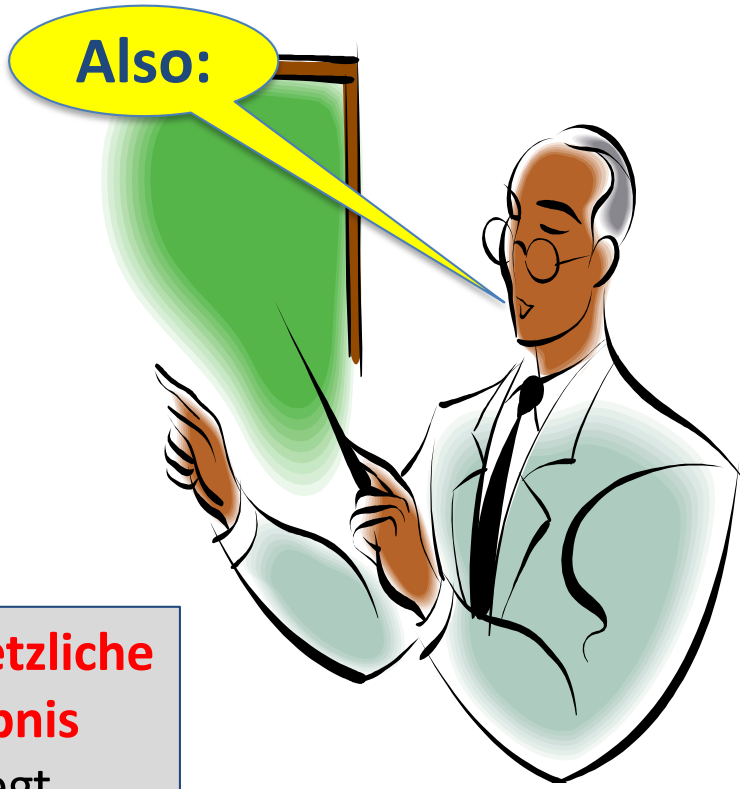


*soweit der Betroffene nach Maßgabe der **Art. 6 und 8 DS-GVO eingewilligt hat***

oder

eine **gesetzliche Erlaubnis** vorliegt.

*Das **Erheben**, **Verarbeiten** und **Nutzen** von **personenbezogener Daten** (**Art. 4 Nr. 1 DS-GVO**) für eigene Geschäftszwecke **ist damit grundsätzlich (nur) zulässig**:*



*soweit der Betroffene nach Maßgabe der **Art. 6 und 8 DS-GVO eingewilligt hat***

oder

eine **gesetzliche Erlaubnis** vorliegt.

Art. 6 DS-VGO enthält eine Auflistung von **gesetzlichen Erlaubnissen**. Das **Erheben, Verarbeiten** und **Nutzen** von **personenbezogener Daten ist insbesondere zulässig soweit**:

- die Verarbeitung für die **Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist,** oder zur **Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen erforderlich ist**;
- die Verarbeitung **zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt**;
- die Verarbeitung **zum Schutz lebenswichtiger Interessen** der **betroffenen Person** oder **einer anderen natürlichen Person erforderlich ist**;
- die Verarbeitung **für die Wahrnehmung einer Aufgabe erforderlich ist, die dem Verantwortlichen übertragen wurde, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt**;
- die Verarbeitung **zur Wahrung der berechtigten Interessen des Verantwortlichen** oder **eines Dritten erforderlich ist**, sofern **nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen**.

Art. 6 DS-VGO enthält eine Auflistung von **gesetzlichen Erlaubnissen**. Das **Erheben, V… …ten ist insbesondere zulässig soweit:**

Eine gesetzliche Erlaubnis ergibt sich also insbesondere für

- **die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist**

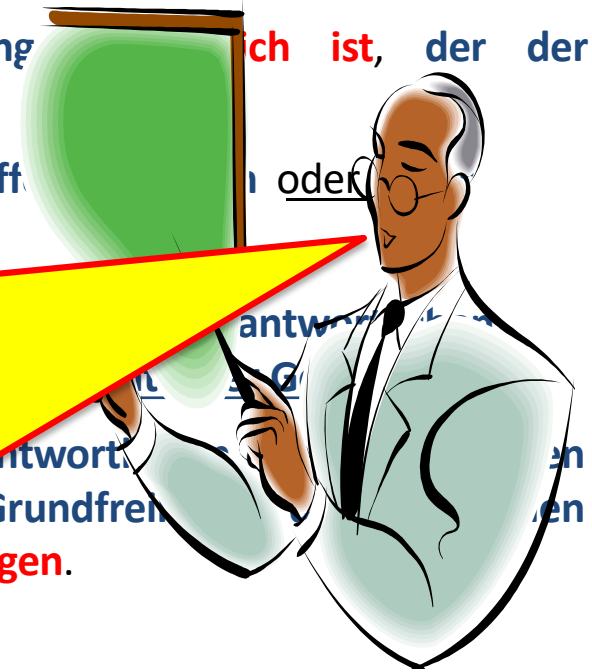
oder

- **zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen!**

…ertragspartei die betroffene Person ist,
… auf Anfrage der betroffenen Person

…pflichtung … ich ist, der der

…er betroff… …n oder



…antw… …G…

…ntwort… …en
…and Grundfrei… …en
…überwiegen.

Art. 6 DS-VGO enthält eine Auflistung von **gesetzlichen Erlaubnissen**. Das **Erheben**, **V**…**en ist insbesondere zulässig soweit**:

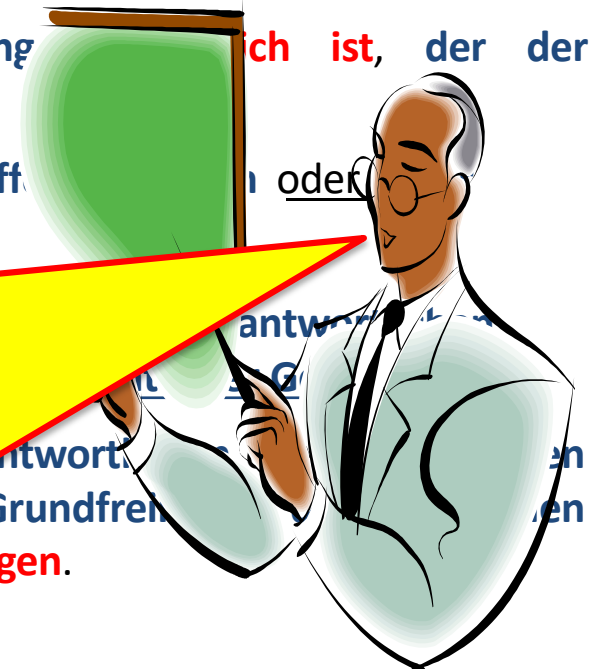
…ertragspartei die betroffene Person ist,
… auf Anfrage der betroffenen Person

…pflichtung …ich ist, der der

…er betroff… …n oder

…antw… …G…

…ntwort… …n
…und Grundfrei… …en
…überwiegen.



Weggefallen ist in diesem Zusammenhang aber das sog. „*Listenprivileg*“ des § 28 Abs. 3 BDSG!

Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung war zulässig:

gemäß § 28 Abs. 3 S. 2 BDSG wenn es sich um **listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelte**, die sich auf die **Zugehörigkeit des Betroffenen zu dieser Personengruppe**, seine **Berufs-, Branchen-** oder **Geschäftsbezeichnung**, seinen **Titel**, **akademischen Grad**, seine **Anschrift** und sein **Geburtsjahr** beschränkten **und** die **Verarbeitung oder Nutzung erforderlich waren,**

für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit **beim Betroffenen** nach Absatz 1 Satz 1 Nummer 1 oder **aus allgemein zugänglichen Adress-, Rufnummern-, Branchen oder vergleichbaren Verzeichnissen erhoben hatte, § 28 Abs. 3 S. 2, 1. Alt. BDSG**,

für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift, § 28 Abs. 3 S. 2, 2. Alt. BDSG oder

für Zwecke der Werbung für Spenden, § 28 Abs. 3 S. 2, 3 Alt. BDSG.

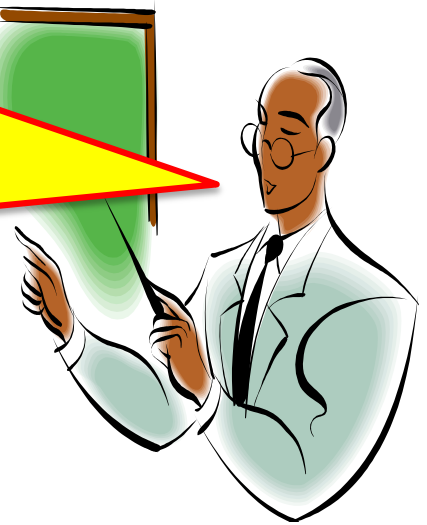
Die **Verarbeitung** oder **Nutzung** personenbezogener Daten für Zwecke

sammengefasste Daten über Angehörige einer
nen zu dieser Personengruppe, seine **Berufs-**,
Grad, seine **Anschrift** und sein **Geburtsjahr**

der Werbung im
die berufliche
es Betroffenen
iner beruflichen
Abs. 3 S. 2,

für Zwecke der Werbung für Spenden, § 28 Abs. 3 S. 2, 3 Alt. BDSG.

Hat sich also erledigt!!!



... und Achtung:
Dann gibt's noch den
§ 7 Abs. 2 UWG!!!

§ 7 Abs. 2 UWG

*(2) Eine **unzumutbare Belästigung** ist **stets** anzunehmen*

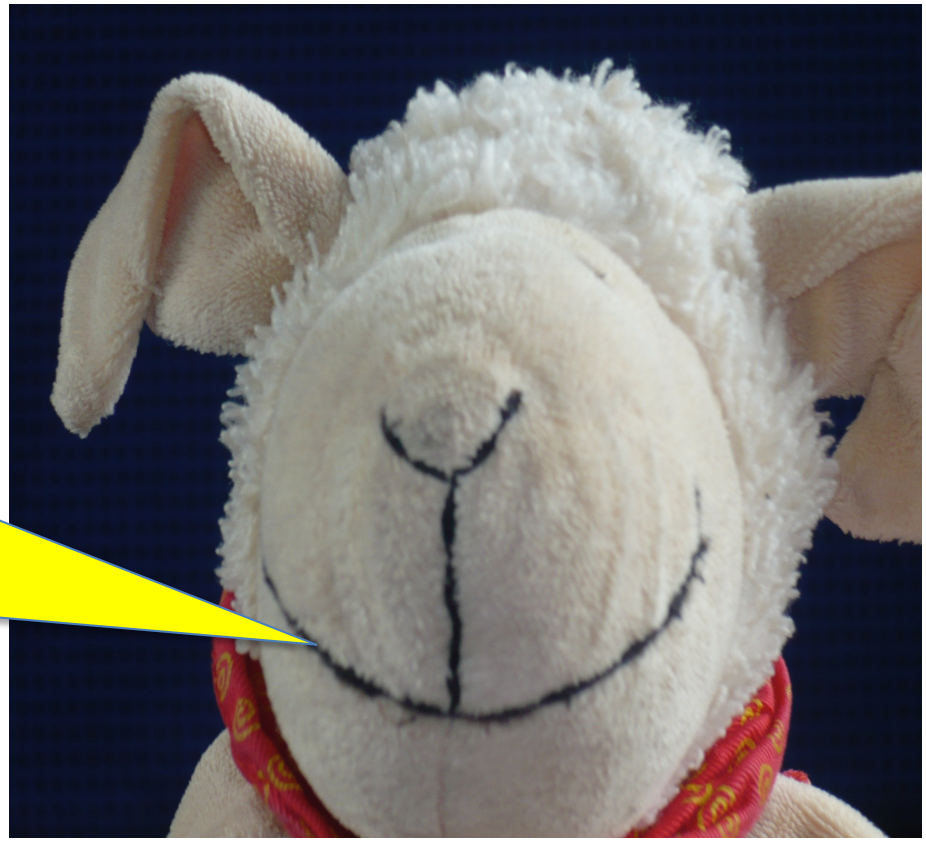
1. bei Werbung unter Verwendung eines in den **Nummern 2 und 3 nicht aufgeführten**, für den **Fernabsatz** geeigneten Mittels der kommerziellen Kommunikation, **durch die ein Verbraucher hartnäckig angesprochen wird, obwohl er dies erkennbar nicht wünscht**;

2. bei Werbung mit einem **Telefonanruf** gegenüber einem **Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder** gegenüber einem **sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung;**

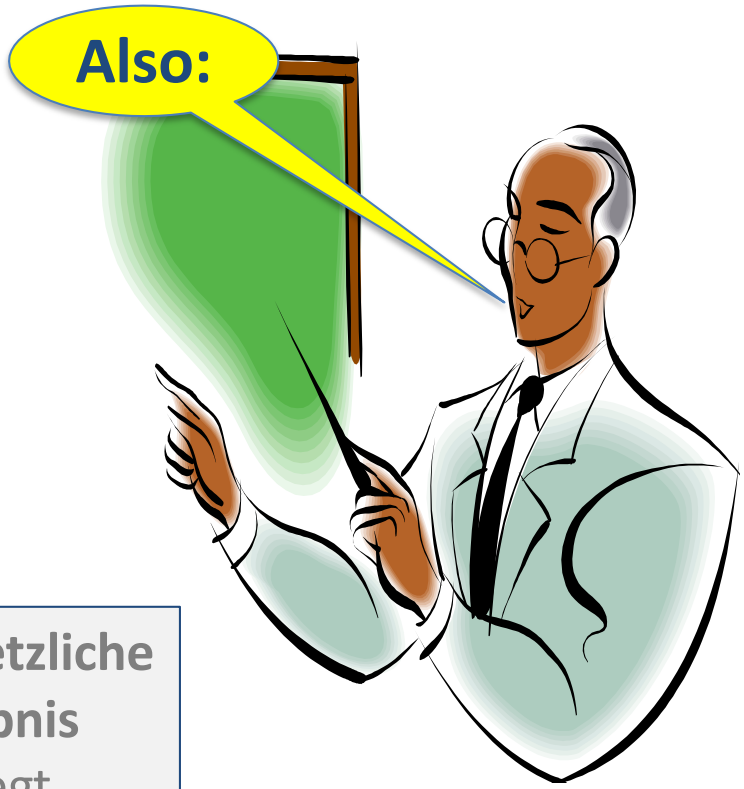
3. bei Werbung unter Verwendung einer **automatischen Anrufmaschine**, eines **Faxgerätes** oder **elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt**, oder

4. bei **sonstigen gravierenden Verstößen** im Sinne von **§ 7 Abs. 2 Nr. 4 a) – c) UWG**

Weiter geht´s!



*Das **Erheben**, **Verarbeiten** und **Nutzen** von **personenbezogener Daten** (**Art. 4 Nr. 1 DS-GVO**) für eigene Geschäftszwecke **ist damit zunächst grundsätzlich (nur) zulässig**:*



*soweit der Betroffene nach Maßgabe der **Art. 6 und 8 DS-GVO eingewilligt hat***

oder

eine **gesetzliche Erlaubnis** vorliegt.

Sie erinnern sich!? Eine „*Einwilligung*“, im Sinne des Art. 4 Nr. 11 DS-GVO ist

jede

- freiwillig für den bestimmten Fall,
- in informierter Weise und
- unmissverständlich

abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

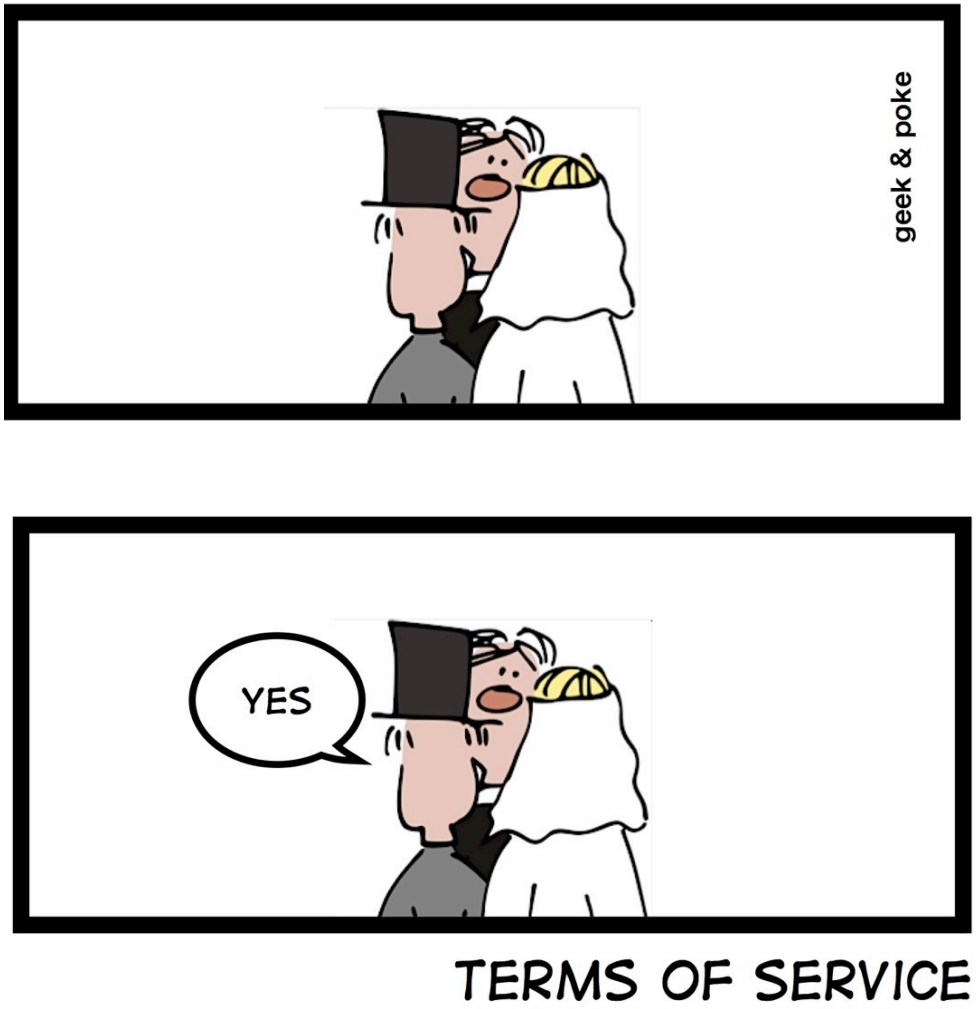
Bedingungen für die Einwilligung der betroffenen Person gem. Art. 6 DS-GVO:

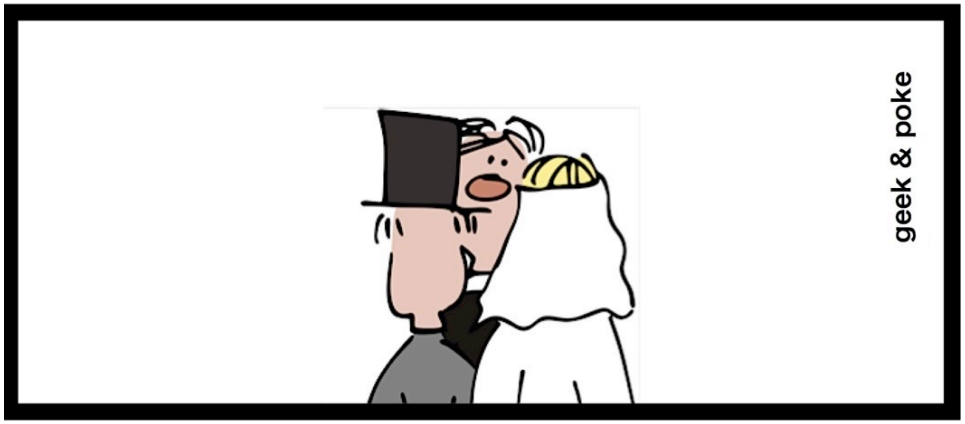
Die **Einwilligung** der betroffenen Person muss also auf seiner **freien Entscheidung** beruhen. Die betroffene Person **muss daher über das, in was er einwilligt, vollständig informiert sein**!

Darüber hinaus darf die Einwilligung **nicht mit sachfremden Umständen** z.B. **nicht zur Erfüllung des Vertrages notwendigen Vorgaben** verknüpft werden.

Schließlich muss die betroffene Person **vor Abgabe der Einwilligung darauf hingewiesen werden, dass sie ihre Einwilligung jederzeit widerrufen kann und muss die Möglichkeit zum Widerruf so einfach wie die Erteilung der Einwilligung ausgestaltet sein**.


SIMPLY EXPLAINED
The iTunes Store, Mac App Store, App Store, and iBookstore services ("Services") accept these forms of payment: credit cards issued by U.S. banks, payments through your PayPal account, iTunes Cards, iTunes Store Gift Certificates, Content Codes, and Allowance Account balances. If a credit card or your PayPal account is being used for a transaction, Apple may obtain preapproval for an amount up to the amount of the order. Billing occurs at the time of or shortly after your transaction. If you are using 1-Click purchasing or your PayPal account, your order may be authorized and billed in increments during one purchasing session, so it may appear as multiple orders on your statement. If an iTunes Card, iTunes Store Gift Certificate, or Allowance Account is used for a transaction, the amount is deducted at the time of your transaction. When making purchases, content credits are used first, followed by Gift Certificate, iTunes Card, or Allowance Account credits; your credit card or PayPal account is then charged for any remaining balance.You agree that you will pay for all products you purchase through the Services, and that Apple may charge your credit card or PayPal account for any products purchased and for any additional amounts (including any taxes and late fees, as applicable) that may be accrued by or in connection with your Account. YOU ARE RESPONSIBLE FOR THE TIMELY PAYMENT OF ALL FEES AND FOR PROVIDING APPLE WITH A VALID CREDIT CARD OR PAYPAL ACCOUNT DETAILS FOR PAYMENT OF ALL FEES. All fees will be billed to the credit card or PayPal account you designate during the registration process. If you want to designate a different credit card or if there is a change in your credit card or PayPal account status, you must change your information online in the Account Information section of iTunes; this may temporarily disrupt your access to the Services while Apple verifies your new payment information.Your total price will include the price of the product plus any applicable sales tax; such sales tax is based on the bill-to address and the sales tax rate in effect at the time you download the product. We will charge tax only in states where digital goods are taxable.All sales and rentals of products are final.Prices for products offered via the Services may change at any time, and the Services do not provide price protection or refunds in the event of a price reduction or promotional offering.If a product becomes unavailable following a transaction but prior to download, your sole remedy is a refund. If technical problems prevent or unreasonably delay delivery of your product, your exclusive and sole remedy is either replacement or refund of the price paid, as determined by Apple.1-Click®1-Click is a registered service mark of Amazon.com, Inc., used under license. 1-Click is a convenient feature that allows you to make a purchase from the Services with a single click of your mouse or other input device. When accessing the Services on your computer, 1-Click purchasing may be activated via the dialog that appears when you click a Buy button. (You may reset this selection at any time by clicking Reset Warnings in your Account information). When accessing the Services on your Apple-branded products running iOS such as an iPad, iPod touch, or iPhone ("iOS Device"), 1-Click is activated for each transaction by tapping the button showing the price of the product, which reveals the Buy button. When 1-Click is activated, clicking or tapping the Buy button starts the download immediately and completes your transaction without any further steps.GIFT CERTIFICATES, iTUNES CARDS, ALLOWANCES, AND CONTENT CODESGift Certificates, iTunes Cards, and Allowances are issued and managed by Apple Value Services, LLC ("Issuer").Gift Certificates, iTunes Cards, Content Codes, and Allowances, in addition to unused balances, are not redeemable for cash and cannot be returned for a cash refund (except as required by law); exchanged; resold; used to purchase Gifts, Gift Certificates, or iTunes Cards; used to provide Allowances; used for purchases on the Apple Online Store; or used in Apple Retail Stores. Unused balances are not transferable.Gift Certificates, iTunes Cards, Content Codes, and Allowances purchased in the United States may be redeemed through the Services only in the United States, its territories, and possessions.The Gift Certificate/iTunes Card cash value is 1/10 of one cent.Neither Issuer nor Apple is responsible for lost or stolen Gift Certificates, iTunes Cards, Content Codes, or Allowances. Risk of loss and title for Gift Certificates, iTunes Cards, and Allowances transmitted electronically pass to the purchaser in Virginia upon electronic transmission to the recipient. Risk of loss and title for Content Codes transmitted electronically pass in California upon electronic transmission from Apple; for avoidance of doubt, such recipient may not always be you.Apple reserves the right to close accounts and request alternative forms of payment if a Gift Certificate, iTunes Card, Content Code, or Allowance is fraudulently obtained or used on the Service.APPLE, ISSUER, AND THEIR LICENSEES, AFFILIATES, ?AND LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO GIFT CERTIFICATES, iTUNES CARDS, CONTENT CODES, ALLOWANCES, OR THE iTUNES STORE, APP STORE, MAC APP STORE, OR iBOOKSTORE, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN THE EVENT THAT A GIFT CERTIFICATE, iTUNES CARD, CONTENT CODE, OR ALLOWANCE IS NONFUNCTIONAL, YOUR SOLE REMEDY, AND OUR SOLE LIABILITY, SHALL BE THE REPLACEMENT OF SUCH GIFT CERTIFICATE, iTUNES CARD, CONTENT CODE, OR ALLOWANCE. THESE LIMITATIONS MAY NOT APPLY TO YOU. CERTAIN STATE LAWS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY ALSO HAVE ADDITIONAL RIGHTS.GIFTSGifts purchased from the Services may be purchased only for, and redeemed only by, persons in the United States, its territories, and possessions. Gift recipients must have compatible hardware and parental control settings to utilize some gifts
?

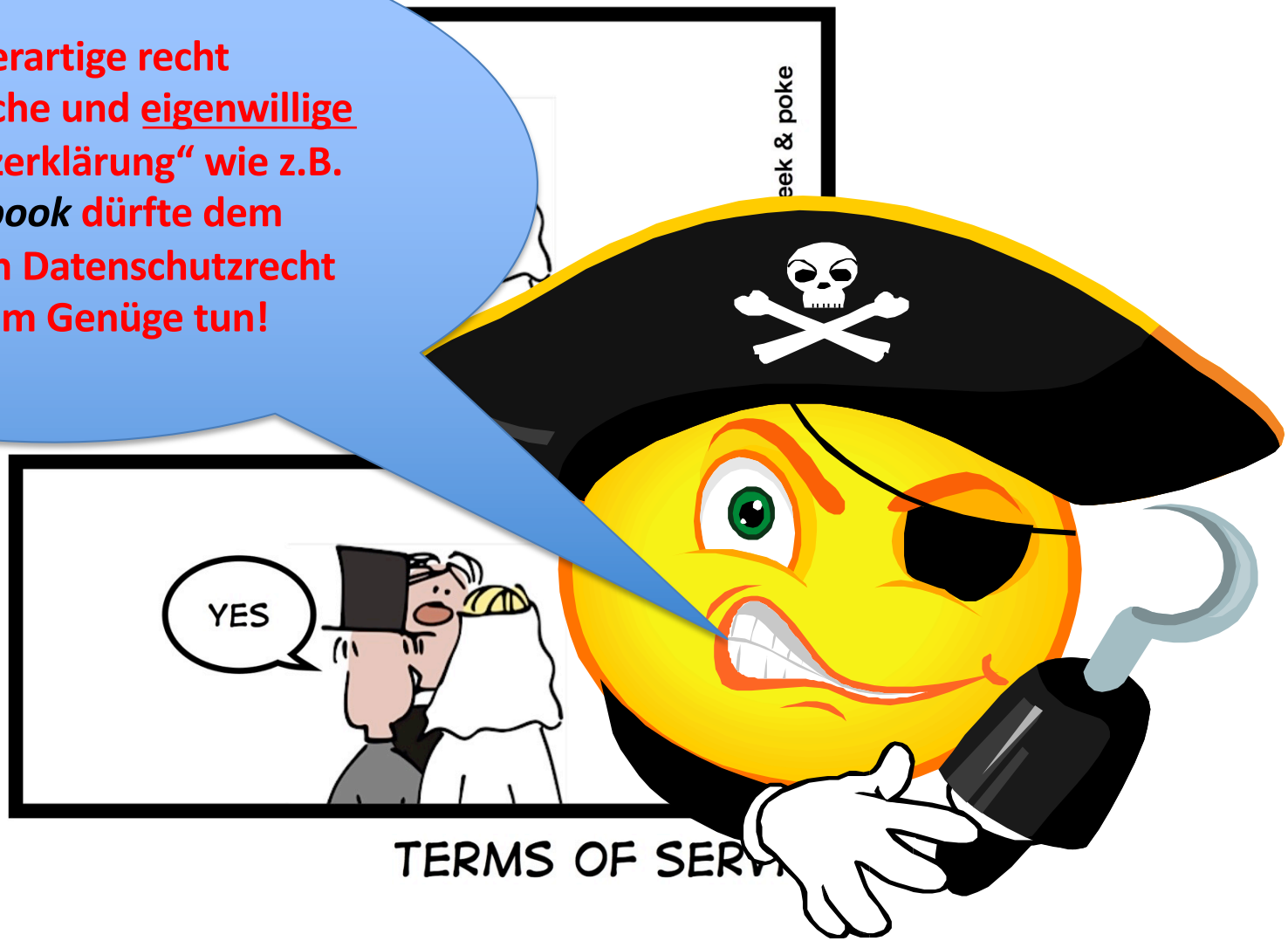

geek & poke
YES
TERMS OF SERVICE


geek & poke


YES

???

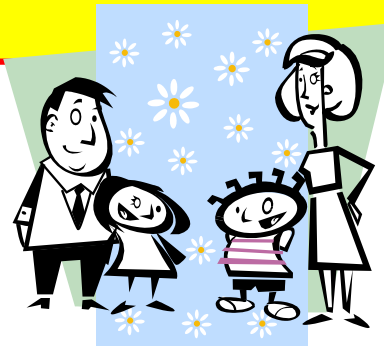
Eine derartige recht unübersichtliche und eigenwillige „Datenschutzerklärung“ wie z.B. von *Facebook* dürfte dem europäischen Datenschutzrecht wohl kaum Genüge tun!



Besonderheiten gelten nach **Art. 8 DS-GVO** für **die Einwilligung von Minderjährigen**

Die Verarbeitung von personenbezogenen Daten eines **Kindes** ist grundsätzlich **nur rechtmäßig**, wenn das Kind das **sechzehnte Lebensjahr vollendet hat**!

Ist dies **nicht** der Fall, so ist die Verarbeitung nur rechtmäßig, sofern durch die **Eltern /Erziehungsberechtigten die Zustimmung erteilt wurde**!

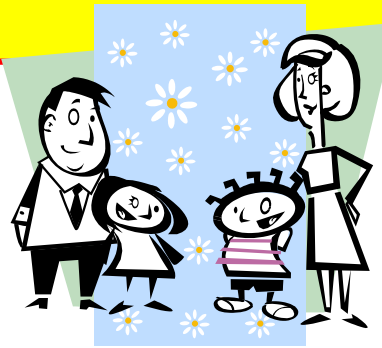


Darüber hinaus ist der **Verantwortliche verpflichtet**, **sich zu vergewissern, dass die Zustimmung der Eltern gegeben ist**!

Besonderheiten gelten nach **Art. 8 DS-GVO** für **die Einwilligung von Minderjährigen**

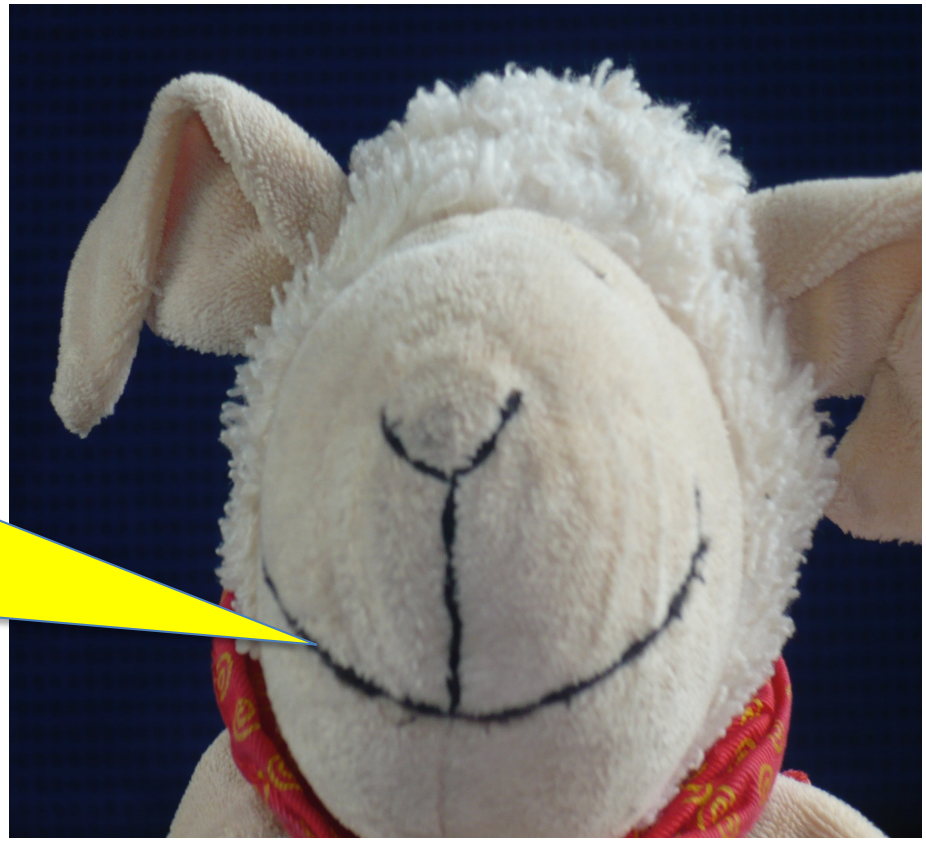
Die Verarbeitung von personenbezogenen Daten eines **Kindes** ist grundsätzlich **nur rechtmäßig**, wenn das Kind das **sechzehnte Lebensjahr vollendet hat**!

Ist dies **nicht** der Fall, so ist die Verarbeitung nur rechtmäßig, sofern durch die **Eltern /Erziehungsberechtigten die Zustimmung erteilt wurde**!



Die Mitgliedsstaaten sind berechtigt das insoweit maßgebliche Lebensalter herabzusetzen, indes darf die Vollendung des dreizehnten Lebensjahres nicht unterschritten werden!

Weiter geht´s!



Grundsätze für die Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 9 DS-GVO

Jede Verarbeitung **personenbezogener Daten**, aus denen

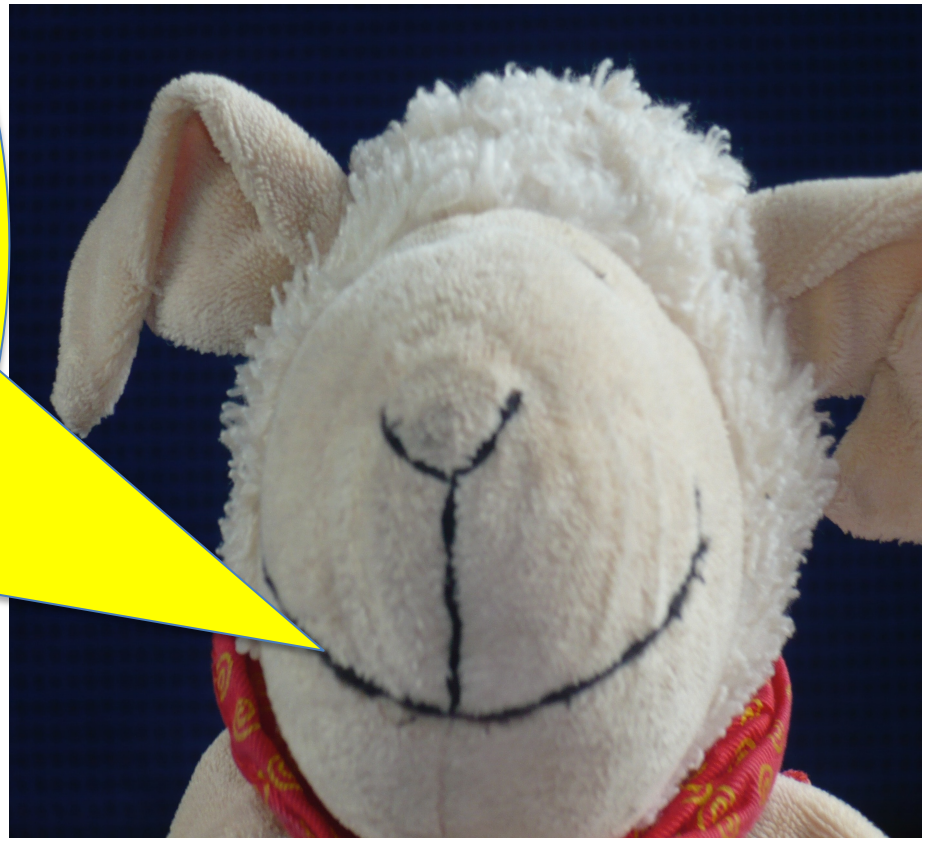
- die **rassische** und **ethnische Herkunft**,
- **politische Meinungen**,
- **religiöse** oder **weltanschauliche Überzeugungen** oder
- die **Gewerkschaftszugehörigkeit**

hervorgehen, sowie

- die Verarbeitung von **genetischen Daten**,
- **biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person**,
- **Gesundheitsdaten** oder
- Daten zum **Sexualleben** oder der **sexuellen Orientierung**

einer **natürlichen Person** ist gem. **Art. 9 Abs. 1 DS-GVO zunächst einmal grundsätzlich untersagt** und wäre damit **rechtswidrig**.

Geht also gar nicht, wenn nicht die besonderen und engen Voraussetzungen des Art. 9 DS-GVO vorliegen!



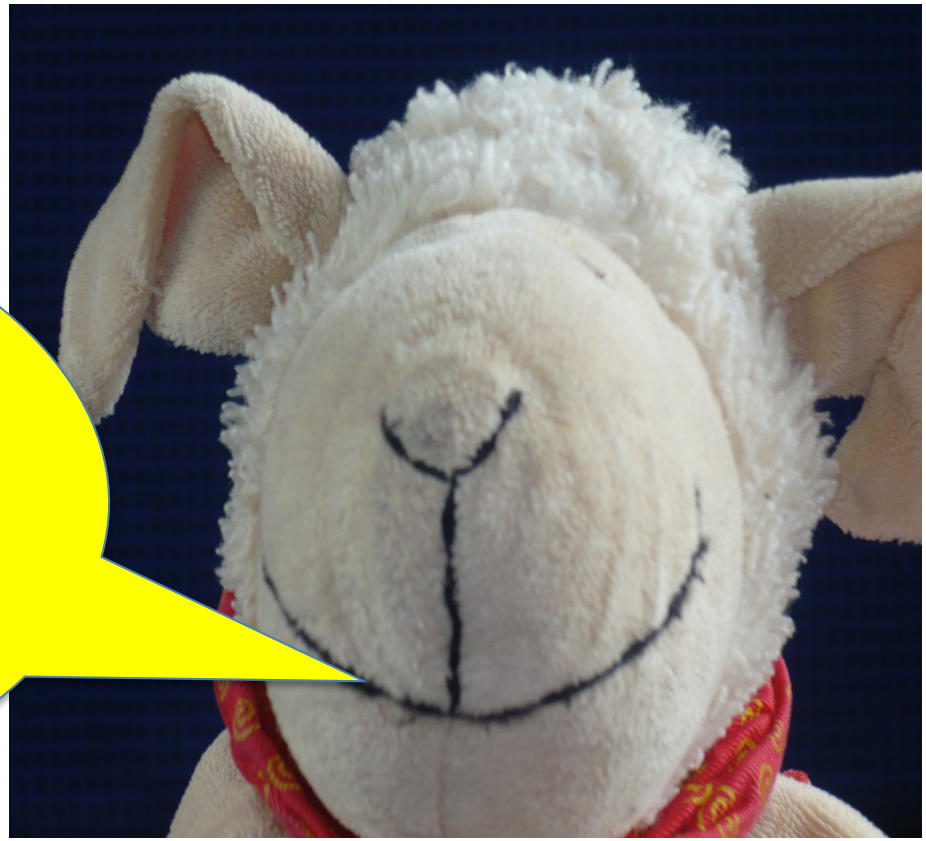
Besondere Arten von personenbezogenen Daten erfordern **darüber hinaus** eine **besonders ausgestaltete Einwilligung!** Es gilt insoweit ergänzend **Art. 9 DS-GVO!**

Der Kunde, Patient, Mandant, Lieferant, Mitarbeiter muss darüber informiert werden,

- welche besonderen personenbezogenen Daten genau der Verantwortliche
- zu welchem konkreten Zweck
- an wen speziell
- warum

weitergeben will.

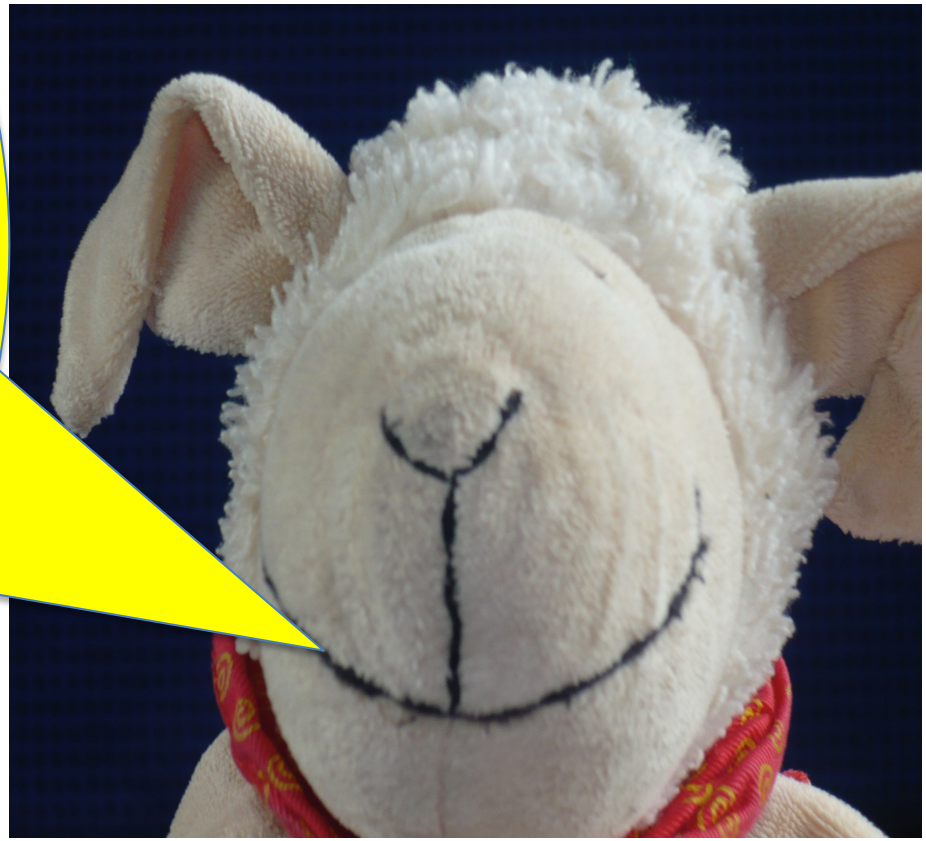
Weiter geht's mit den
„Rechten des Betroffenen“



Die **DS-GVO** sieht ferner zahlreiche **Rechte/Ansprüche** der **betroffenen Person** gegenüber dem **Verantwortlichen** bzw. **Pflichten** des **Verantwortlichen** vor!

- Das Recht auf transparente Information und Kommunikation, Art. 12 DS-GVO
- Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten, Art. 13 DS-GVO
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, Art. 14 DS-GVO
- Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- Recht auf Berichtigung, Art. 16 DS-GVO
- Recht auf Löschung, "Recht auf Vergessenwerden" Art. 17 DS-GVO
- Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO
- Mitteilungspflicht im Zusammenhang mit der Berichtigung/ Löschung/Einschränkung der Verarbeitung, Art. 19 DS-GVO
- Recht auf Datenübertragung, Art. 20 DS-GVO

Im Einzelnen!



Das Recht auf transparente Information und Kommunikation, Art. 12 DS-GVO

Der Verantwortliche hat der betroffenen Person auf deren Antrag, gem. **Art. 12 Abs. 1 DS-GVO** **unverzüglich** und **unentgeltlich** **alle Informationen** zu deren Übermittlung er gem. **Art. 13** und **14 DS-GVO** **verpflichtet ist** und alle **Mitteilungen** gem. **Art. 15 – 22** und **Art. 34 DS-GVO** die er zu erteilen hat, in

- **präziser**,
- **transparenter**,
- **verständlicher** und
- **leicht zugänglicher Form**
- **in einer klaren** und
- **einfachen Sprache**

zu übermitteln!

Wird der Verantwortliche **nicht tätig**, so hat er gem. **Art. 12 Abs. 4 DS-GVO** die betroffene Person **ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrages** über die **Gründe** hierfür und über die Möglichkeit bei der Aufsichtsbehörde **Beschwerde** einzulegen zu unterrichten.

Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten Art. 13 DS-GVO

Soweit personenbezogene Daten **bei** der **betroffenen Person** erhoben werden, teilt der Verantwortliche dieser **zum Zeitpunkt der Erhebung** gem. **Art. 13 Abs. 1 DS-GVO insbesondere** Folgendes mit:

- den **Namen** und die **Kontaktdaten** des **Verantwortlichen**,
- die **Kontaktdaten** des **Datenschutzbeauftragten**,
- die **Zwecke** und die **Rechtsgrundlage** der Verarbeitung
- Im Falle einer Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (**Art. 6 Abs. 1 f**) die **berechtigten Interessen**,
- den **Empfänger** bzw. die **Empfängerkategorien**,
- die **Absicht** und das **Vorliegen der dafür vorgegebenen Voraussetzungen**, die personenbezogenen Daten an ein **Drittland** o. eine **internationale Organisation** zu übermitteln,
- die **Dauer** der beabsichtigten Speicherung,
- das **Bestehen** eines **Rechts** auf **Auskunft**, **Berichtigung** o. **Löschung** o. **Einschränkung der Verarbeitung**,
- das **Bestehen** eines **Widerspruchsrechts** und eines **Beschwerderechts**,
- das **Bestehen** des **Rechts**, die **Einwilligung jederzeit zu widerrufen**.

Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Art. 13 DS-GVO

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese erhoben wurden, so hat er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen Zweck und alle anderen maßgeblichen Informationen im Sinne des Art. 13 DS-GVO zur Verfügung zu stellen!

rhoben werden, teilt der
13 Abs. 1 DS-GVO

- die **Absicht** und das **Vorliegen der dafür vorgegebenen Voraussetzungen**, die p… zogenen D… an ein **Drittland** o. eine **internationale Organisation** zu übermitteln,
- die **Dauer** der beabsichtigten Speicherung,
- das **Bestehen** eines **Rechts** auf **Auskunft**, **Berichtigung** o. **Löschung** o. **Einschränk…**
- das **Bestehen** eines **Widerspruchsrechts** und eines **Beschwerderechts**,
- das **Bestehen** des **Rechts**, die **Einwilligung jederzeit zu widerrufen**.

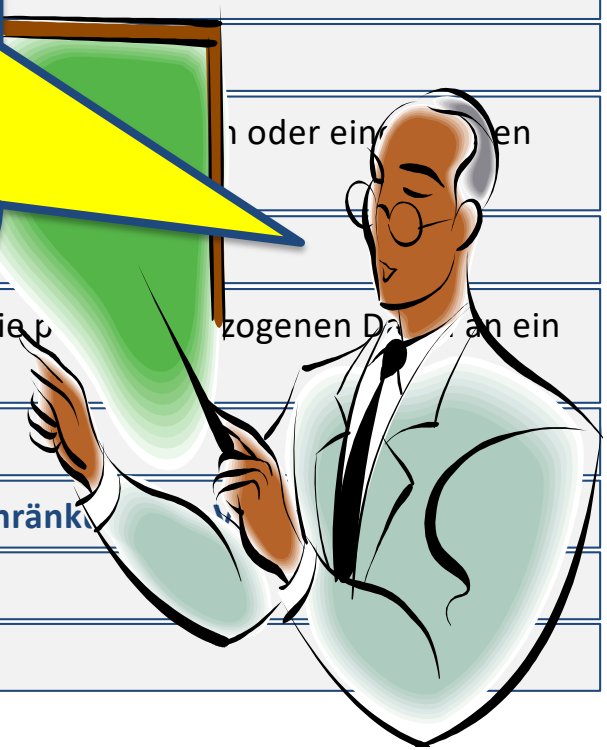
Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Art. 13 DS-GVO

Hier wird nunmehr über die Regelungen der im bislang geltenden BDSG festgelegten *„Zweckbindung“* hinausgehend, im Rahmen der DS-GVO eine Änderung bzw. Erweiterung des Zwecks zugelassen! Der angemessene Ausgleich soll sich aus der insoweit bestehenden Benachrichtigungspflicht und dem Widerspruchsrecht ergeben.

rhoben werden, teilt der
13 Abs. 1 DS-GVO

- die Absicht und das Vorliegen der dafür vorgegebenen Voraussetzungen, die p… zogenen D… an ein Drittland o. eine internationale Organisation zu übermitteln,
- die Dauer der beabsichtigten Speicherung,
- das Bestehen eines Rechts auf Auskunft, Berichtigung o. Löschung o. Einschränk…
- das Bestehen eines Widerspruchsrechts und eines Beschwerderechts,
- das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen.



Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

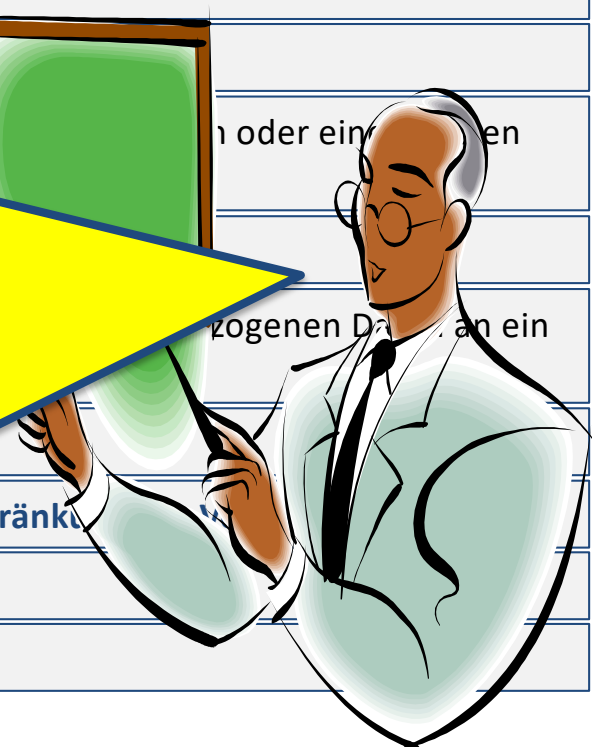
Art. 13 DS-GVO

erhoben werden, teilt der
13 Abs. 1 DS-GVO

Das ist dann aber auf der Grundlage des Art. 6 Abs. 2 DS-GVO in der Bundesrepublik nach heftigen Diskussionen durch § 24 BGSG wieder eingeschränkt worden, der eine Verarbeitung zu einem anderen Zweck als demjenigen, zu dem die Daten erhoben wurden, für nichtöffentliche Stellen nur für zulässig erklärt, wenn

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder
2. sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist und

sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.



- das Bestehen eines Widerspruchsrechts und eines Beschwerderechts,
- das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen.

Informationspflicht wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, Art. 14 DS-GVO

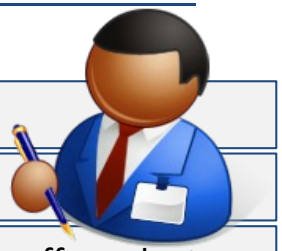
Soweit personenbezogene Daten **nicht bei** der betroffenen Person erhoben werden, teilt der Verantwortliche dieser **zum Zeitpunkt der Erhebung** gem. **Art. 13 Abs. 1 DS-GVO** zum einen all das mit, was er auch im Falle des **Art. 12 DS-GVO** mitzuteilen hat und **darüber hinaus insbesondere noch Folgendes** mit:

- die **Kategorien** der personenbezogenen Daten, die verarbeitet werden sollen,
- aus welcher **Quelle** die personenbezogenen Daten stammen.

*

Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Jede betroffene Person hat das Recht, von dem Verantwortlichen eine **Bestätigung** darüber zu verlangen, **ob sie betreffende personenbezogene Daten verarbeitet werden**; ist **dies der Fall**, so hat sie ein **Recht auf Auskunft** über **diese personenbezogenen Daten** und **insbesondere** auf **folgende Informationen**:



- die **Verarbeitungszwecke**;
- die **Kategorien personenbezogener Daten**, die verarbeitet werden;
- die **Empfänger**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden;
- die **geplante Dauer**, für die die personenbezogenen Daten gespeichert werden;
- das **Bestehen eines Rechts auf Berichtigung** oder **Löschung** der sie betreffenden personenbezogenen Daten oder auf **Einschränkung der Verarbeitung**;
- das **Bestehen eines Widerspruchsrechts und eines Beschwerderechts**;
- wenn die **personenbezogenen Daten nicht bei der betroffenen Person erhoben werden**, **alle verfügbaren Informationen über die Herkunft der Daten**;
- *das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich **Profiling** gemäß **Artikel 22 Absätze 1** und **4** und — zumindest in diesen Fällen — **aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person**.*

*

Recht auf Berichtigung, Art. 16 DS-GVO

Die betroffene Person hat gem. **Art. 16 DS-GVO** ein **Berichtigungsrecht**

Das Recht auf Berichtigung besteht in zweierlei Hinsicht:

Die betroffene Person hat das **Recht**, von dem **Verantwortlichen** unverzüglich die **Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen**.

Die betroffene Person hat das Recht, die **Vervollständigung unvollständiger personenbezogener Daten** — auch mittels einer ergänzenden Erklärung — zu verlangen.

Recht auf Löschung, "Recht auf Vergessenwerden", Art. 17 DS-GVO

Die betroffene Person hat das **Recht**, von dem **Verantwortlichen** zu verlangen, dass **sie betreffende personenbezogene Daten unverzüglich gelöscht werden**, und der Verantwortliche ist **verpflichtet**, **personenbezogene Daten unverzüglich zu löschen, sofern insbesondere einer der folgenden Gründe zutrifft**:

- die personenbezogenen Daten sind für **die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden**, **nicht mehr notwendig**;
- die betroffene Person **widerruft ihre Einwilligung**, auf die sich die Verarbeitung stützte, **und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung**;
- die betroffene Person legt gemäß **Widerspruch** gegen die Verarbeitung ein;
- die personenbezogenen Daten wurden **unrechtmäßig verarbeitet**.

*

Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO

*Die betroffene Person hat das Recht, von dem Verantwortlichen die **Einschränkung** der Verarbeitung zu verlangen, wenn insbesondere eine der folgenden Voraussetzungen gegeben ist:*

- *die **Richtigkeit** der personenbezogenen Daten von der betroffenen Person **bestritten wird**, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;*
- *die Verarbeitung **unrechtmäßig** ist und die betroffene Person die **Löschung** der personenbezogenen Daten **ablehnt** und stattdessen die **Einschränkung der Nutzung** der personenbezogenen Daten **verlangt**;*
- *der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung **nicht länger benötigt**, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** benötigt, oder*
- *die betroffene Person **Widerspruch** gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person **überwiegen**.*

*

Mitteilungspflicht im Zusammenhang mit der Berichtigung/ Löschung/Einschränkung der Verarbeitung, Art. 19 DS-GVO

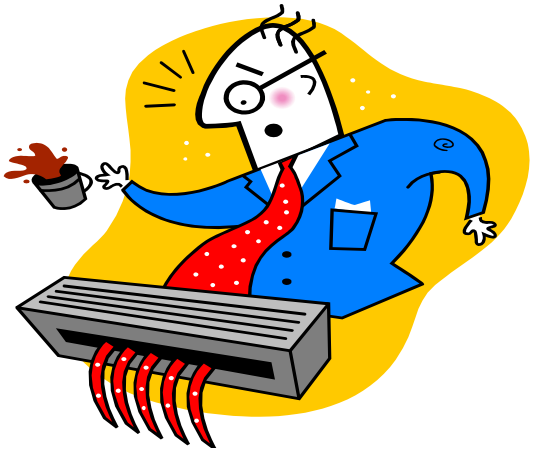
Der Verantwortliche hat gem. **Art. 19 DS-GVO** **allen** **Empfängern gegenüber**, denen **personenbezogene Daten offengelegt wurden**, **jede** **Berichtigung** oder **Löschung** der personenbezogenen Daten oder eine **Einschränkung der Verarbeitung** **mitzuteilen**, es sei denn, dies erweist sich als **unmöglich** oder ist mit einem **unverhältnismäßigen Aufwand** verbunden.

Der Verantwortliche hat ferner die betroffene Person über diese Empfänger zu unterrichten, wenn die betroffene Person dies verlangt.

Recht auf Datenübertragbarkeit, Art. 20 DS-GVO

Die **betroffene Person** hat ferner gem. **Art. 20 DS-GVO** das **Recht**, **die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten**, und **sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln**, sofern:

- die Verarbeitung auf einer **Einwilligung** gemäß **Art. 6 Abs. 1 a / Art. 9 Abs. 2 a DS-GVO** oder auf einem **Vertrag** gemäß **Art. 6 Abs. 1 b DS-GVO** beruht und
- *die **Verarbeitung mithilfe automatisierter Verfahren erfolgt**.*



Wichtig sind dann noch:

- **das Widerspruchsrecht**
- **die Einschränkung von automatisierten Entscheidungen**
- **die Pflicht zur Benachrichtigung von einer Verletzung personenbezogener Daten**

Widerspruchsrecht, Art. 21 DS-GVO

Die **betroffene Person** hat gem. **Art. 21 DS-GVO** das **Recht**, aus Gründen, **die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten**, die aufgrund von **Artikel 6 Absatz 1 Buchstaben e (öffentliches Interesse)** oder **f (berechtigte Interessen des Verantwortlichen)** erfolgt, **Widerspruch einzulegen**; dies gilt auch für ein auf diese Bestimmungen gestütztes **Profiling**.

Automatisierte Entscheidungen im Einzelfall, Art. 22 DS-GVO

Die betroffene Person hat gem. **Art. 22 DS-GVO** das **Recht**, **nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt**, es sei denn:

- *dass die Entscheidung für den **Abschluss** oder die **Erfüllung eines Vertrags** zwischen der betroffenen Person und dem Verantwortlichen **erforderlich ist**,*
- ***dass die Entscheidung aufgrund von Rechtsvorschriften** der **Union** oder der **Mitglied-staaten**, denen der Verantwortliche unterliegt, **zulässig ist** und **diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten***
- *dass die Entscheidung mit **ausdrücklicher Einwilligung der betroffenen Person** erfolgt.*

*

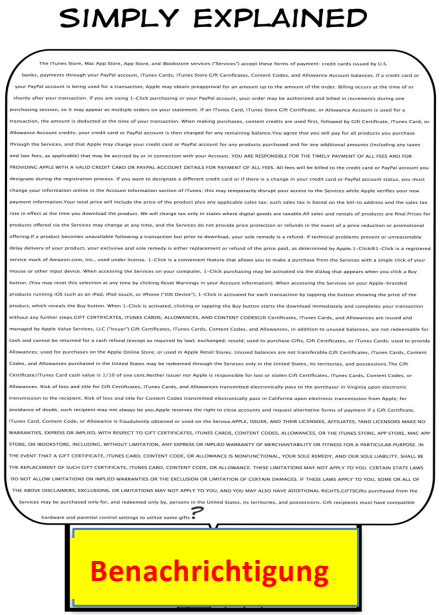
Automatisierte Entscheidungen im Einzelfall, Art. 22 DS-GVO

Die Möglichkeit des Treffens einer automatisierten Entscheidung im Einzelfall erscheint insbesondere bei der 1. Alternative auf den ersten Blick als nicht mit den Grundrechten der Bundesrepublik und den Grundrechten und Grundfreiheiten der EU in Einklang zu bringen zu sein. Zu berücksichtigen ist allerdings, dass es sich insoweit nicht um eine nachteilige Entscheidung, wie z.B. eine Ablehnung, sondern lediglich – wie die Worte „Abschluss“ oder „Erfüllung“ zeigen – um eine zumindest neutrale, wenn nicht sogar positive Entscheidung handelt, so dass unter Berücksichtigung der weiteren dem Betroffenen zustehenden Rechte hinsichtlich der Verfassungsmäßigkeit bzw. den Grundechten und Grundfreiheiten der EU keine Bedenken bestehen dürften.

…cht einer ausschließlich auf …Profiling — beruhenden …che Wirkung entfaltet oder

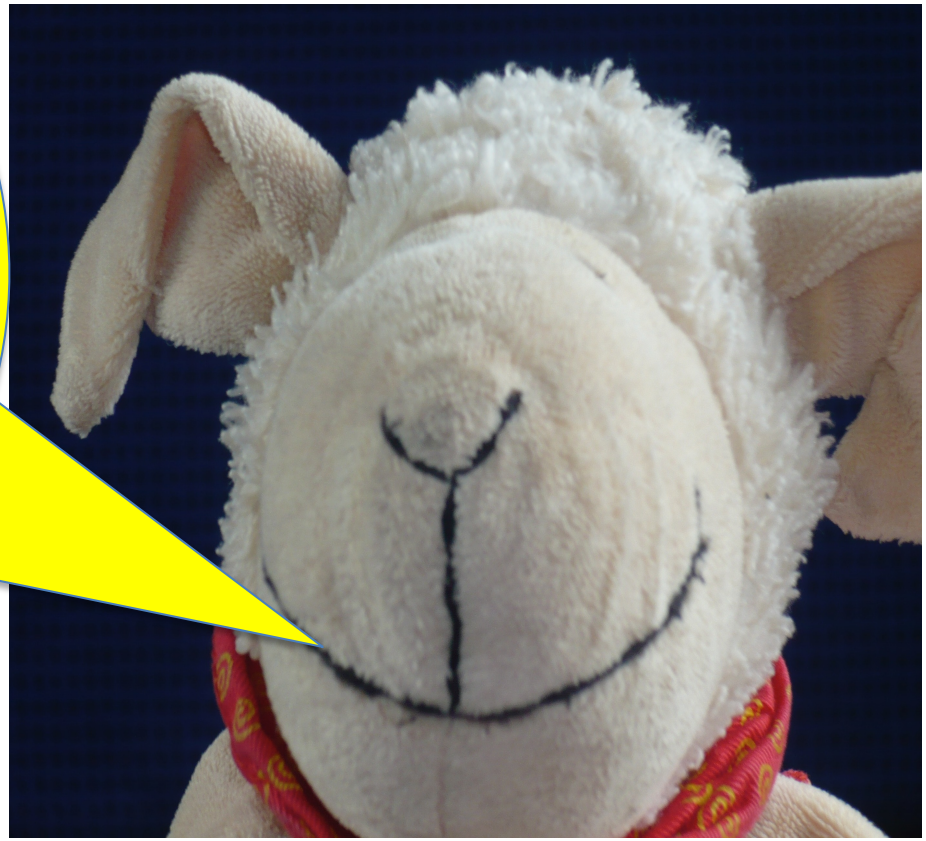
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Art. 34 DS-GVO

Soweit eine **Verletzung der Rechte des Betroffenen erfolgt ist**, die ein **hohes Risiko für seine persönlichen Rechte und Freiheiten** hat, ist der Verantwortliche gem. **Art. 34 DS-GVO verpflichtet** den Betroffenen von der Verletzung des Schutzes personenbezogener Daten **zu benachrichtigen**.



*Die in Absatz 1 genannte Benachrichtigung der betroffenen Person **beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten** und **enthält** zumindest die in **Artikel 33 Absatz 3 Buchstaben b, c** und **d** (z.B. „**was ist passiert**“, „**welche Folgen drohen**“) genannten **Informationen** und **Maßnahmen**.*

Jetzt nochmals zurück zu den handelnden Personen oder „*üblichen Verdächtigen*“!



Soweit ein **Unternehmen** **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

Auf jeden Fall ist es „Verantwortlicher“, i.S.d. Art. 4 Nr. 7 DS-GVO

Soweit ein **Unternehmen** **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

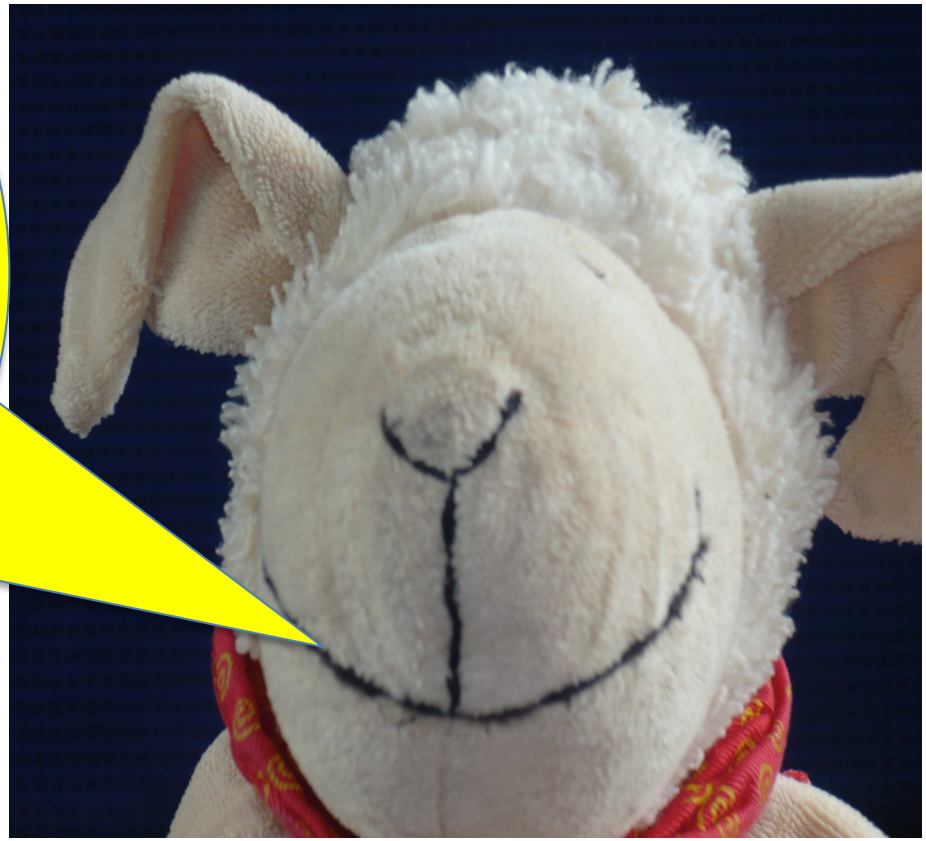
im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

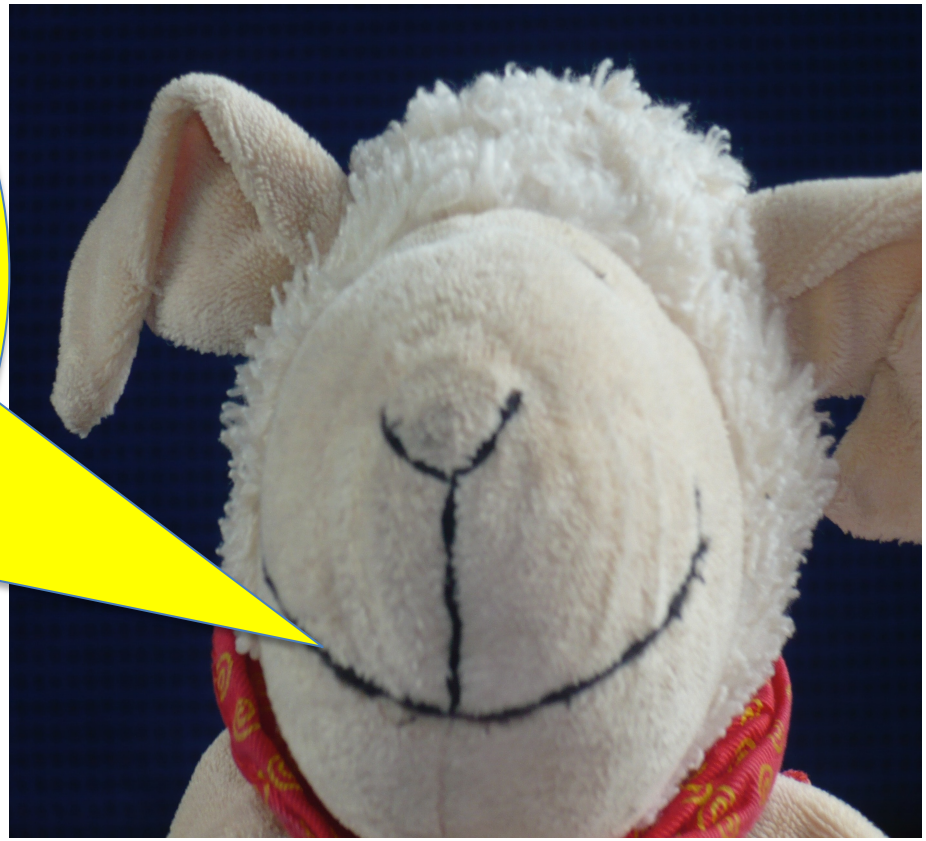
greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

Beiden Beteiligten gemeinsam ist, dass sie (irgendwie) „handeln“!

Auf jeden Fall sind die „Handelnden“ zunächst einmal gem. Art. 24 DS-GVO verpflichtet mit der Aufsichtsbehörde zusammenzuarbeiten!



Die *„Zusammenarbeit“* geht aber noch erheblich weiter!!!



Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DS-GVO

Der **Verantwortliche** ist grundsätzlich verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten **möglichst binnen 72 Stunden**, **nachdem ihm die Verletzung bekannt wurde**, diese der gemäß **Artikel 51** zuständigen Aufsichtsbehörde zu melden. Diese Verpflichtung entfällt nur, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko für die Rechte und Freiheiten** natürlicher Personen führt.

Erfolgt die Meldung an die Aufsichtsbehörde **nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen**.

Die Meldung enthält zumindest folgende **Informationen**:

- *eine **Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten**, soweit möglich **mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen**, **der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze**;*

- *den **Namen** und die **Kontaktdaten** des **Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen;*

- *eine **Beschreibung der wahrscheinlichen Folgen der Verletzung** des Schutzes personenbezogener Daten;*

- *eine **Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen**.*

Meldung von Verletzungen des Schutzes personenbezogener Daten an die

Aufsichtsbehörde gem. Art. 33 DS-GVO

...iner Verletzung des Schutzes
...n die Verletzung bekannt wurde,
Diese Verpflichtung entfällt nur,
...tlich **nicht** zu einem Risiko für die

...o ist ihr eine **Begründung** für die

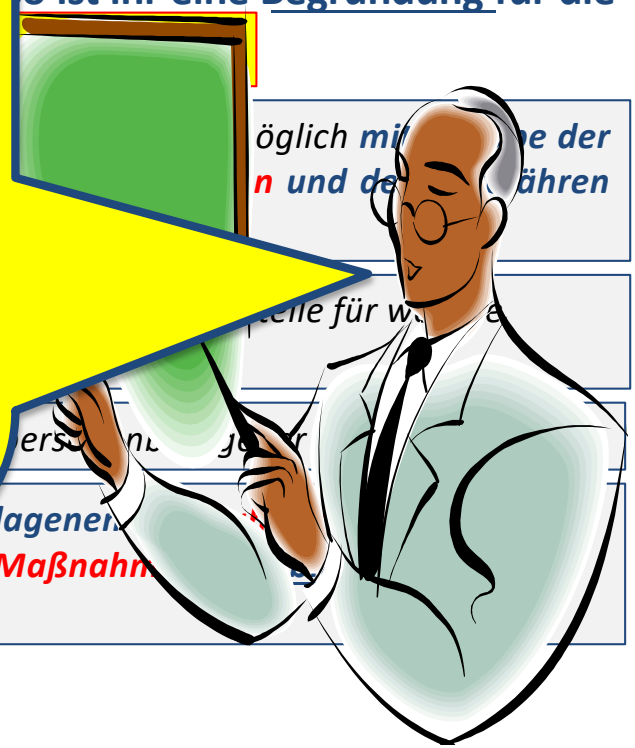
...öglich mi... ...e der
...n und de... ...ähren

...eile für w... ...e

...ers... ...nl... ...jeder

- ...nlagener...
  der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahm...
  möglichen nachteiligen Auswirkungen.

Darüber hinaus ist der Verantwortliche gem. Art. 33 DS-GVO verpflichtet, die Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren.
Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen!!!



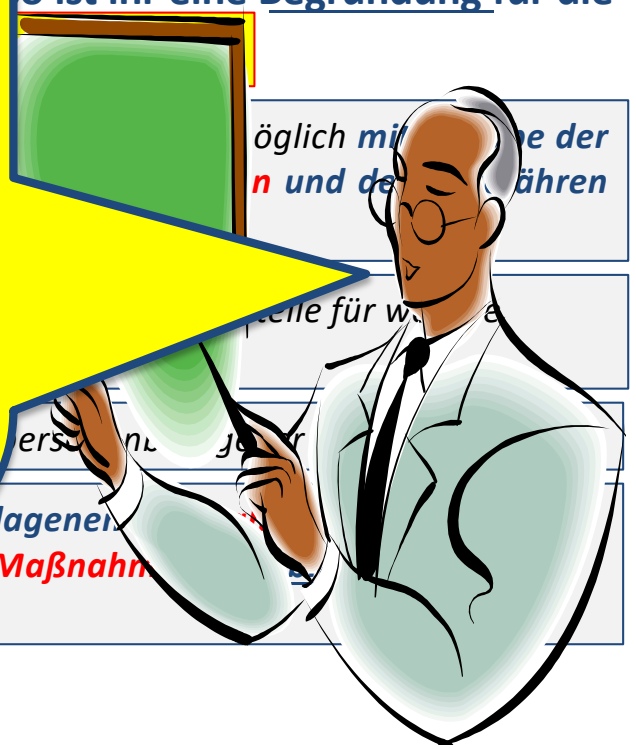
Meldung von Verletzungen des Schutzes personenbezogener Daten an die

Aufsichtsbehörde Art. 33 DS-GVO

iner Verletzung des Schutzes
n die Verletzung bekannt wurde,
Diese Verpflichtung entfällt nur,
tlich **nicht** zu einem Risiko für die

o ist ihr eine Begründung für die

*Soweit dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, ist auch **dieser** verpflichtet **diese unverzüglich dem Verantwortlichen zu melden**.*



öglich mi e der
n und de ähren

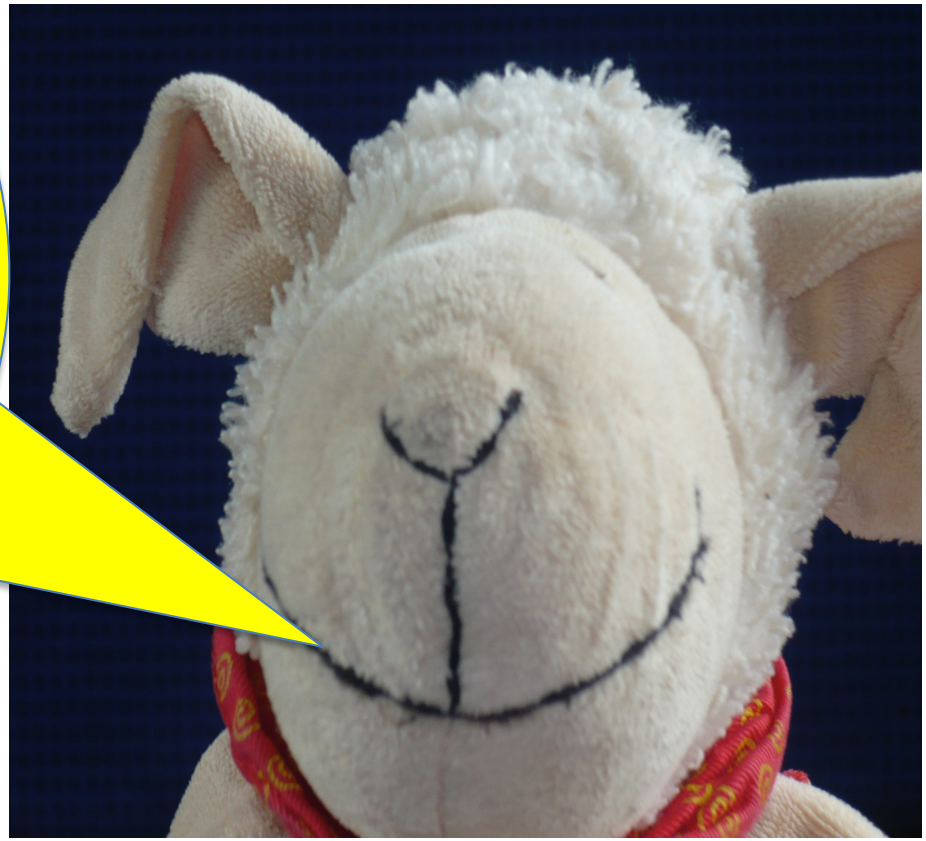
elle für w e

ersc nl j r

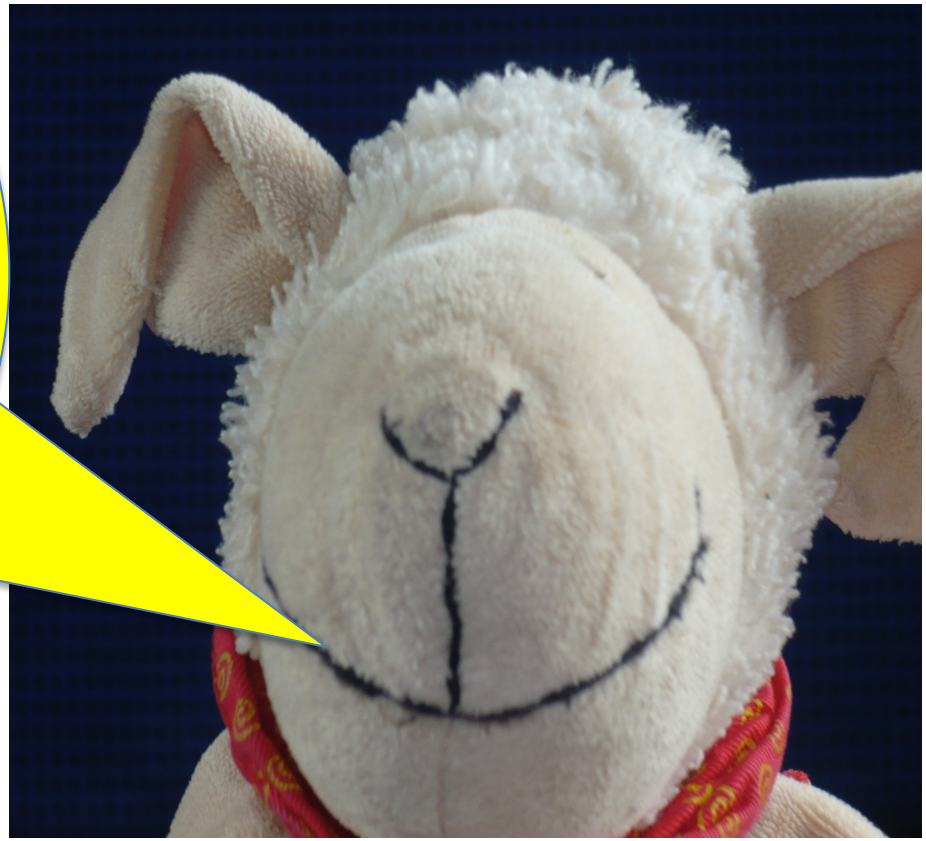
nlagene

der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahm
möglichen nachteiligen Auswirkungen.

Weitere Pflichten der „Handelnden“ bestimmen sich aus Art. 24 DS-GVO ff!



Art. 24 DS-GVO listet zunächst allgemein die Pflichten des „Verantwortlichen“ auf!



Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24 DS-GVO

Der Verantwortliche ist gem. **Art. 24 Abs. 1 DS-GVO** unter Berücksichtigung **der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen verpflichtet geeignete *technische* und *organisatorische* Maßnahmen** umzusetzen, **um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt**.

Diese Maßnahmen sind gem. **Art. 24 Abs. 1 S. 2 DS-GVO** vom Verantwortlichen **stetig** zu **überprüfen** und zu **aktualisieren**.

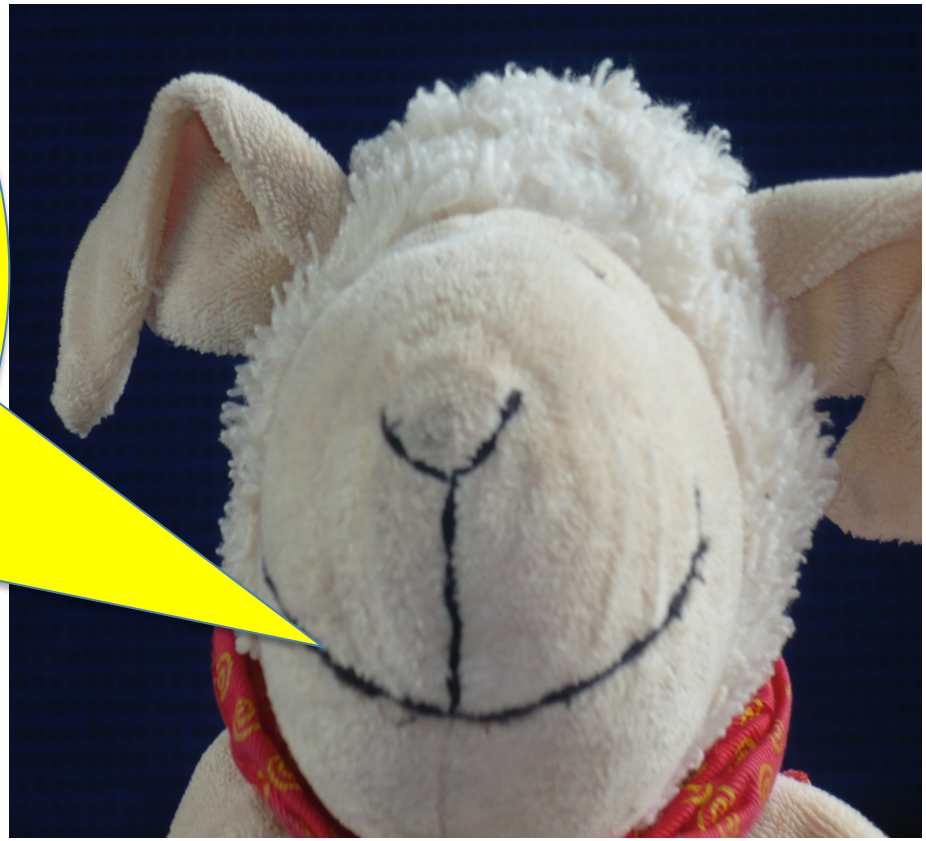
Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24 DS-GVO

Allerdings **kann** die Einhaltung der **genehmigten Verhaltensregeln** gemäß **Artikel 40** oder eines **genehmigten Zertifizierungsverfahrens** gemäß **Artikel 42** **als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.**

Berücksichtigung **der Art, des sowie der unterschiedlichen die Rechte und Freiheiten** ***rganisatorische*** **Maßnahmen bringen zu können, dass die**

rtlichen **stetig** zu

Dies wird dann weiter konkretisiert in Art. 32 DS-GVO!



Sicherheit der Verarbeitung, Art. 32 DS-GVO

Der Verantwortliche und der Auftragsverarbeiter haben nach Art. 32 DS-GVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Dies beinhaltet unter anderem:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

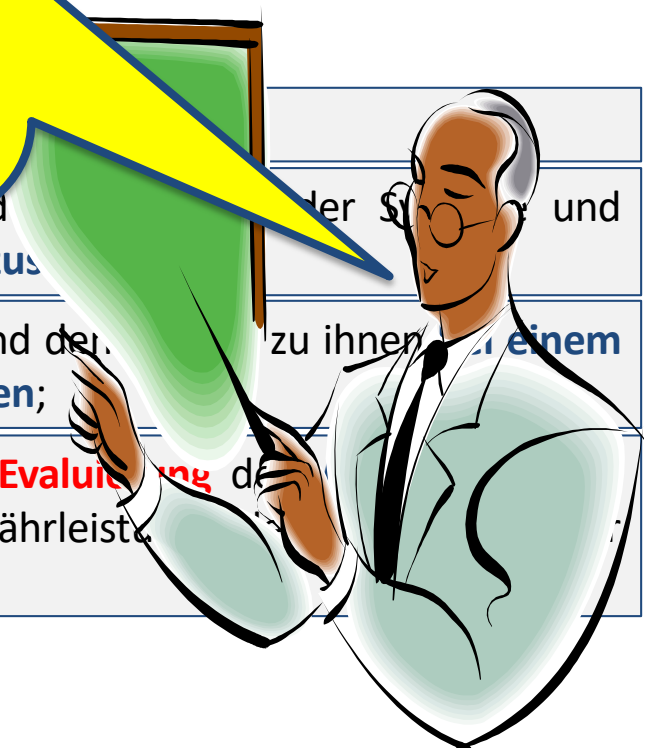
Sicherheit der Verarbeitung, Art. 32 DS-GVO

Achtung: Das neue Zauberwort ist auch hier:

„Stand der Technik“

nach **Art. 32 DS-GVO** unter
ngskosten und der **Art**, des
sowie der **unterschiedlichen**
die **Rechte** und **Freiheiten**
satorische **Maßnahmen**, um

- der S und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzus**
- die **Fähigkeit**, die **Verfügbarkeit** der personenbezogenen Daten und der zu ihnen einem **physischen** oder **technischen** Zwischenfall **rasch wiederherzustellen**;
- ein **Verfahren** zur **regelmäßigen Überprüfung**, **Bewertung** und **Evaluie ng** d **technischen und organisatorischen Maßnahmen** zur Gewährleist Verarbeitung.



Sicherheit der Verarbeitung, Art. 32 DS-GVO

...nach **Art. 32 DS-GVO** unter ...ngskosten und der **Art**, des ...sowie der **unterschiedlichen** ...die **Rechte** und **Freiheiten** ...satorische **Maßnahmen**, um

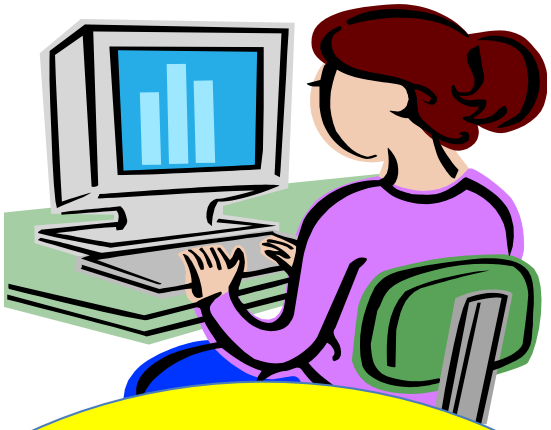
Allerdings **kann** auch hier die Einhaltung der **genehmigten Verhaltensregeln** gemäß **Artikel 40** oder eines **genehmigten Zertifizierungsverfahrens** gemäß **Artikel 42** **als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.**

- ...der S... und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzus...**
- die **Fähigkeit**, die **Verfügbarkeit** der personenbezogenen Daten und der... zu ihnen ...einem **physischen** oder **technischen** Zwischenfall **rasch wiederherzustellen**;
- ein **Verfahren** zur **regelmäßigen Überprüfung**, **Bewertung** und **Evaluie...ng** d... **technischen und organisatorischen Maßnahmen** zur Gewährleist... ... Verarbeitung.

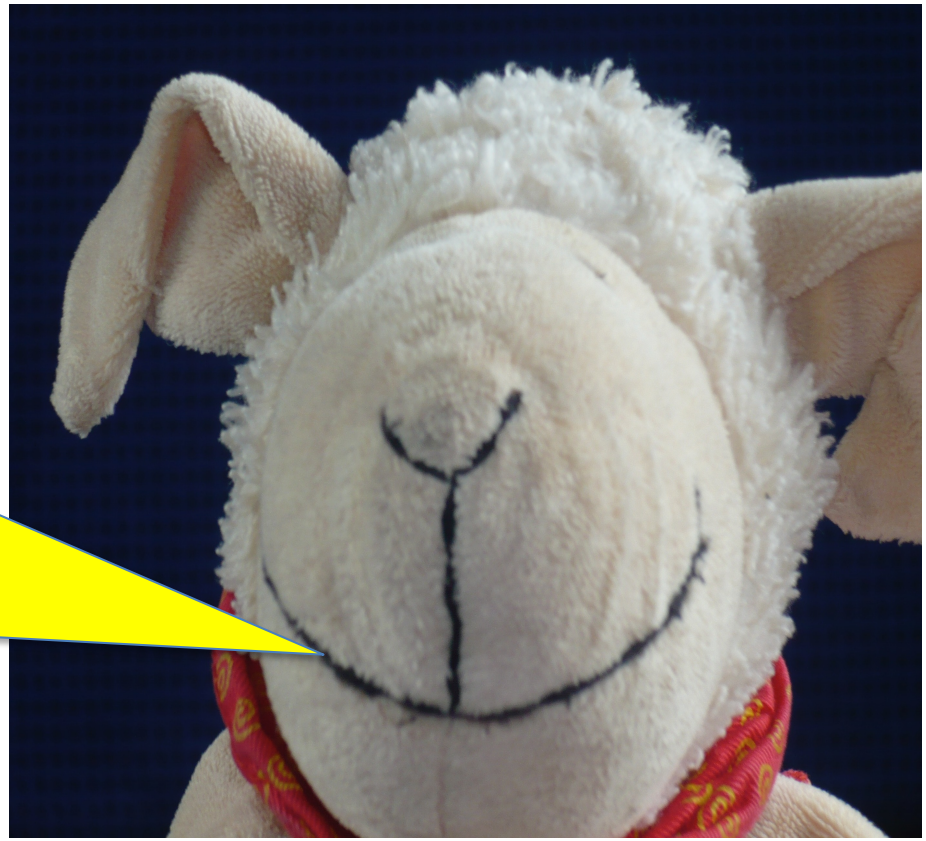
Systematisch ist den Regelungen gemeinsam, dass **keine konkreten Maßnahmen** vorgegeben werden, sondern dem Verantwortlichen lediglich **Ziele** und **Kriterien** zur Beurteilung der Risikoeinschätzung und Geeignetheit gegeben werden. Hierdurch wird versucht, der **DS-GVO** eine Regelungsdauer zu geben. Der Datenverarbeiter ist in der Verantwortung, technisch und organisatorisch Daten auf dem **aktuellen Stand der Technik** zu verarbeiten. Hilfestellung soll durch **Leitlinien** und **Hinweise** des **Europäischen Datenschutzausschusses** (**Art. 68 ff. DS-GVO**), der **Verbände** und der **Datenschutzbeauftragten** erfolgen (s.h. auch. ErwG 77 d. Verordnung). Insbesondere sollen nach **Art. 40 Abs. 2 Buchst. h Verhaltensregeln** aufgestellt werden, die dem verantwortlichen Hinweise zur Erfüllung seiner Verpflichtungen geben. Hierdurch wird eine kontinuierliche Fortentwicklung auf den **jeweils aktuellen Stand der Technik** ermöglicht.*

Zur Zeit stehen derartige Regelungen und Hilfestellungen erst nur teilweise zur Verfügung. Deshalb sollte auf den schon bisher vom Verantwortlichen nach dem **BDSG** erwarteten Maßnahmen aufgebaut werden. Zu beachten bleibt aber, dass - anders als bisher - nunmehr auch in diesem Bereich die Einhaltung des „**Stand der Technik**“ vorgegeben ist!

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 24 Rdn. 2



Dies war früher geregelt in der Anlage zu § 9 BDSG (alt)!

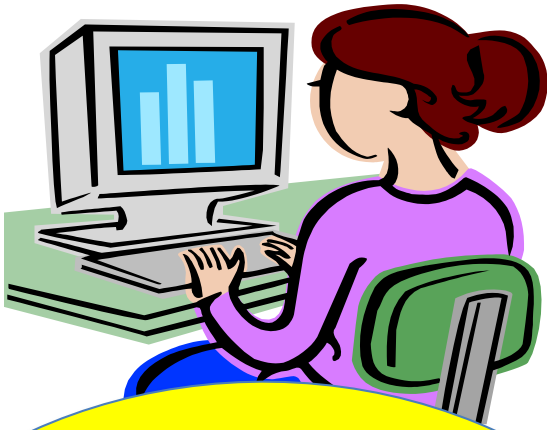


§ 9 BDSG Technische und organisatorische Maßnahmen

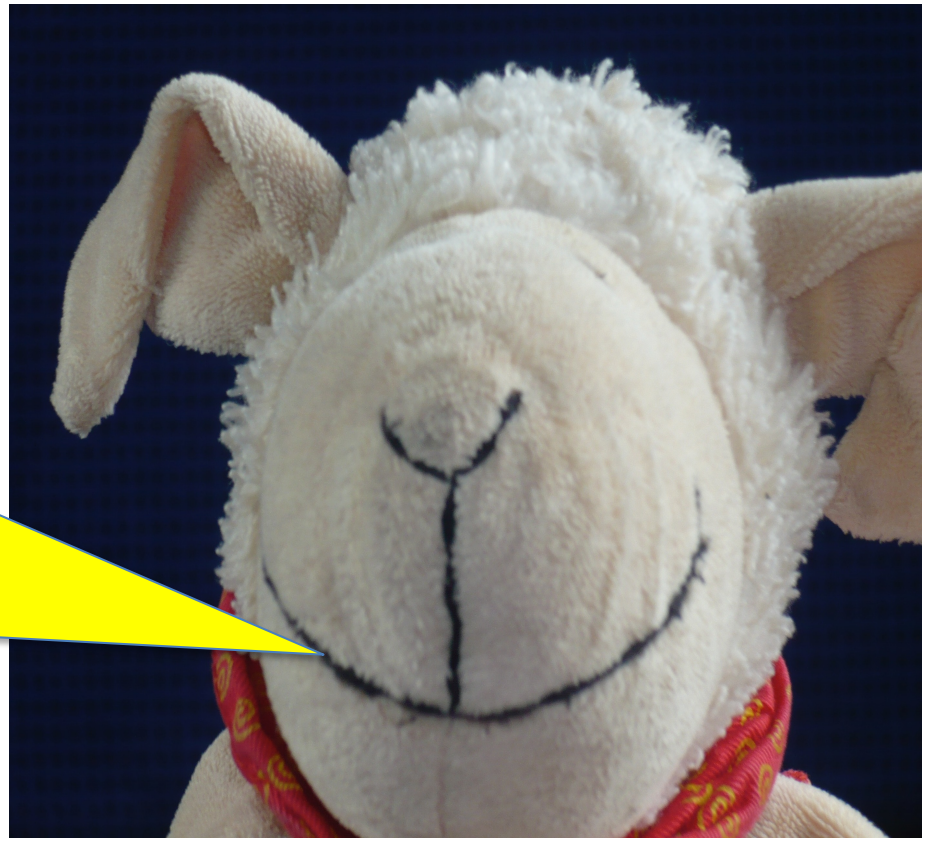
[1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. [2]Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Technische und organisatorische Maßnahmen i.S.d. Anlage zu § 9 BDSG

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



Heute findet sich dies in § 64 BDSG (neu)!



Technische und organisatorische Maßnahmen im Sinne von § 64 BDSG

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Die zu vereinbarenden technischen und **organisatorischen** Maßnahmen i.S.d. **Anlage zu § 64 BDSG** beinhalten:

- **Zugangskontrolle**
  Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung personenbezogene Daten durchgeführt wird, zu verwehren;
- **Datenträgerkontrolle**
  zu verhindern, dass Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können;
- **Speicherkontrolle**
  zu verhindern, dass personenbezogene Daten unbefugt eingegeben sowie gespeicherte personenbezogene Daten unbefugt zur Kenntnis genommen, verändert oder gelöscht werden;
- **Benutzerkontrolle**
  zu verhindern, dass automatisierte Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung unbefugt genutzt werden;
- **Zugriffskontrolle**
  zu gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben;

Die zu vereinbarenden technischen und **organisatorischen** Maßnahmen i.S.d. **Anlage zu § 64 BDSG** beinhalten:

- **Übertragungskontrolle**
  zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogener Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können;
- **Eingabekontrolle**
  zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind
- **Transportkontrolle**
  zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden;
- **Wiederherstellbarkeit**
  zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können;

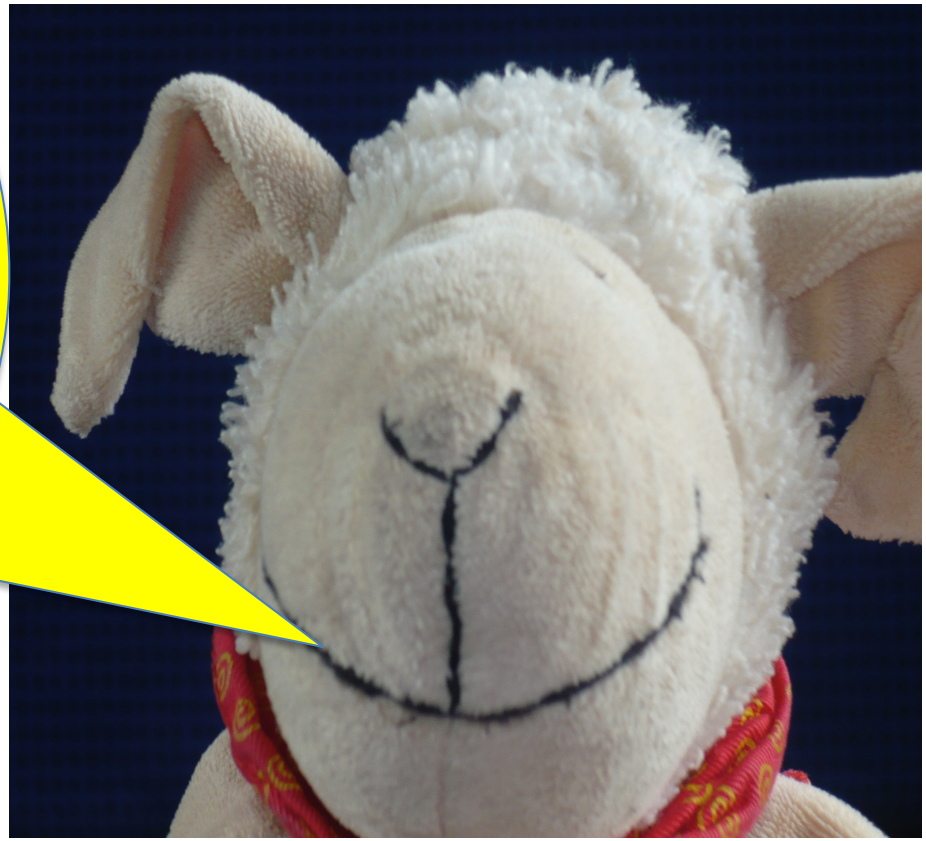
Die zu vereinbarenden technischen und **organisatorischen** Maßnahmen i.S.d. **Anlage zu § 64 BDSG** beinhalten:

- **Zuverlässigkeit**
  zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden;
- **Datenintegrität**
  zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können;
- **Auftragskontrolle**
  zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können;
- **Verfügbarkeitskontrolle**
  zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind;
- **Trennbarkeit**
  zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.


Das kann einem
ganz schön den
Tach versauen!!!


Und was sind bitte nun schon wieder „Zertifizierungen“!

„*Zertifizierungen*“ und
„*Verhaltensregeln*“
sollen sicherstellen, das
die aufgestellten
Anforderungen auch
nachweislich eingehalten
werden!



Zertifizierungen und Verhaltensregeln, Art. 40 ff. DS-GVO

In **Art. 40 DS-GVO** heißt es: Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission **fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen**.

Darüber hinaus sind auch **Verbände** und **andere Vereinigungen**, **die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten**, **nach bestimmten Vorgaben dazu aufgerufen Verhaltensregeln auszuarbeiten**, oder **zu ändern** bzw. **zu erweitern**, um sie sodann der **jeweiligen Aufsichtsbehörde zur Genehmigung vorzulegen**.

Zertifizierungen und Verhaltensregeln, Art. 40 ff. DS-GVO

In **Art. 40 DS-GVO** heißt es: Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission **fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unter… ordnungsgemäßen Anwendu… …en sollen.**

D… d… ver… Verha… erweitern, u… …ligen Aufsichtsbehö… Genehmigung vorzulegen.

Haben wir aber noch kaum welche!!!

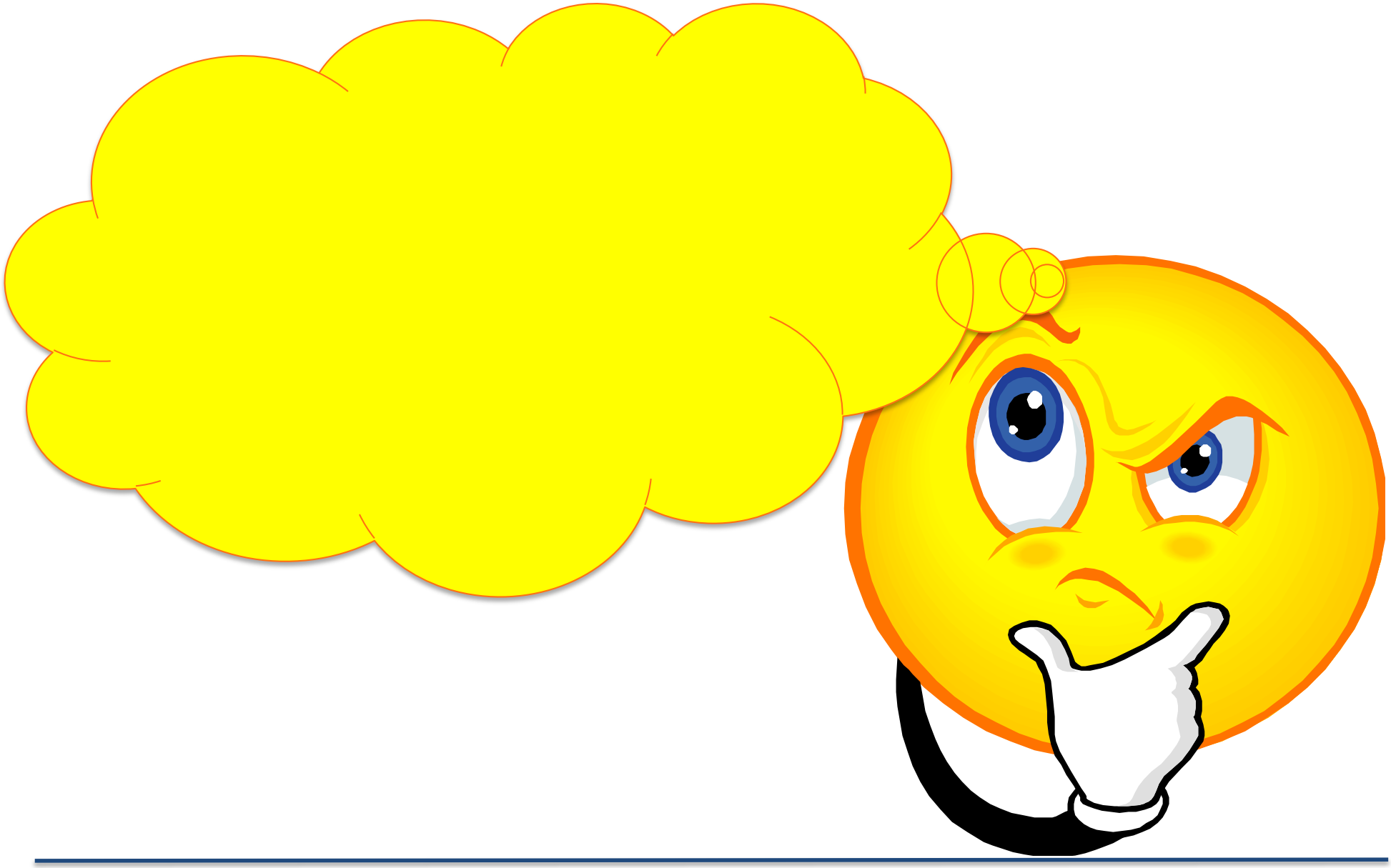
Überwachung der genehmigten Verhaltensregeln, Art. 41 DS-GVO

Die **Überwachung der Einhaltung** der genehmigten Verhaltensregeln obliegt dann neben den **Aufsichtsbehörden** auch nach **Art. 41 DS-GVO besonders akkreditierten Stellen**, die u.a. **entsprechendes Fachwissen** und **ihre Unabhängigkeit** nachgewiesen haben.

Überwachung der genehmigten Verhaltensregeln, Art. 41 DS-GVO

Die **Überwachung der Einhaltung** der genehmigten Verhaltensregeln obliegt dann neben den **Aufsichtsbehörden** auch nach **Art. 41 DS-GVO besonders akkreditierten Stellen**, die u.a. **entsprechendes Fachwissen** und **ihre Unabhängigkeit** nachgewiesen haben.

„Die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, erfolgt durch die für die datenschutzrechtliche Aufsicht über die Zertifizierungsstelle zuständige Aufsichtsbehörde des Bundes oder der Länder auf der Grundlage einer Akkreditierung durch die Deutsche Akkreditierungsstelle.
§ 2 Absatz 3 Satz 2, § 4 Absatz 3 und § 10 Absatz 1 Satz 1 Nummer 3 des Akkreditierungsstellengesetzes finden mit der Maßgabe Anwendung, dass der Datenschutz als ein dem Anwendungsbereich des § 1 Absatz 2 Satz 2 unterfallender Bereich gilt.“



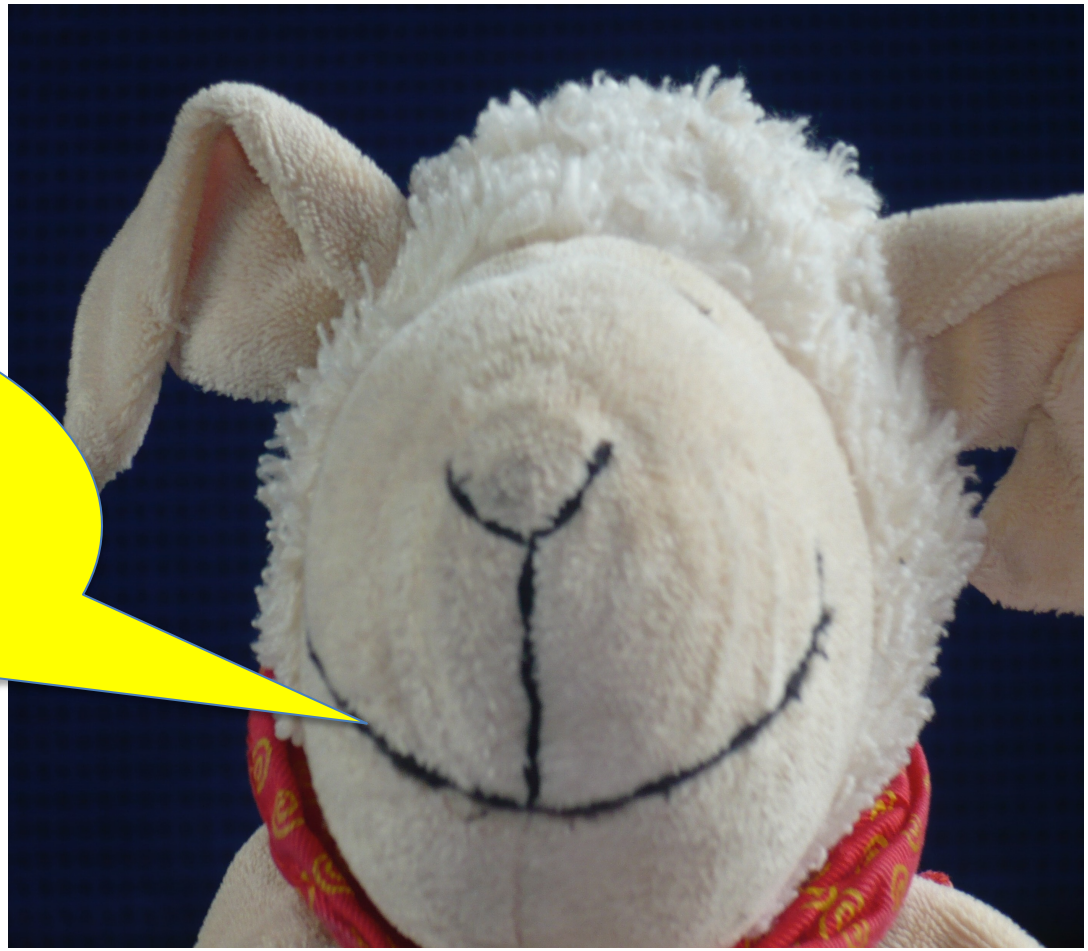
Zertifizierung, Art. 42 DS-GVO

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein und eine entsprechende Zertifizierung wird für eine Höchstdauer von 3 Jahren erteilt .

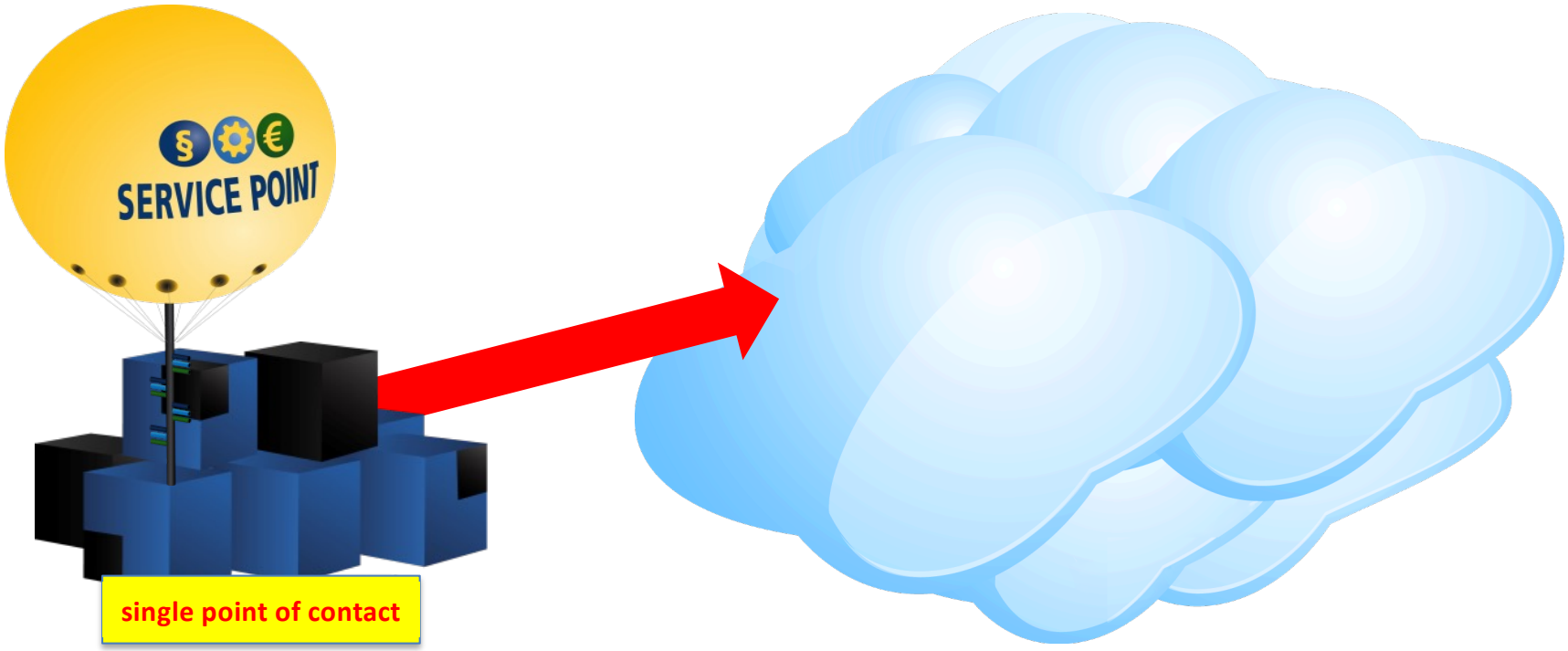
Eine Zertifizierung mindert indes nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.

Eine zusätzliche neue Verpflichtung ergibt sich dann noch aus Art. 25 DS-GVO!



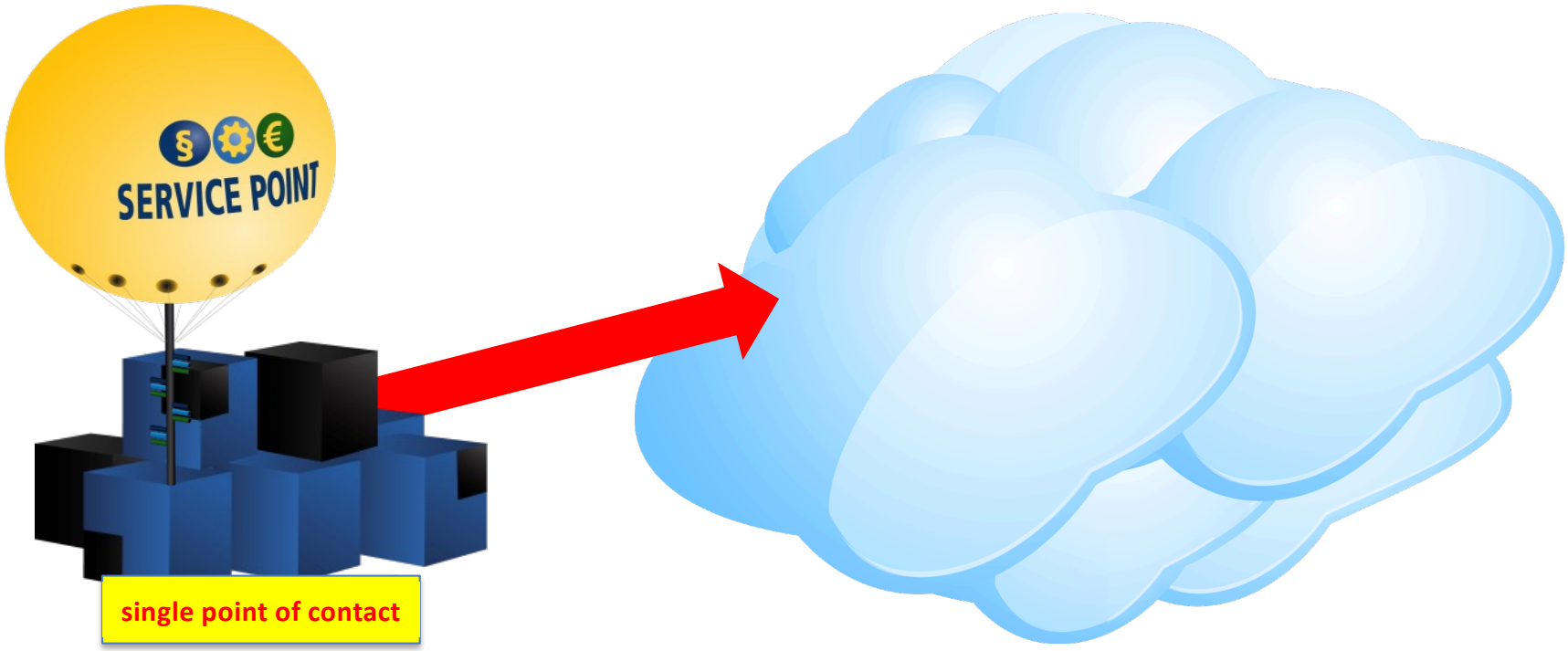
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO

Der Verantwortliche ist gem. **Art. 25 DS-GVO** verpflichtet unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** der Verarbeitung sowie der **unterschiedlichen Eintrittswahrscheinlichkeit** und **Schwere der mit der Verarbeitung verbundenen Risiken** für die Rechte und Freiheiten natürlicher Personen **sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung, als auch zum Zeitpunkt der eigentlichen Verarbeitung** geeignete **technische** und **organisatorische Maßnahmen** — wie z. B. **Pseudonymisierung** — zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa **Datenminimierung** wirksam umzusetzen und die **notwendigen Garantien** in die Verarbeitung aufzunehmen, **um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.**



Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO

Der Verantwortliche ist **ferner** verpflichtet durch geeignete **technische** und **organisatorische Maßnahmen**, die sicherstellen, dass durch **Voreinstellung grundsätzlich nur** personenbezogene Daten, **deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden**.
Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang ihrer Verarbeitung**, ihre **Speicherfrist** und ihre **Zugänglichkeit**.



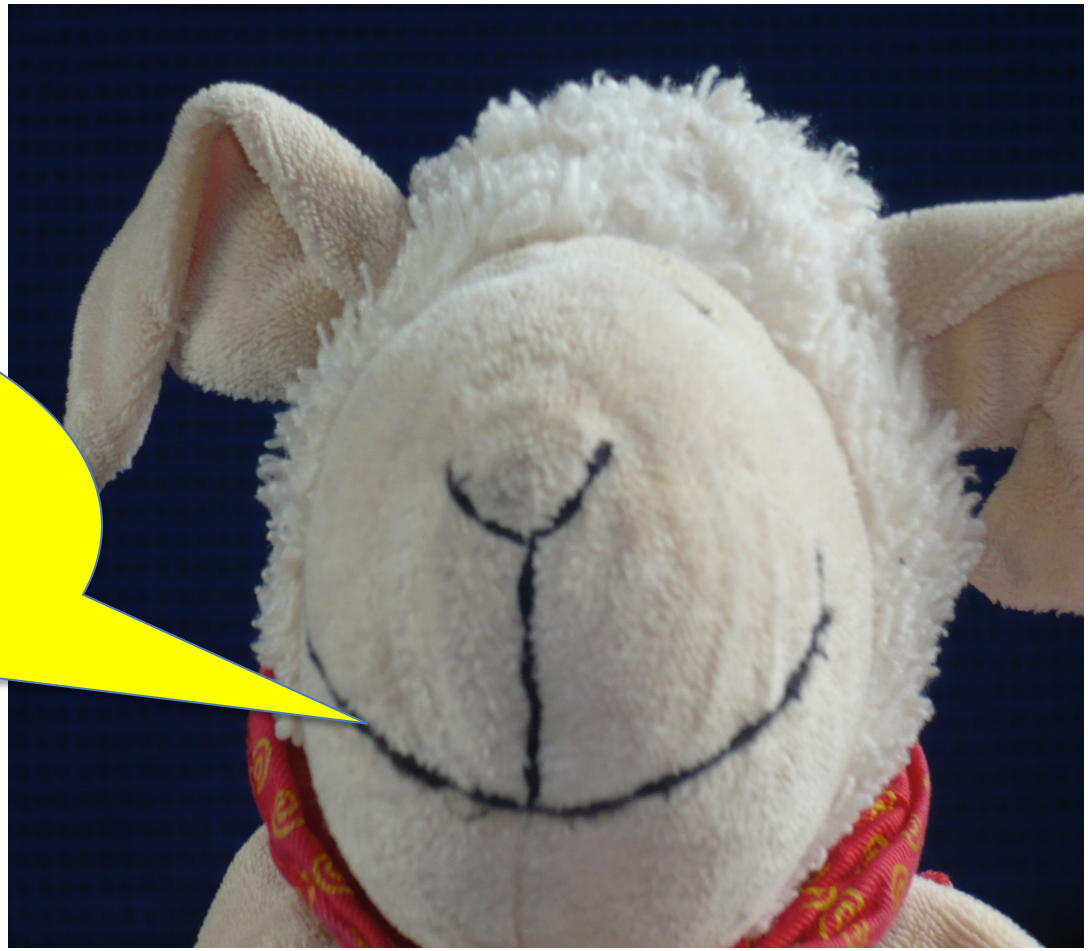
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO

d **organisatorische Maßnahmen**, die
Daten, **deren Verarbeitung für den**

, den **Umfang ihrer Verarbeitung**, ihre

Allerdings **kann** auch hier wieder die Einhaltung der **genehmigten Verhaltensregeln** gemäß **Artikel 40** oder eines **genehmigten Zertifizierungsverfahrens** gemäß **Artikel 42 als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.**

Eine zusätzliche neue Verpflichtung ergibt sich auch aus Art. 27 DS-GVO!



Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern, Art. 27 DS-GVO

Soweit eine Verarbeitung von personenbezogenen Daten von betroffenen Personen die sich in der EU befinden **durch nicht in der Union niedergelassene Verantwortliche oder Auftragsdatenverarbeiter erfolgt**, und die Datenverarbeitung im Zusammenhang damit steht,

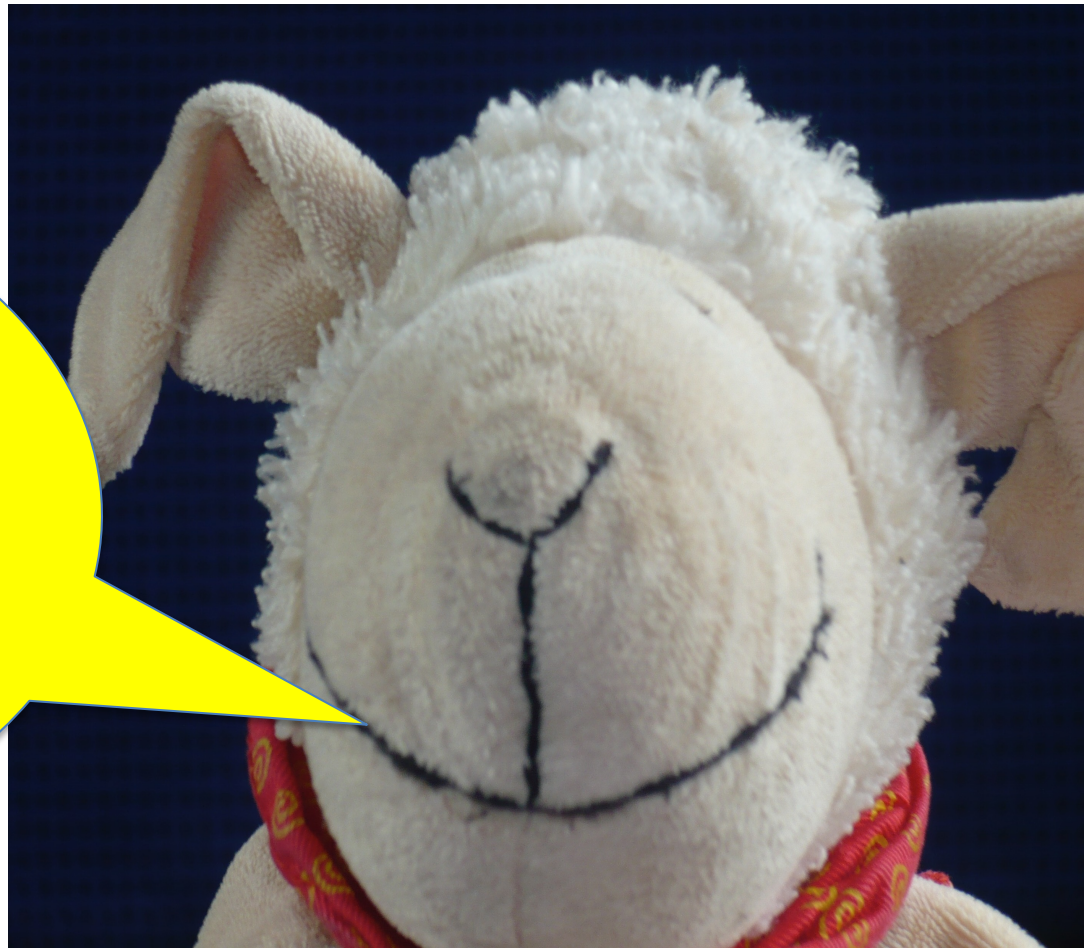
- betroffenen Personen **in** der Union **Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist**;
- **das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt**.

*ist der **Verantwortliche** oder der **Auftragsverarbeiter grundsätzlich verpflichtet schriftlich einen Vertreter in der Union zu benennen**.*

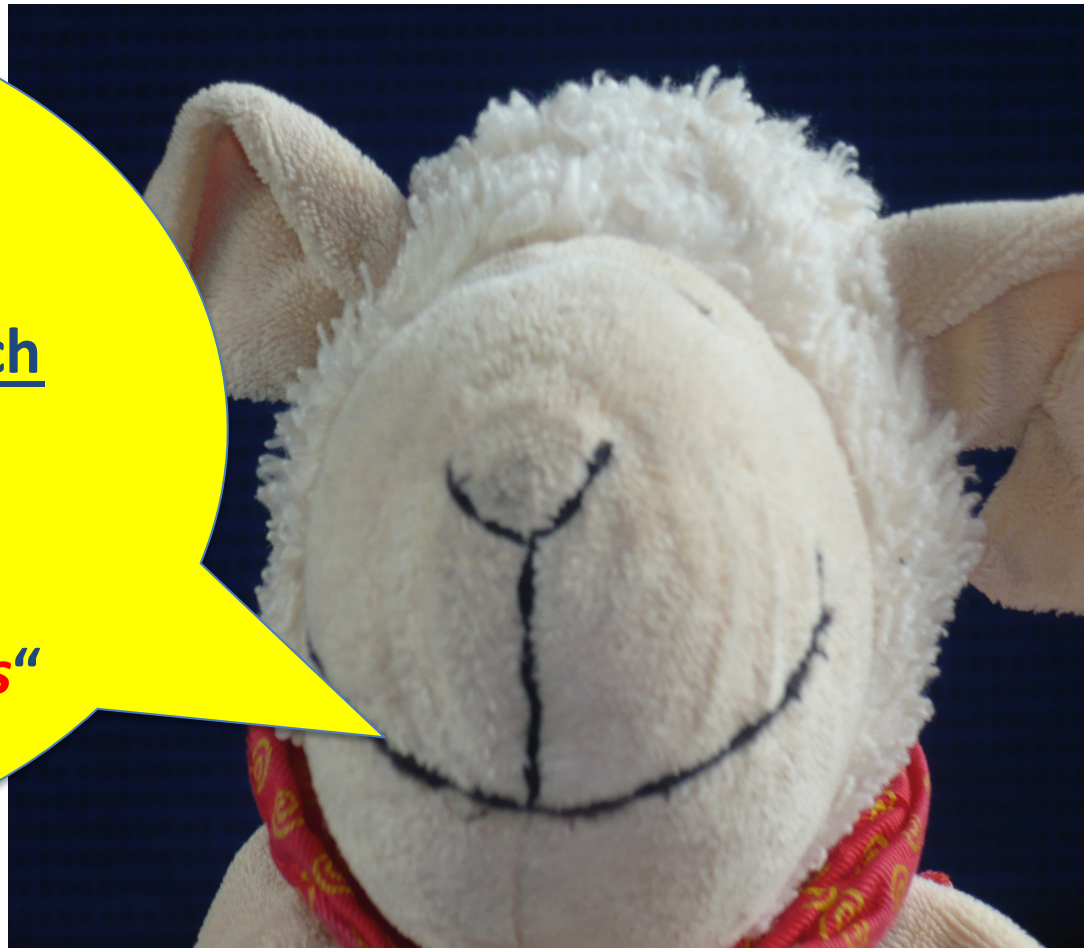
***Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden**.*

*Die Benennung eines Vertreters durch den Verantwortlichen oder den Auftragsverarbeiter **erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst**.*

Und eine schöne neue zusätzliche Verpflichtung ergibt sich auch noch aus Art. 30 DS-GVO!



Gemäß
Art. 30 DS-GVO ist
nunmehr durch den
Verantwortlichen und auch
durch den
Auftragsverarbeiter
ein sog.
„*Verarbeitungsverzeichnis*“
zu führen!



Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

Gemäß **Art. 30 DS-GVO müssen**

alle **Verantwortlichen** und alle **Auftragverarbeiter**

ein **Verzeichnis von Verarbeitungstätigkeiten führen!**

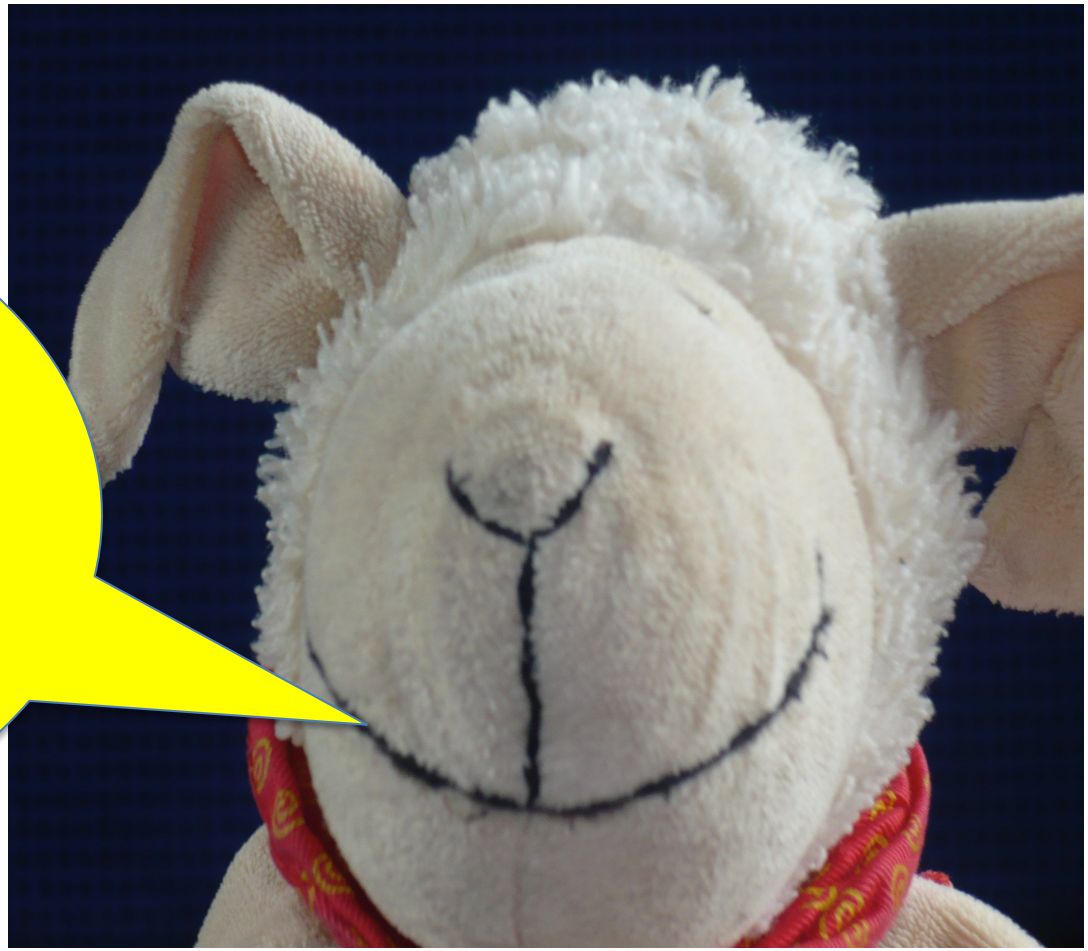
Dieses muss insbesondere enthalten:

- den **Namen** und die **Kontaktdaten** des **Verantwortlichen**
  - **die Kategorien von Empfängern**
- den etwaigen **Datenschutz-beauftragten**
  - die **vorgesehenen Fristen** für die **Löschung** der verschiedenen Datenkategorien
- die **Zwecke der Verarbeitung**
  - eine **allgemeine Beschreibung der technischen** und **organisatorischen Maßnahmen** gemäß **Artikel 32 Absatz 1**
- eine Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten**
  - den Namen und die Kontaktdaten **jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist**

Die Verpflichtung gilt nach dem Wortlaut des **Art. 30 Abs. 5 DS-GVO** indes **nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen**, sofern es sei denn

- die von ihnen vorgenommene Verarbeitung **nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt**,
- **die Verarbeitung nicht nur gelegentlich erfolgt** oder
- **nicht die Verarbeitung besonderer Datenkategorien** gemäß **Artikel 9 Absatz 1** bzw. die **Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten** im Sinne des **Artikels 10** einschließt.

Aber Achtung:
Die doppelte Verneinung hat es in sich!



Eine nur „*gelegentliche*“ **Tätigkeit** liegt insbesondere vor, wenn sie **ohne Wiederholungsabsicht erfolgt**, wobei sich die Wiederholungsabsicht sich bei einem Auftragsverarbeiter **nicht** auf **denselben Auftraggeber** beziehen muß, sondern sich **auf die Auftragsverarbeitung als solche** bezieht.*

Da heutzutage nahezu jede Datensammlung **regelmäßig** und **nicht nur gelegentlich** automatisiert verarbeitet wird, dürfte, worauf auch *Schaffland/Holthaus*** zu Recht verweisen, auch im Rahmen der 2. Alternative die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten **auch bei Unternehmen mit weniger als 250 Mitarbeitern die Regel sein**.
Dazu kommt, dass **häufig kleinere Unternehmen von größeren Unternehmen im Rahmen der Auftragsverarbeitung beauftragt werden** und **diese Beauftragung wegen der dementsprechenden Verpflichtung der größeren Unternehmen, von diesen für eine Auftragserteilung an die kleineren Unternehmen zur Bedingung für die Beauftragung gemacht werden wird**.

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 30 Rdn. 47

**Schaffland/Holthaus DS-GVO – Kommentar, Art. 30 Rdn. 50

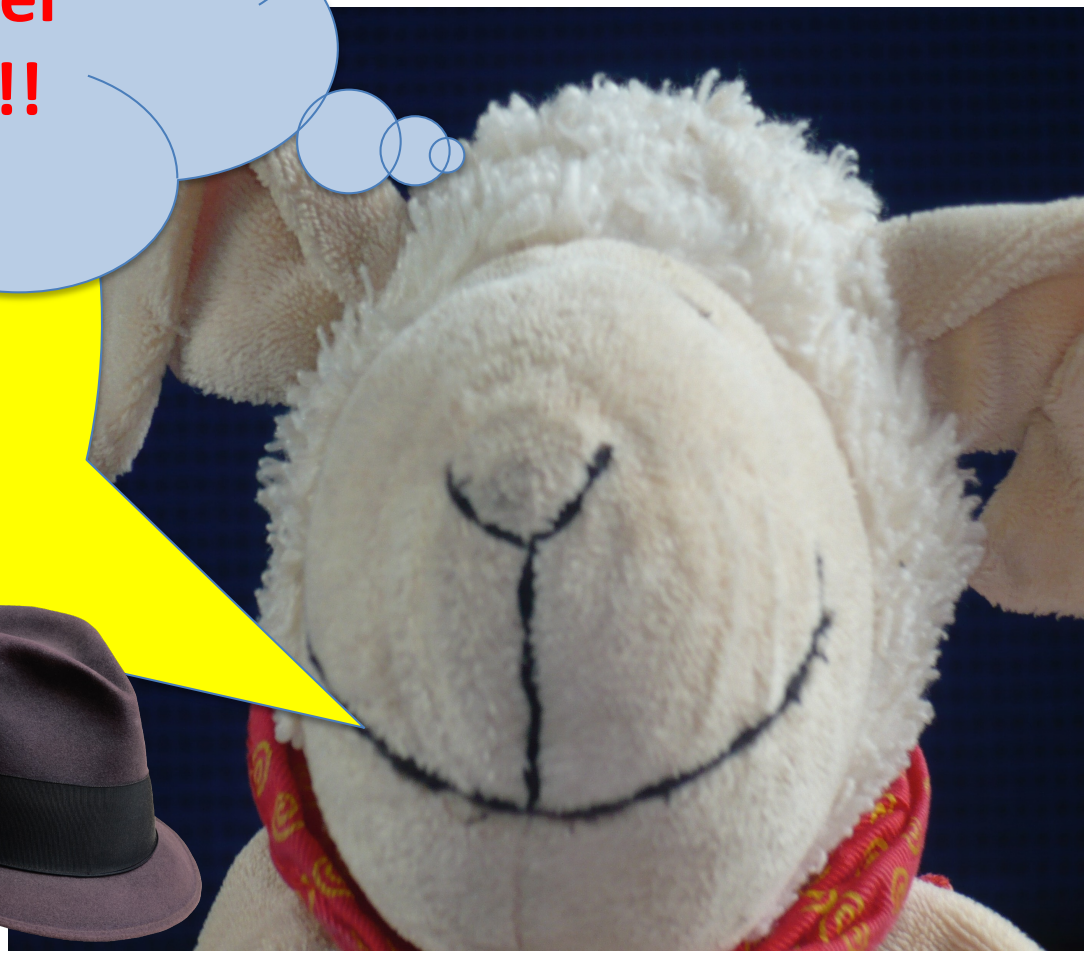

Eigentlich ist dies aber eigentlich zumindest teilweise ein „alter Hut“!

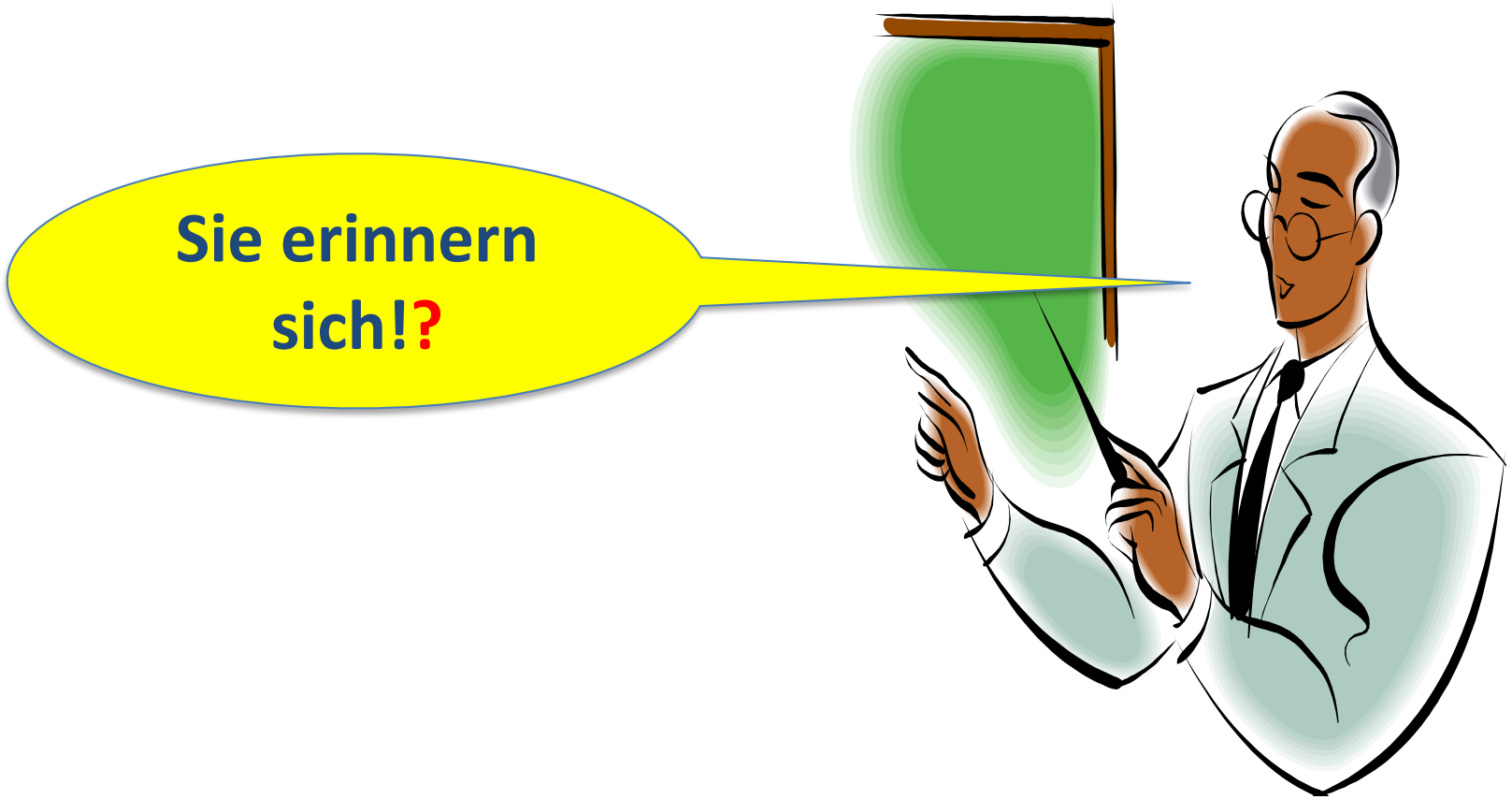

Wieso???

Na weil Du eigentlich schon aus anderen Gründen verpflichtet bist Ähnliches zu machen!

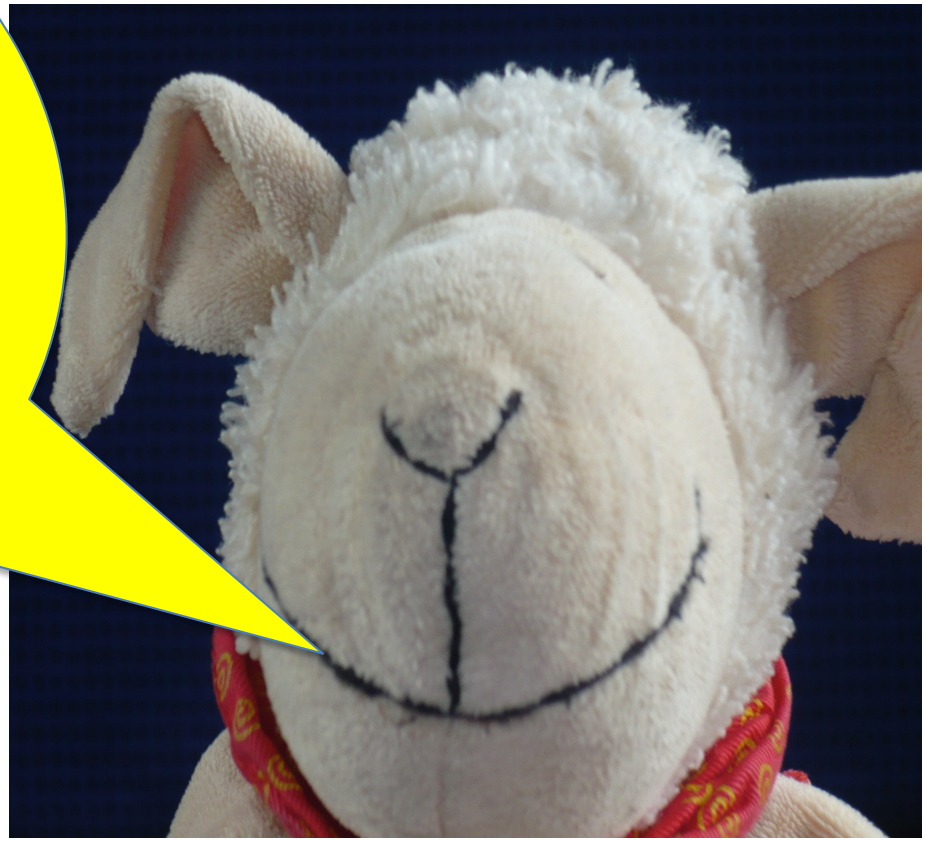
Es wahrscheinlich aber
nicht gemacht hast!!!

Grun
verpflichtet bist
Ähnliches zu
machen!




Sie erinnern sich!?

Im Prinzip gilt auch hier nichts anderes, als das, was wir schon kennen!
Das Stichwort ist
„Compliance in der IT“

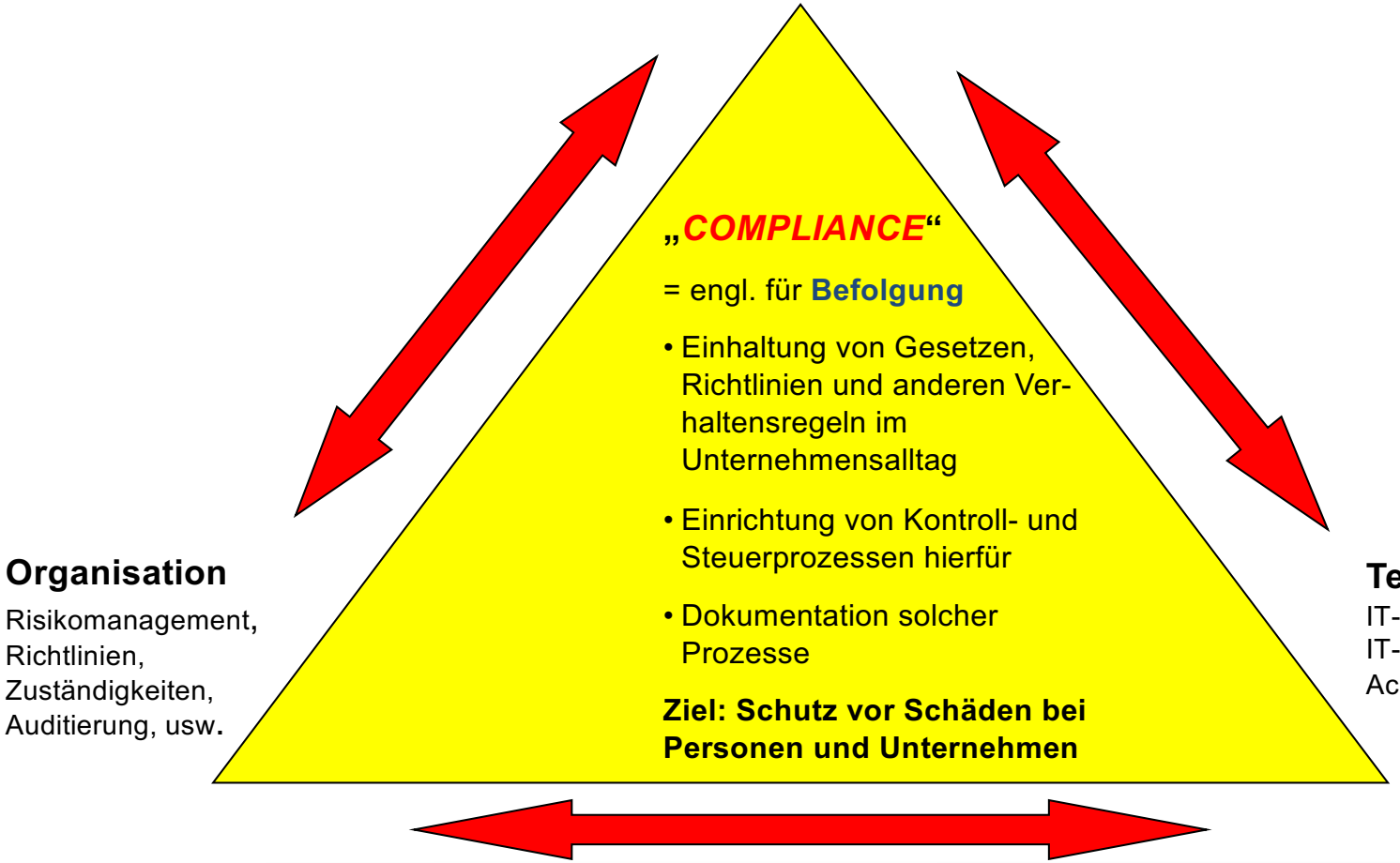



Mir schwant Übles!!!

IT-Compliance beschreibt das Spannungsfeld von Organisation, Technik und regulatorischen Anforderungen:

gesetzliche Anforderungen

KonTraG*, Basel II, GDPdU**, DS-GVO, BDSG usw.



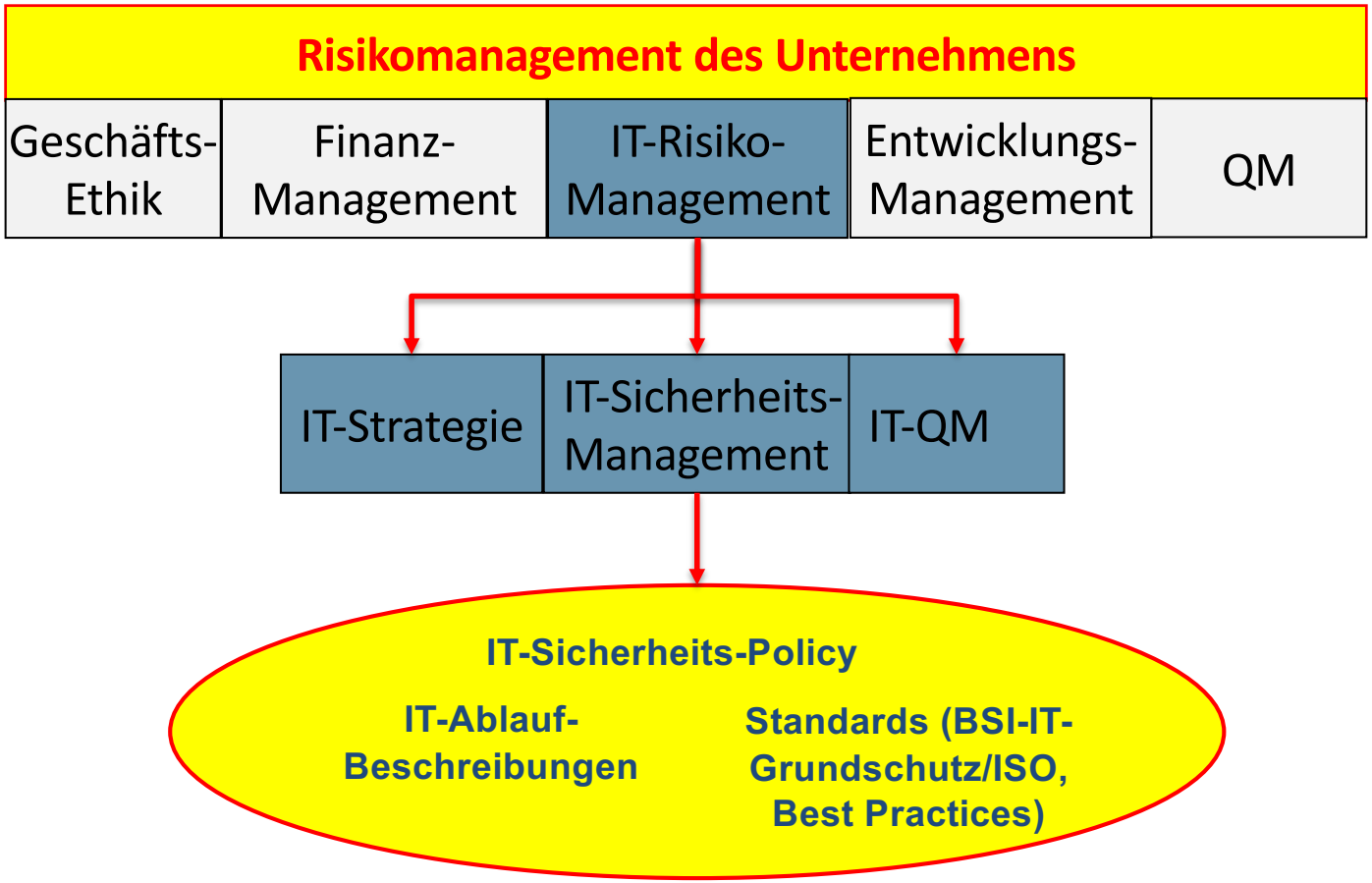
Organisation
Risikomanagement, Richtlinien, Zuständigkeiten, Auditierung, usw.

Technik
IT-Security, IT-Risikoanalyse, Achivierung usw.

*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich v. 1. Mai 1998

**„Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“

Die **Geschäftsführung/der Vorstand** muss ein (**IT-**)**Risiko-Früherkennungssystem** einführen und dessen Qualität **ständig kontrollieren** und immer wieder an **neue/geänderte Bedürfnisse anpassen!**



Als Beispiel für die Umsetzung der vorstehend aufgeführten Maßnahmen, kann hier der von der Bundesnetzagentur aufgestellte „**IT-Sicherheitskatalog**“ gemäß **§ 11 Absatz 1a Energiewirtschaftsgesetz** für die **Energiewirtschaft** dienen.

Als Beispiel für die Umsetzung der vorstehend aufgeführten Maßnahmen, kann **aber auch** der von der Bundesnetzagentur aufgestellte „**IT-Sicherheitskatalog**“ gemäß **§ 109 TKG** für die **Betreiber von öffentlichen Kommunikationsnetzen** und **Erbringer von öffentlich zugänglichen Telekommunikations-diensten** dienen.

IT-Recht Grundlagen für Informatiker
Problem- und praxisorientierte Tipps für die Vertragsgestaltung
Datenschutz

Inhaltsverzeichnis

Als Beispiel für die Umsetzung der vorstehend aufgeführten Maßnahmen, kann hier der von der Bundesnetzagentur aufgestellte „**IT-Sicherheitskatalog**“ gemäß **§ 11 Absatz 1a Energiewirtschaftsgesetz** für die **Energiewirtschaft** dienen.

Als Beispiel für die Umsetzung der vorstehend aufgeführten Maßnahmen, kann **aber auch** der von der Bundesnetzagentur aufgestellte „**IT-Sicherheitskatalog**“ gemäß **§ 109 TKG** für die **Betreiber von öffentlichen Kommunikationsnetzen** und **Erbringer von öffentlich zugänglichen Telekommunikations-diensten** dienen.

Kernforderung beider Sicherheitskataloge ist die **Einführung eines Informationssicherheits-Managements** (**ISMS**) gemäß **DIN ISO/IEC 27001 sowie** die **Zertifizierung durch eine unabhängige hierfür zugelassene Stelle**.

Darüber hinaus kommt auch hier anderes Altbekanntes wieder zum Tragen nämlich die **Security-Policy!**

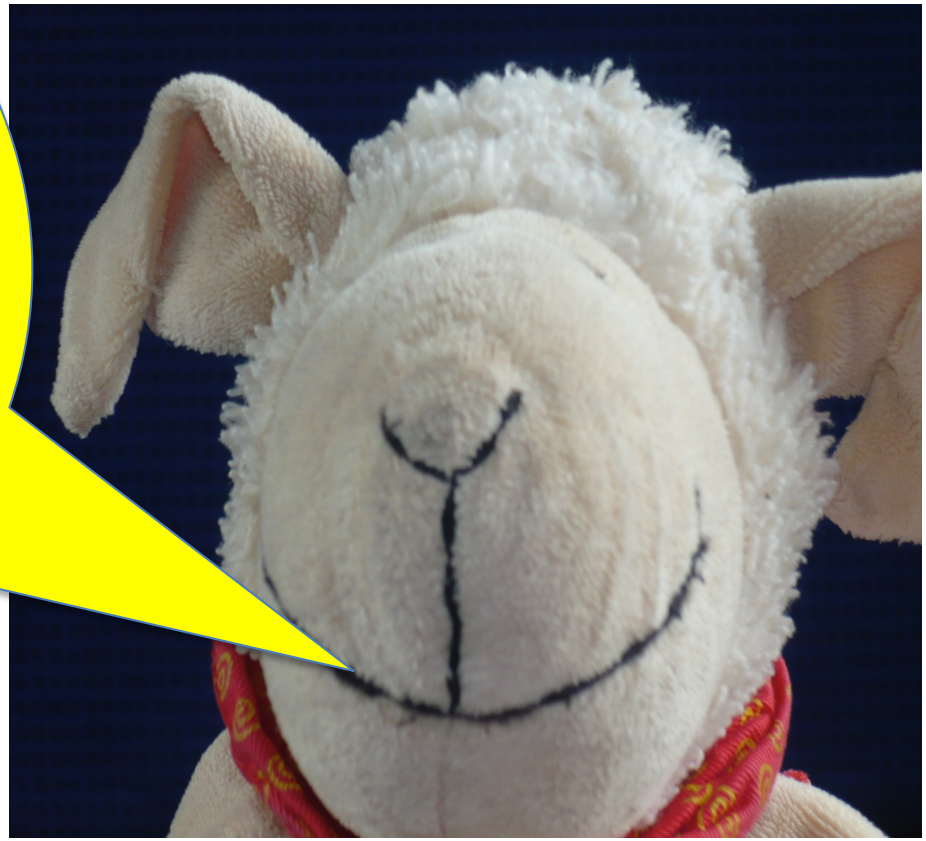
Sie erinnern sich!!!???

Beispielhafter Aufbau eines Regelwerkes zur IT-Security als „*Brandschutzmauer*“ des Unternehmens:

Ausführungsbestimmungen/Hand-outs/technische Konzepte für einzelne Personengrupen (z.B. Nutzer, Servicepartner, Admistratoren)		
Notfallkonzept	Konzept zur Rückholung ausgelagerter Daten	Sicherung des Know Hows versus „Kopfdokumentation/-monopol“
Outsourcing	Cloud-Computing	BYOD
Nutzungsrechte	Externe Partner und „Dienstleister“ des Unternehmens	FOS/Opensource-Software
Datensicherheit und Archivierung	Verwendung von Internet und @-mail im Unternehmen	Malware und Virenschutz
Festlegung des Schutzbedarfs	IT-Sicherheitsorganisation = Verantwortlichkeiten/Zuständigkeiten	Physischer Schutz § 64 BDSG (neu)
IT-Security („*Security-Policy*“)		


Na herzlichen Glückwunsch!!!

„*Neu im Angebot*“ ist dann noch ein weiteres schönes Instrumentarium!



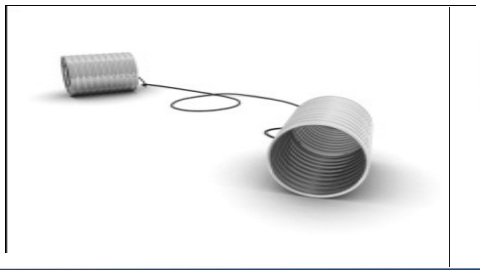
Die
„Datenschutz-Folgenabschätzung“

Datenschutz-Folgenabschätzung, Art. 35 DS-GVO

Der Verantwortliche ist verpflichtet, wenn eine Form der Verarbeitung, insbesondere bei Verwendung *neuer Technologien*, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

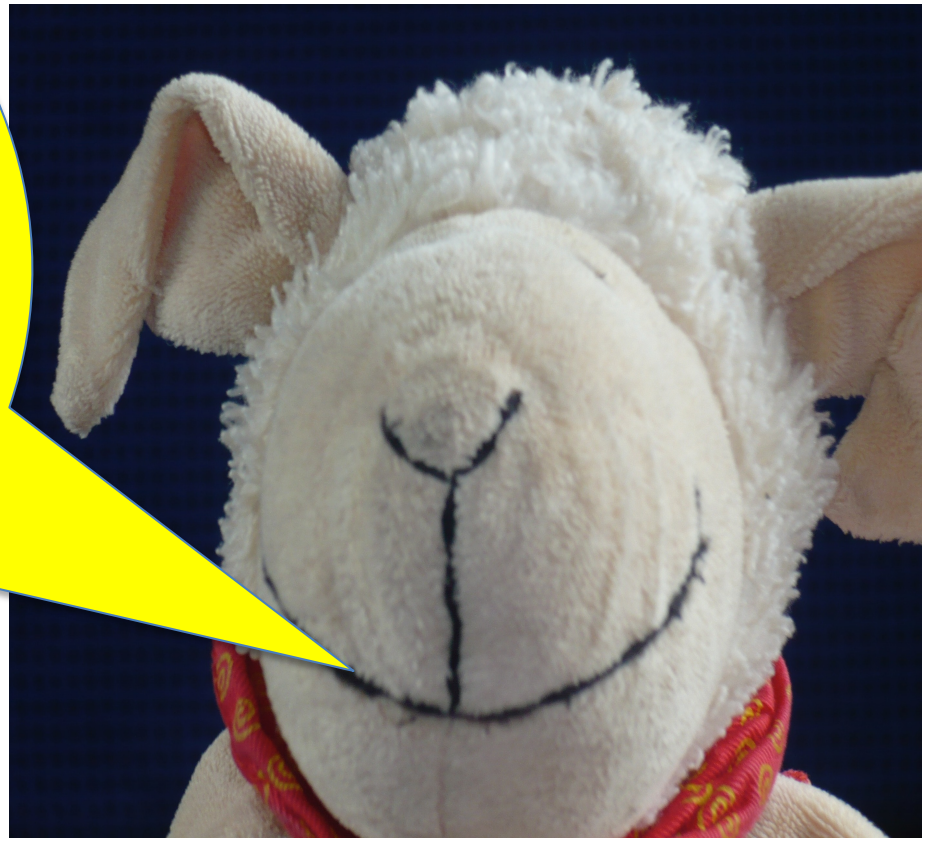
Die Folgenabschätzung **enthält zumindest Folgendes**:

- eine **systematische Beschreibung der geplanten Verarbeitungsvorgänge** und **der Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine **Bewertung** der **Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck**;
- eine **Bewertung** der **Risiken für die Rechte und Freiheiten der betroffenen Personen** gemäß Absatz 1 und
- *die **zur Bewältigung der Risiken geplanten Abhilfemaßnahmen**, einschließlich **Garantien**, **Sicherheitsvorkehrungen** und **Verfahren**, **durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird**, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.*



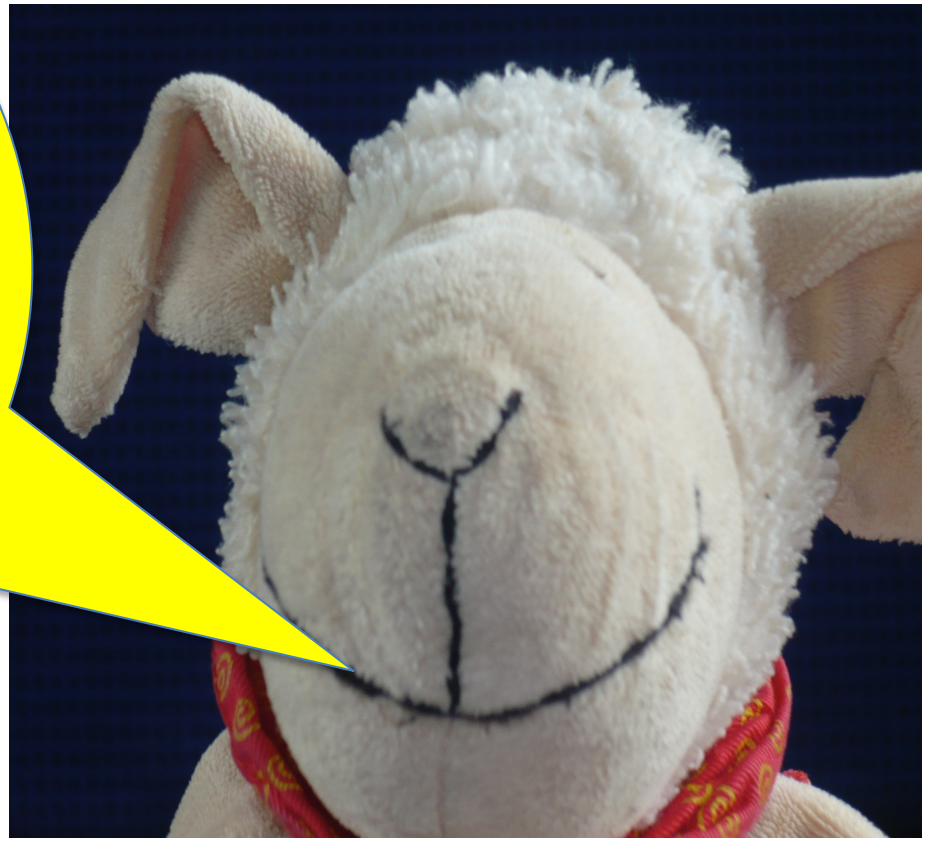

Darüber hinaus ist ggf. auch noch eine „vorherige Konsultation“ der Aufsichtsbehörde erforderlich!



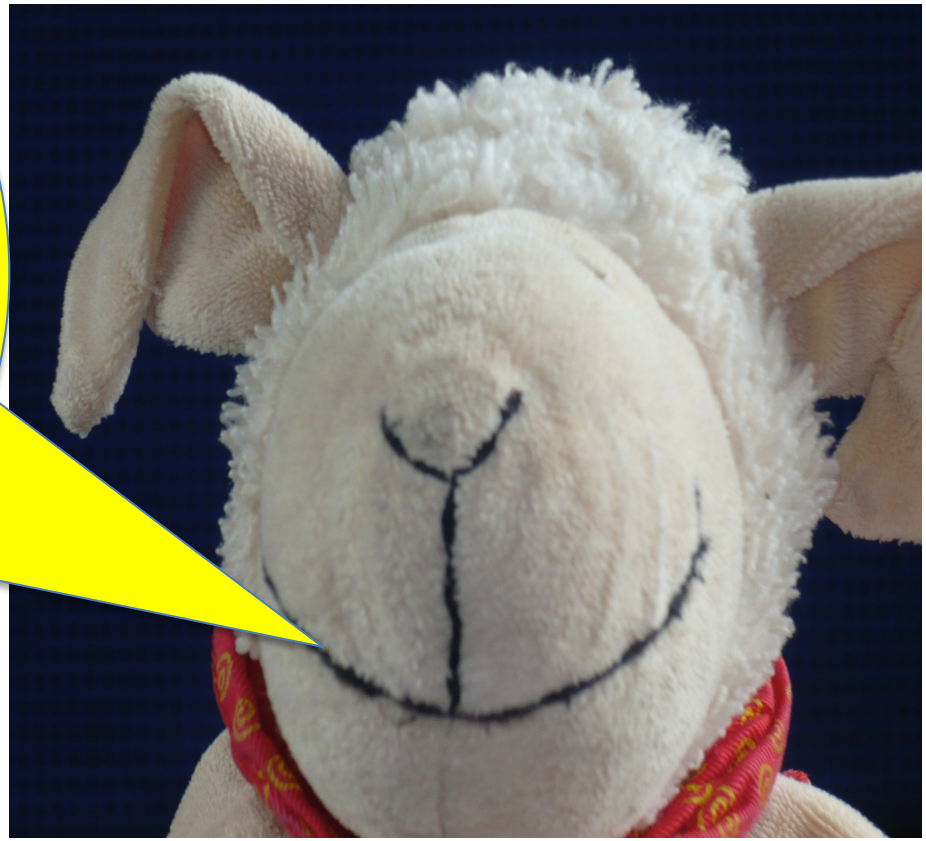
Vorherige Konsultation, Art. 36 DS-GVO

Der Verantwortliche ist **verpflichtet, vor der Verarbeitung die Aufsichtsbehörde zu konsultieren**, wenn **aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte**, **sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft**.

So jetzt aber zum
„Auftragsverarbeiter“!



Sie erinnern sich!?



Soweit ein Unternehmen **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

Die sog. „**Auftragsverarbeitung**“ liegt (nur) vor, wenn die personenbezogenen Daten **im Auftrag und auf Weisung** erhoben, verarbeitet oder genutzt werden.
Dies ergibt sich aus **Art. 4 Nr. 8 DS-GVO**, wonach „**Auftragsverarbeiter**“ **eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ist, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet**.

Hierzu gehört insbesondere z.B. der Betrieb eines **Rechenzentrums** in dem Daten für einen Anderen im Auftrag verarbeitet werden.

Hierzu gehören aber wohl auch nach neuem Recht auch **Pflege- und Wartungsarbeiten (§ 11 Abs. 5 BDSG (alt))**

*Nach Art. 4 DS-GVO zählen auch das Auslesen und Abfragen sowie die Offenbarung von personenbezogenen Daten als Verarbeitung. Daher muss auch der Verantwortliche auch zukünftig unter der Geltung der DS-GVO umfassende Vereinbarungen mit den Erbringern von Wartungs- und Pflegeleistungen abschließen. (vgl. Beck´sche Kurzkommentare DS-GVO- Bertermann, Art. 28 Rdn. 7)

Auftragsverarbeitung liegt (nur) vor, wenn der **Auftragnehmer**:

personenbezogene Daten für den **Auftraggeber** (z.B. im Rahmen einer rein technischen Auslagerung) **streng weisungsgebunden und ohne eigenen Bewertungs- und Entscheidungsspielraum** erhebt, verarbeitet oder nutzt.

Der **Auftraggeber** muss den **Auftragnehmer** unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen **sorgfältig auswählen und** mit ihm eine **präzise Vereinbarung** i.S.v. **Art. 28 Abs. 3 DS-GVO treffen!** Diese muss insbesondere Regelungen enthalten über:

- die nach **Art. 28 Abs. 1 DS-GVO** zu treffenden **technischen** und **organisatorischen Maßnahmen**,
- den **Gegenstand** und die **Dauer der Verarbeitung**, **Art** und **Zweck der Verarbeitung**,
- die **Art der personenbezogenen Daten**, die **Kategorien betroffener Personen**
- die nach **Art. 28 Abs. 3 DS-GVO bestehenden Rechte des Auftraggebers und die nach Abs. 3 h)** bestehenden **Pflichten des Auftragnehmers**, insbesondere die von ihm zu duldenden **Überprüfungen** einschließlich **Inspektionen**,
- **Art** und **Umfang der Weisungsbefugnisse**, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- …

Auftragsverarbeitung liegt (nur) vor, wenn der **Auftragnehmer**:

personenbezogene Daten für den **Auftraggeber** (z.B. im Rahmen einer rein technischen Auslagerung) **streng weisungsgebu** **ohne eigenen Bewertungs- und Entscheidungsspielraum** erhebt, v

Der **Auftraggeber** muss den A sichtigung der Eignung der von ihm getroffenen technischen **fältig auswählen und** mit ihm eine **präzise Vereinbarung** i.S muss insbesondere Regelungen enthalten über:

- die nach **Art. 28 Abs. 1 DS-G anisatorischen Maßnahmen**,
- den **Gegenstand** und die **Dau der Verarbeitung**,
- die **Art der personenbezogenen ener Personen**
- die nach **Art. 28 Abs. 3 DS-GVO bes es Auftraggebers und die nach Abs. 3 h)** bestehenden **Pflichten des Auftragnehmers**, insbesondere die von ihm zu duldenden **Überprüfungen** einschließlich **Inspektionen**,
- **Art** und **Umfang der Weisungsbefugnisse**, die sich der Auftraggeber gegenüber dem

d.h. der Auftraggeber **muss** jederzeit ***„Herr der Daten“*** sein!!!

Auswahl und Überwachung

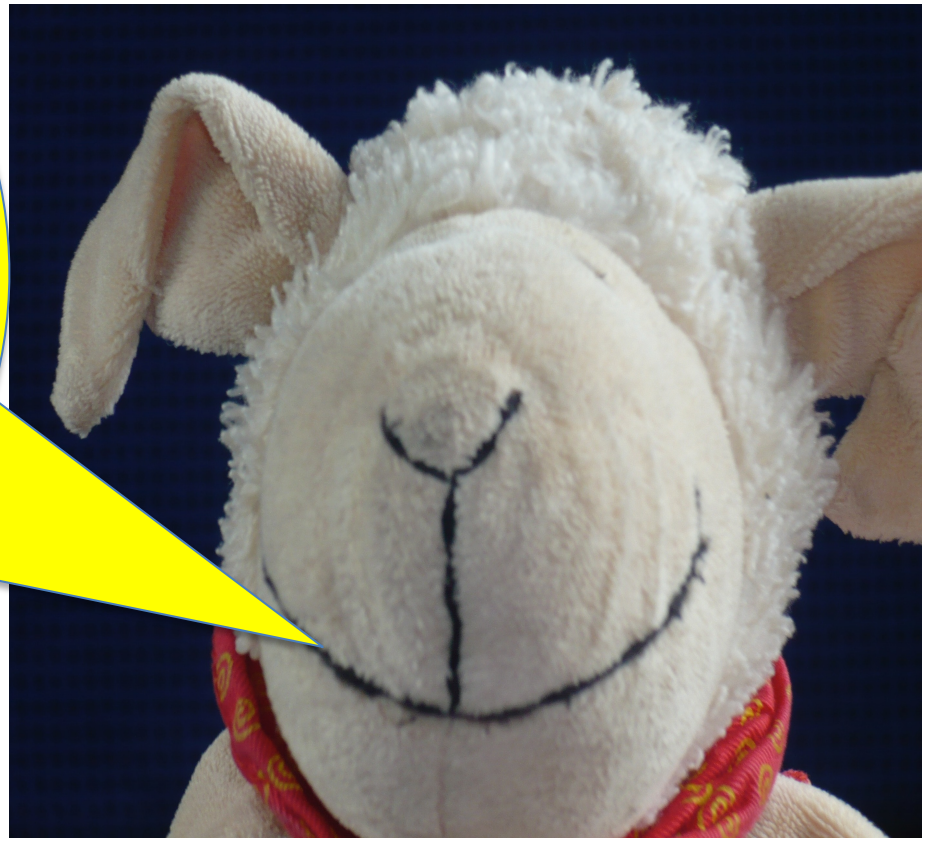
Der **Auftraggeber** muss sich deshalb

- **vor** der Auftragsvergabe von der besonderen fachlichen Eignung des **Auftragnehmers** überzeugen und
- **während** der Auftragsverarbeitung die Einhaltung der vereinbarten **technischen** und **organisatorischen Maßnahmen** regelmäßig kontrollieren.

Er muss sich dabei auf objektiver Basis (z.B. durch **Zertifizierungen**, **regelmäßige Berichtspflichten**, **Auditierung**) die konkrete Gewissheit verschaffen, dass die Einhaltung der gebotenen Schutzstandards gewährleistet ist!*

*so schon Wedde, in Däubler/Klebe/Wedde/Weichert, BDSG, § 11, Rdn. 26;

Sie erinnern sich!?



Systematisch ist den Regelungen gemeinsam, dass **keine konkreten Maßnahmen** vorgegeben werden, sondern dem Verantwortlichen lediglich **Ziele** und **Kriterien** zur Beurteilung der Risikoeinschätzung und Geeignetheit gegeben werden. Hierdurch wird versucht, der **DS-GVO** eine Regelungsdauer zu geben. Der Datenverarbeiter ist in der Verantwortung, technisch und organisatorisch Daten auf dem **aktuellen Stand der Technik** zu verarbeiten. Hilfestellung soll durch Leitlinien und Hinweise des **Europäischen Datenschutzausschusses** (**Art. 68 ff. DS-GVO**), der **Verbände** und der **Datenschutzbeauftragten** erfolgen (s.h. auch. ErwG 77 d. Verordnung). Insbesondere sollen nach **Art. 40 Abs. 2 Buchst. h Verhaltenregeln** aufgestellt werden, die dem Verantwortlichen Hinweise zur Erfüllung seiner Verpflichtungen geben. Hierdurch wird eine kontinuierliche Fortentwicklung auf den jeweils **aktuellen Stand der Technik** ermöglicht.*

Zur Zeit stehen derartige Regelungen und Hilfestellungen noch nicht zur Verfügung. Deshalb sollte auf den schon bisher vom Verantwortlichen nach dem **BDSG** erwarteten Maßnahmen aufgebaut werden. Zu beachten ist aber, dass - anders als bisher - nunmehr auch in diesem Bereich die Einhaltung des „**Stand der Technik**“ vorgegeben ist!

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 24 Rdn. 2

Sie erinnern sich an § 64 BDSG!?

Technische und **organisatorische** Maßnahmen im Sinne von **§ 64 BDSG**

- **Zugangs**kontrolle
- **Datenträger**kontrolle
- **Speicher**kontrolle
- **Benutzer**kontrolle
- **Zugriffs**kontrolle
- **Übertragungs**kontrolle
- **Eingabe**kontrolle
- **Transport**kontrolle
- **Wiederherstellbarkeit**
- **Zuverlässigkeit**
- **Datenintegrität**
- **Auftrags**kontrolle
- **Verfügbarkeits**kontrolle
- **Trennbarkeit**

Vereinbarung über Auftragsverarbeitung nach Art. 28 DS-GVO (Aufbau)

Präambel

1. *Anwendungsbereich*
2. *Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag*
3. *Pflichten des Auftragnehmers*
4. *Pflichten des Auftraggebers*
5. *Anfragen Betroffener an den Auftraggeber*
6. *Kontrollrechte*
7. *Haftung*
8. *Sonstiges*

Anhänge: (Gegenstand und Umfang der Auftragsverarbeitung, Art der Daten, Kreis der Betroffenen, Weisungsberechtigte beim AG, Weisungsempfänger beim AN, technische Einrichtungen zur Auftragsverarbeitung, Datensicherheitskonzept mit Festlegungen entsprechend der Anlage zu § 9 BDSG)

und Achtung:

Art. 28 Abs. 3 DS-GVO lautet:

(3) *Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags** oder eines **anderen Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter **in Bezug auf den Verantwortlichen bindet** und in dem **Gegenstand** und **Dauer der Verarbeitung**, **Art** und **Zweck der Verarbeitung**, die **Art der personenbezogenen Daten**, die **Kategorien betroffener Personen** und die **Pflichten** und **Rechte** des **Verantwortlichen festgelegt sind**. Dieser **Vertrag** bzw. dieses **andere Rechtsinstrument sieht insbesondere vor**, dass der Auftragsverarbeiter: *****

a) *...*

h) *mit Blick auf Unterabsatz 1 Buchstabe h der **Auftragsverarbeiter** **den Verantwortlichen** **unverzüglich informiert**, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.*

und Achtung:

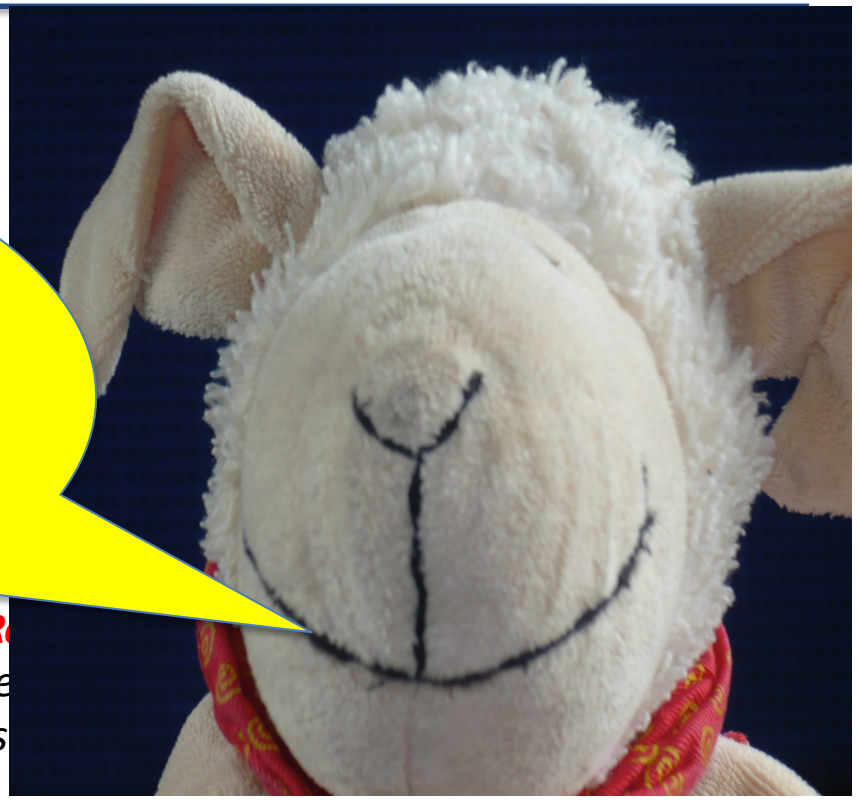
Art. 28 Abs. 3 DS-GVO lautet:

(3) *Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags** oder eines **anderen Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter **in Bezug auf den Verantwortlichen bindet** und in dem **Gegenstand** und **Dauer der Verarbeitung**, **Art** und **Zweck der Verarbeitung**, die **Art der personenbezogenen Daten**, die **Kategorien betroffener Personen** und die **Pflichten** und **Rechte** des **Verantwortlichen festgelegt sind**. Dieser **Vertrag** bzw. dieses **andere Rechtsinstrument sieht insbesondere vor**, dass der Auftragsverarbeiter:*

a) *...*

h) *mit Blick auf Unterabsatz 1 Buchstabe h der **Auftragsverarbeiter den Verantwortlichen unverzüglich informiert**, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.*

und Achtung:



Damit treffen nunmehr den Auftragsverarbeiter eigene, originäre Pflichten, für die er einzustehen hat!!!

Art. 28 A

(

de

Verarb

betroffener *und* ***R***

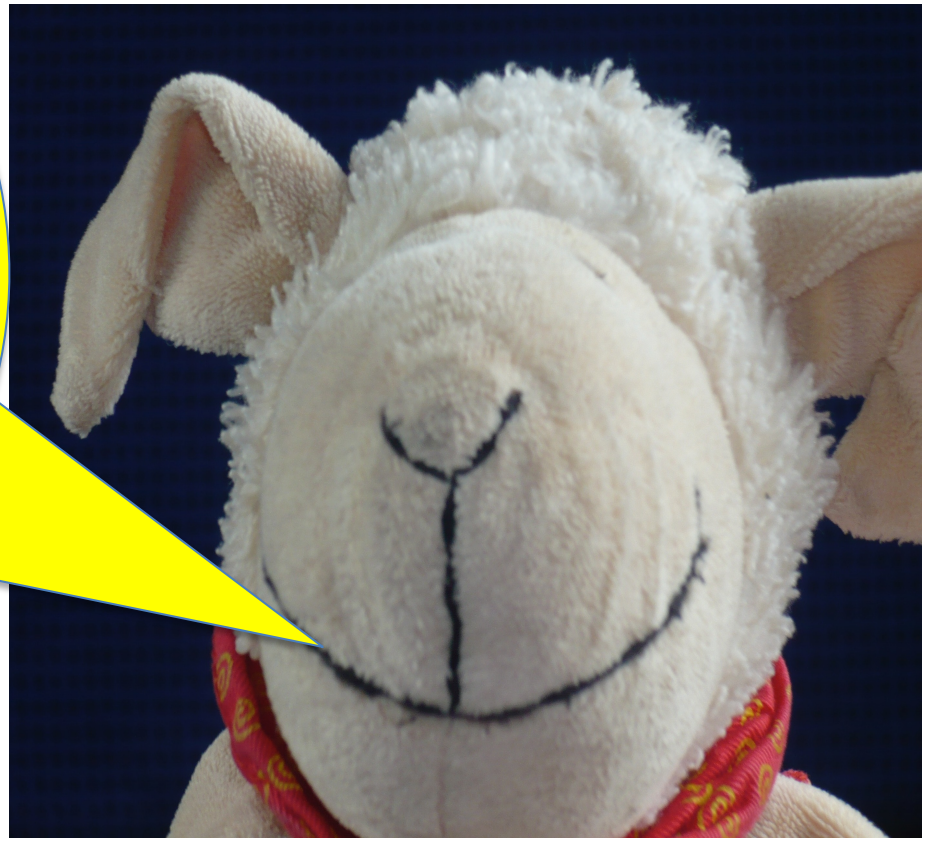
Verantwortlichen festgelegt sind. *Dieser* ***Vertrag*** *bzw. die*

Rechtsinstrument sieht insbesondere vor*, dass der Auftrags*

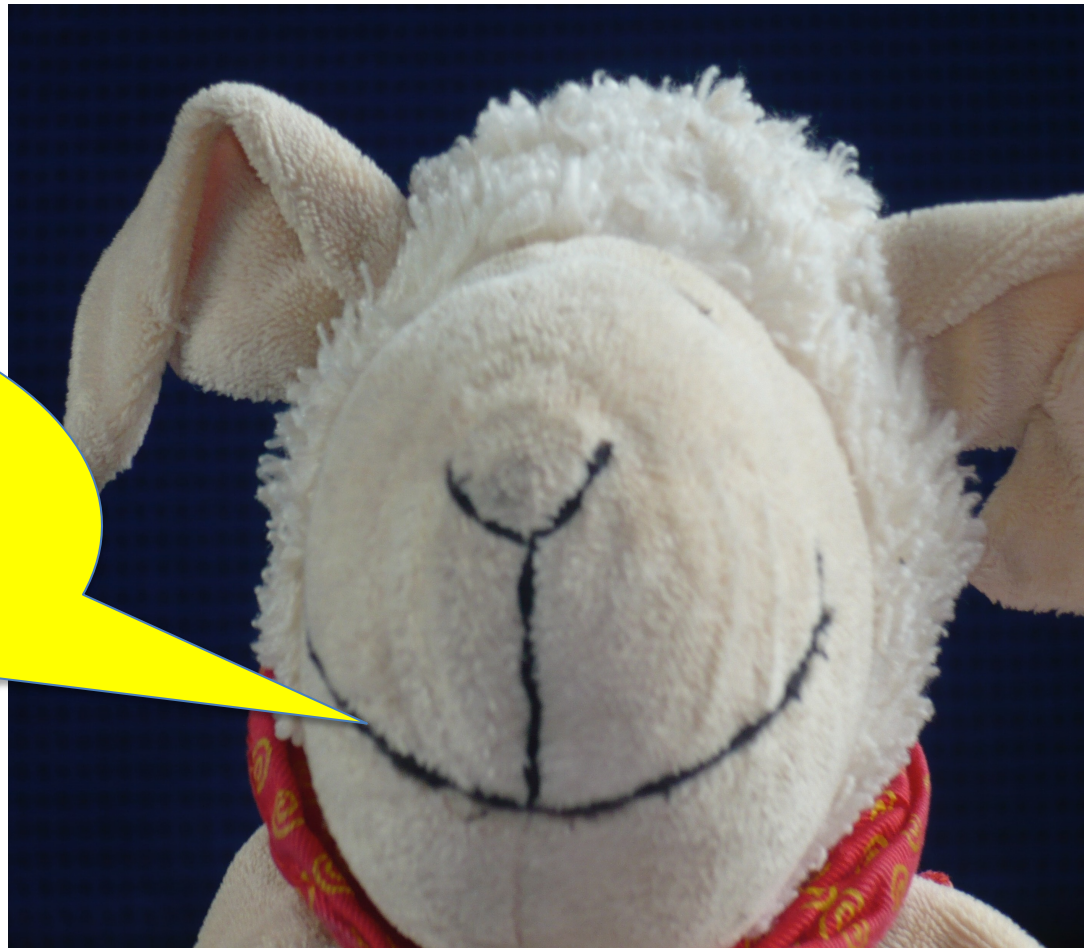
a) *...*

h) *Mit Blick auf Unterabsatz 1 Buchstabe h* ***informiert*** *der* ***Auftragsverarbeiter*** ***den Verantwortlichen*** ***unverzüglich****, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.*

Und das kann teuer werden; aber hierzu noch später!



Das wird noch ergänzt durch Art. 29 DS-GVO!



In **Art. 29 DS-GVO** heißt es insoweit:

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
*Der **Auftragsverarbeiter** und jede dem **Verantwortlichen** oder dem **Auftragsverarbeiter** **unterstellte Person**, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung des Verantwortlichen verarbeiten**, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.*


Das wird dann andersherum ergänzt durch Art. 26 DS-GVO!

Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO

Art. 26 DS-GVO legt fest, dass wenn - wie z.B. innerhalb eines **Wirtschaftskreises** – **mehrere** an der **Verarbeitung** bzw. der **Festlegung der Kriterien der Verarbeitung und der Nutzung** beteiligt sind, auch alle **gemeinsam verantwortlich sind** und der Betroffene seine Ansprüche **jedem gegenüber insgesamt geltend machen kann**.

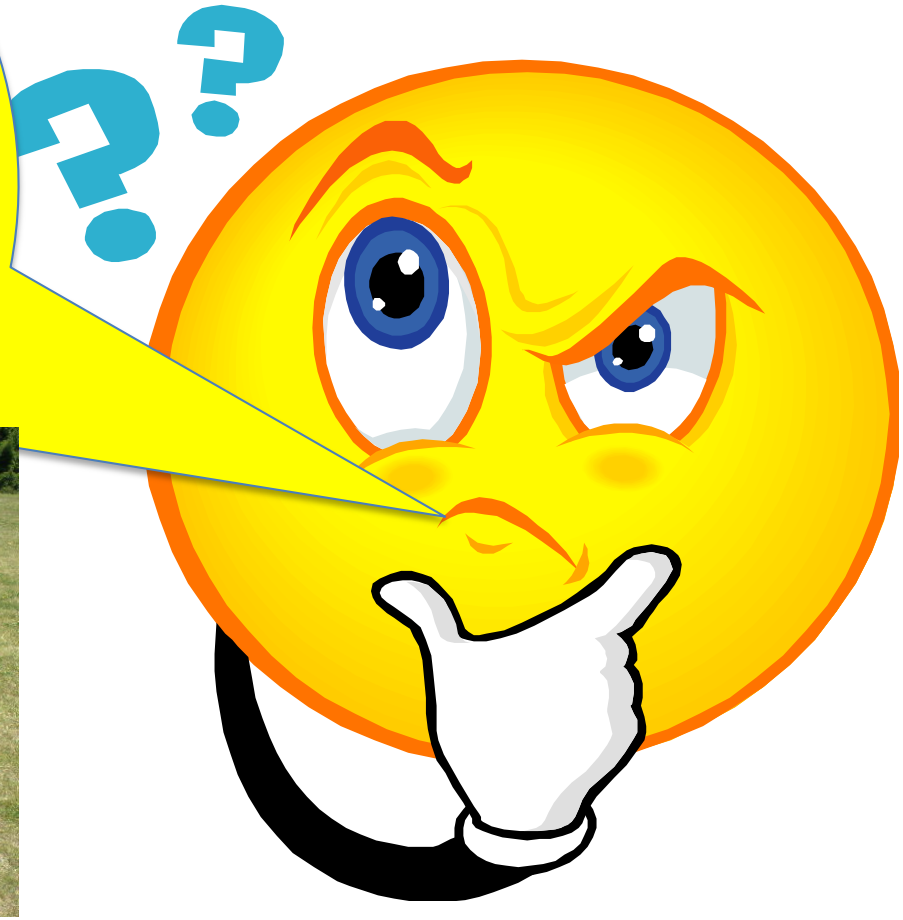
*Anwendungsfelder sind u.a. **Konzerne** (Unternehmensgruppen, **Art. 4 Ziff. 19 DS-GVO**) und **Unternehmens-verbünde**, für die eine gemeinsame Verarbeitung und Nutzung eines Datenpools wichtig ist, aber auch zunehmend für gesamte Wirtschaftssektoren oder ganze Marktsegmente einheitliche Nutzungsangebote, die eine umfassende Zusammenarbeit mehrerer Verantwortlicher entstehen lassen. Hier sind vielfältige Angebote wie **Informationstools für Banken und Versicherungen** und **Buchungsplattformen in der Touristik** zu nennen.**

*Schaffland/Holthaus DS-GVO – Kommentar, Art. 26 Rdn. 5

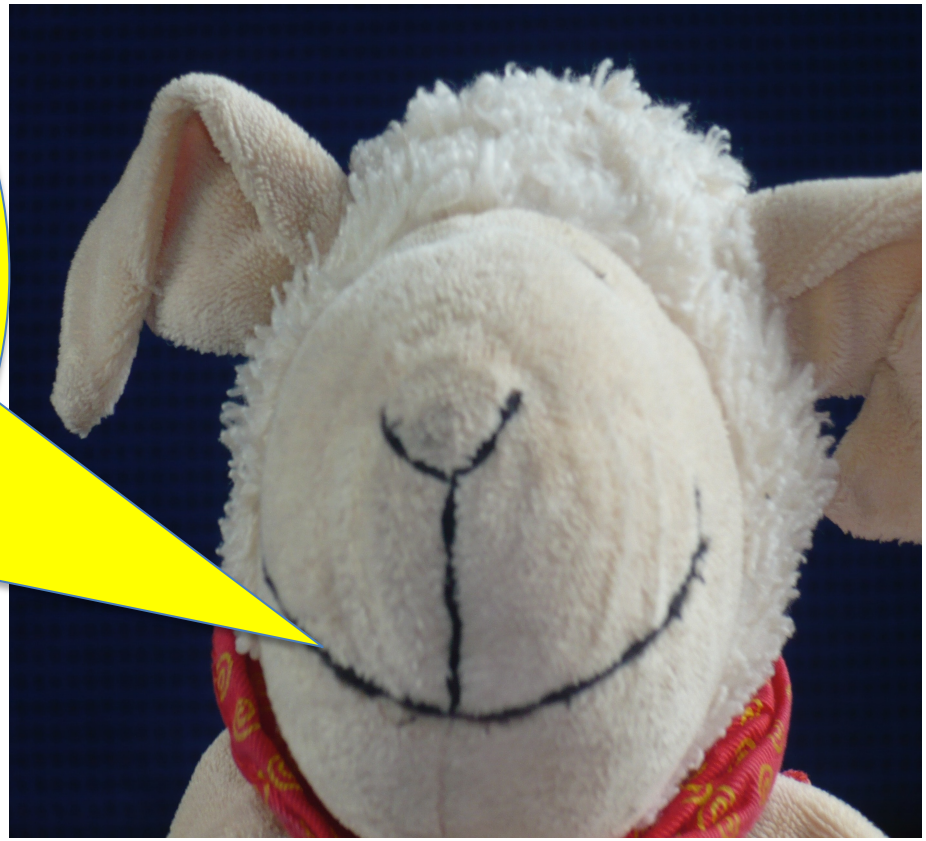

Und das Alles was wir jetzt gehört haben, gildet nun für die ganze Welt!


Natürlich nicht, sondern nur im Rahmen des räumlichen Bereichs der EU.

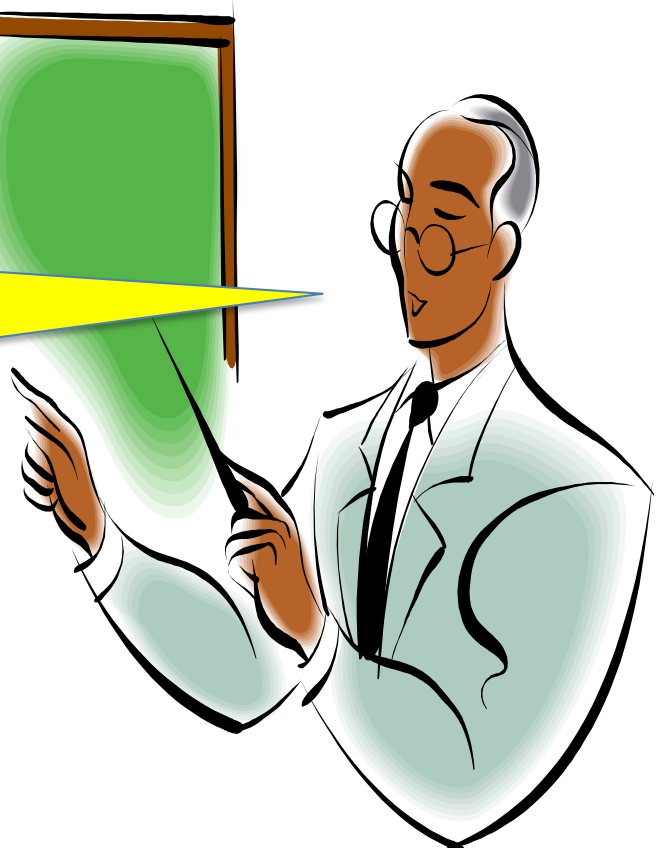
Und wie kann ich nun personenbezogene Daten in die USA schicken?



Natürlich nur unter ganz bestimmten Voraussetzungen!



Sie erinnern sich!?



Soweit ein Unternehmen **personenbezogene Daten** z.B. von **Kunden**, **Patienten**, **Mandanten**, **Lieferanten**, **Mitarbeitern** etc. verarbeitet bzw. nutzt, ist es entweder:

im Unternehmen (selbst) unmittelbar die Daten „verarbeitende“ Stelle

oder

greifen die Grundsätze der „Auftragsverarbeitung“ gemäß Art. 28 DS-GVO ein

Zu berücksichtigen ist ferner noch ob eine Übermittlung/Verarbeitung in

EU bzw. EWR

„Drittländer“ oder internationale Organisationen

stattfindet

Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen, Art. 44 ff DS-GVO

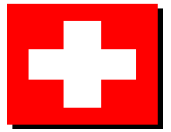
Sollen personenbezogene Daten **in das Ausland** übermittelt werden, so bedarf die Zulässigkeit einer derartigen Übermittlung einer **mehrstufigen Prüfung**:

- Grundsätzlich gelten für die Zulässigkeit die **(allgemeinen) Regeln der DS-GVO (Art. 5 ff DS-GVO)** ggf. i.V.m dem **BDSG sowie** des **bereichsspezifischen Datenschutzes (TKG, TMG)**;

- **Zusätzlich** müssen die datenschutzrechtlichen **Sonderregelungen für die Übermittlung von personenbezogenen Daten in das Ausland** geprüft werden (**Art. 44 ff DS-GVO**):

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, Art. 45 DS-GVO

Die **Kommission** hat eine Reihe von Staaten **als mit einem angemessenen Schutzniveau ausgestattet anerkannt**. Bei diesen Staaten ist eine weitere Prüfung eines angemessenen Schutzniveaus nicht nötig. Hierzu gehören insbesondere:



- **Schweiz** (ABL. EG v. 25.08.2000 Nr. L 215/1)

- **Kanada** (kom. Organisationen) (ABL. EG v. 04.01.2002, Nr. L 2/13)

- **Argentinien** (ABL. EG v. 05.07.2003, Nr. L 187/19)

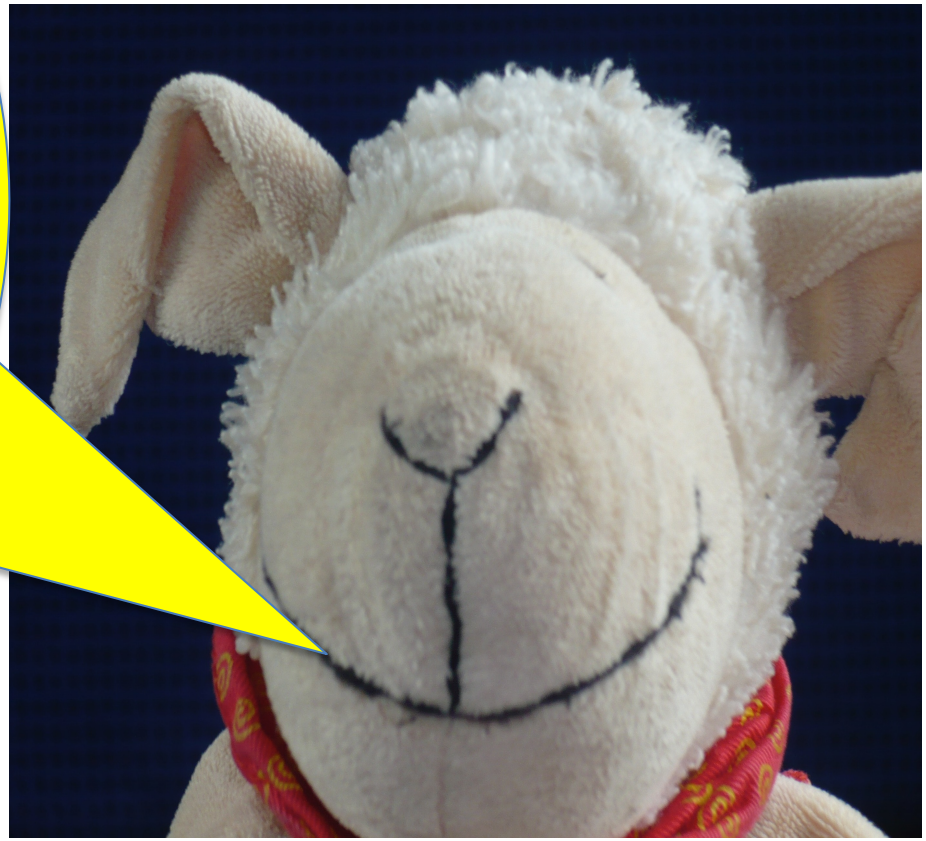
- **Guernsey** (ABL. EG v. 05.07.2003, Nr. L 308/27)

- **Isle of Men** (ABL. EG v. 30.04.2004, Nr. L 151/51)

- **Israel** (ABL. EG v. EG v. 31.01.2011, Nr. L 27/39)

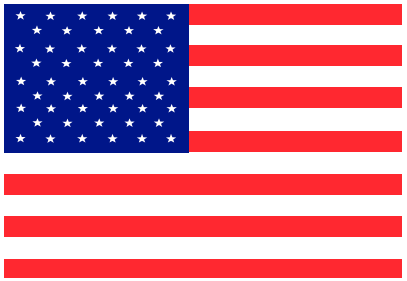
ferner u.a Neuseeland, Uruguay, Jersey, die Färöer-Inseln und Andorra.

Im Rahmen des Urteils *Schrems/Data Protection Commissioner** hat der EuGH Zweifel an der Vereinbarkeit der bisherigen Praxis der Kommission mit EU-Datenschutzrecht, geäußert, so dass die Kommission sich gezwungen sah mit einem neuen Durchführungsbeschluss** strengere Anforderungen aufzustellen, die insbesondere eine regelmäßige Überprüfung des (noch) Vorliegens der Voraussetzungen für einen Angemessenheitsbeschluss vorsehen!



*Rechtssache C-362/14, Maximilian Schrems/Data Protection Commissioner, ECLI:EU:2015:650

** Durchführungsbeschluss (EU) 2016/2295 der Kommission v. 16. Dezember 2016, C(2016) 8353



In Bezug auf die USA war von der EU eine **Sonderlösung** anerkannt worden. In Verhandlungen mit der US-amerikanischen Regierung und der Kommisssion waren vom US-Handelsministerium ausgearbeitete **Grundsätze**, **(„Safe-Harbour-Grundsätze“)** die durch eine Liste „häufig gestellter Fragen“ (FAQ) ergänzt wurden, ausgearbeitet. US-amerikanische Unternehmen, die personenbezogene Daten aus der EU bzw. dem EWR beziehen wollten, mussten sich gegenüber dem US-Handelsministerium verpflichten diese Grundsätze einzuhalten. War dies erfolgt, so war die von der Verpflichtung erfasste Datenübermittlung an das jeweilige US-Unternehmen auch nach EU-Datenschutzrecht rechtmäßig.

- **notice:** Bekanntgabe der Datenverarbeitung an Betroffene;

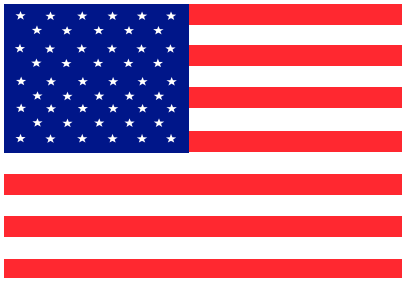
- **choice:** Wahlmöglichkeit des Betroffenen, die Daten nicht weiterleiten zu lassen;

- **onward transfer:** Verpflichtung des Datenempfängers bei Weiterleitung der Daten seinerseits hinreichenden, d.h. diesen Grundsätzen entsprechenden, Datenschutz zu gewährleisten;

- **access:** Anspruch des Betroffenen auf Zugang zu seinen Daten und deren Berichtigung;

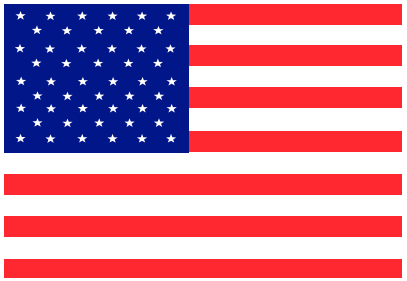
- **security:** personenbezogene Daten sind vor Verlust, Missbrauch, unbefugtem Zugriff, Bekanntgabe, Veränderung und Zerstörung zu schützten.

In Bezug auf die USA war von der EU eine **Sonderlösung** anerkannt worden. In Verhandlungen mit der US-amerikanischen Regierung und der Kommisssion waren vom US-Handelsministerium ausgearbeitete **Grundsätze**, **(„Safe-Harbour-Grundsätze“)** die durch eine Liste „häufig gestellter Fragen“ (FAQ) ergänzt wurden, ausgearbeitet. US-amerikanische Unternehmen, die personenbezogene Daten aus der EU bzw. dem EWR beziehen wollten, mussten sich gegenüber dem US-Handelsministerium verpflichten diese Grundsätze einzuhalten. War dies erfolgt, so war die von der Verpflichtung erfasste Datenübermittlung an das jeweilige US-Unternehmen auch nach EU-Datenschutzrecht rechtmäßig.



Aufgrund des insoweit aber betriebenen häufigen Missbrauchs durch US-amerikanische Unternehmen, wird eine Berufung auf die Safe-Harbor-Principles von deutschen Datenschützern jedenfalls als nicht mehr ausreichend angesehen.
So hat sich durch die Galexia Studie* nachweisen lassen, dass von den ca. 1700 offiziell zertifizierten Unternehmen nur 348 Unternehmen die Kriterien des Abkommens tatsächlich einhalten!
Darüber hat jetzt der EuGH (Urt. v. 6.10.2015 – Rs. C-362/14 – *Maximilian Schrems vs. Data Protection Commissioner*) entschieden, die Entscheidung 2000/520/EG der Kommission v. 26.07.2000 über die Angemessenheit des über „*Safe Harbour*“ gewährleisteten Schutzes für Unionsbürger, ungültig ist!

*Conolly, The US Safe Harbor – Fact or Fiction; abrufbar unter www.galexis.com



In Bezug auf die USA war von der EU eine **Sonderlösung** anerkannt worden. In Verhandlungen mit der US-amerikanischen Regierung und der Kommisssion waren vom US-Handelsministerium ausgearbeitete **Grundsätze**, **(„Safe-Harbour-Grundsätze“)** die durch eine Liste „häufig gestellter Fragen“ (FAQ) ergänzt wurden, ausgearbeitet. US-amerikanische Unternehmen, die personenbezogene Daten aus der EU bzw. dem EWR beziehen wollten, mussten sich gegenüber dem US-Handelsministerium verpflichten diese Grundsätze einzuhalten. War dies erfolgt, so war die von der Verpflichtung erfasste Datenübermittlung an das jeweilige US-Unternehmen auch nach EU-Datenschutzrecht rechtmäßig.

Auch die Nachfolgevereinbarung der sog. „***Privacy Shield***“ oder „***Privacy Act***“bzw. der entsprechende Durchführungsbeschluss* ist, nachdem Präsident Donald Trump am 25. Januar 2017 eine Anordnung unterzeichnet hat, der zufolge die Geltung des *Privacy Acts* für Personen, die **keine US-amerikanischen Staatsangehörigen** oder **keine ständigen rechtmäßigen Einwohner der USA sind**, ausgeschlossen sei, **nicht geeignet** eine **tragfähige Rechtsgrundlage** für einen Austausch von **personenbezogenen Daten** mit den USA zu ermöglichen, da es durch die Anordnung zweifelhaft ist, ob noch von einem „**angemessenen Datenschutzniveau**“ für EU-Bürger ausgegangen werden kann.
Darüber hinaus hat das Europäische Parlament am 6. April 2017 eine kritische Resolution zum “***Privacy Shield***“ verabschiedet und darin erhebliche Defizite beim Datenschutz festgestellt.

*Durchführungsbeschluss (EU) 2016/1250 d. Kommission v. 12.07.2016, C (2016) 4776


Und dann ist da noch die NSA!!!

Datenübermittlung vorbehaltlich geeigneter Garantien, Art. 46 DS-GVO

Falls **kein Angemessenheitsbeschluss** nach **Artikel 45 Absatz 3** vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein **Drittland** oder eine **internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen**.

Geeignete Garantien können u.a. sein:

- **ein rechtlich bindend** und **durchsetzbares Dokument** zwischen den Behörden oder öffentlichen Stellen,
- **verbindliche interne Datenschutzvorschriften** gemäß **Artikel 47 DS-GVO**, „**code of conduct**“ s.u.
- **Standarddatenschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach **Artikel 93 Absatz 2** erlassen werden,
- **genehmigte Verhaltensregeln** gemäß **Artikel 40 DS-GVO zusammen mit rechtsverbindlichen** und **durchsetzbaren Verpflichtungen** des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland **zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen**, oder
- **ein genehmigter Zertifizierungsmechanismus** gemäß **Artikel 42 DS-GVO zusammen mit rechtsverbindlichen** und **durchsetzbaren Verpflichtungen** des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland **zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen**.



Da die EU-Datenschutzstandards im weltweiten Vergleich als sehr hoch zu bewerten sind, hat die EU-Kommission veranlasst, **Standardvertragsklauseln** zu beschließen, deren Verwendung ein angemessenes datenschutzrechtliches Niveau gewährleistet.
Sofern sich der ausländische Datenempfänger auf die Einhaltung der **EU-Standardvertragsklauseln** **verpflichtet**, ist damit nach deutschem Datenschutzrecht ein **angemessenes Datenschutzniveau** gewährleistet.

Verbindliche interne Datenschutzvorschriften, Art. 47 DS-GVO

Eine datenschutzrechtliche Absicherung kann auch mittels eines **Codes of Conduct** erfolgen. Hierbei handelt es sich um die verbindliche Vereinbarung zwischen Unternehmen (z.B. konzernweite verbindliche **Verhaltenskondizies** / **Code of Conduct** für multinationale Konzerne) z.B. in Form von „**Binding Corporate Rules (BCR)**“.

Hierbei handelt es sich um die **Umsetzung** bzw. die **rechtliche Ausgestaltung** des sog. „***Konzernprivilegs***“, mit dem es **international agierenden Unternehmen** unter bestimmten Voraussetzungen ermöglicht werden soll, auf vereinfachte Art und Weise **unternehmensintern personenbezogene Daten** von **Unternehmensangehörigen** auszutauschen bzw. zu verarbeiten.

Ein Austausch innerhalb der Unternehmensgruppe bzw. des Konzerns **soll möglich sein**, **wenn es rechtsverbindliche interne Datenschutzvorschriften** gibt, die es dem Betroffenen ermöglichen seine der DS-GVO entsprechenden **Rechte erfolgreich durchzusetzen**.

Verbindliche interne Datenschutzvorschriften, Art. 47 DS-GVO

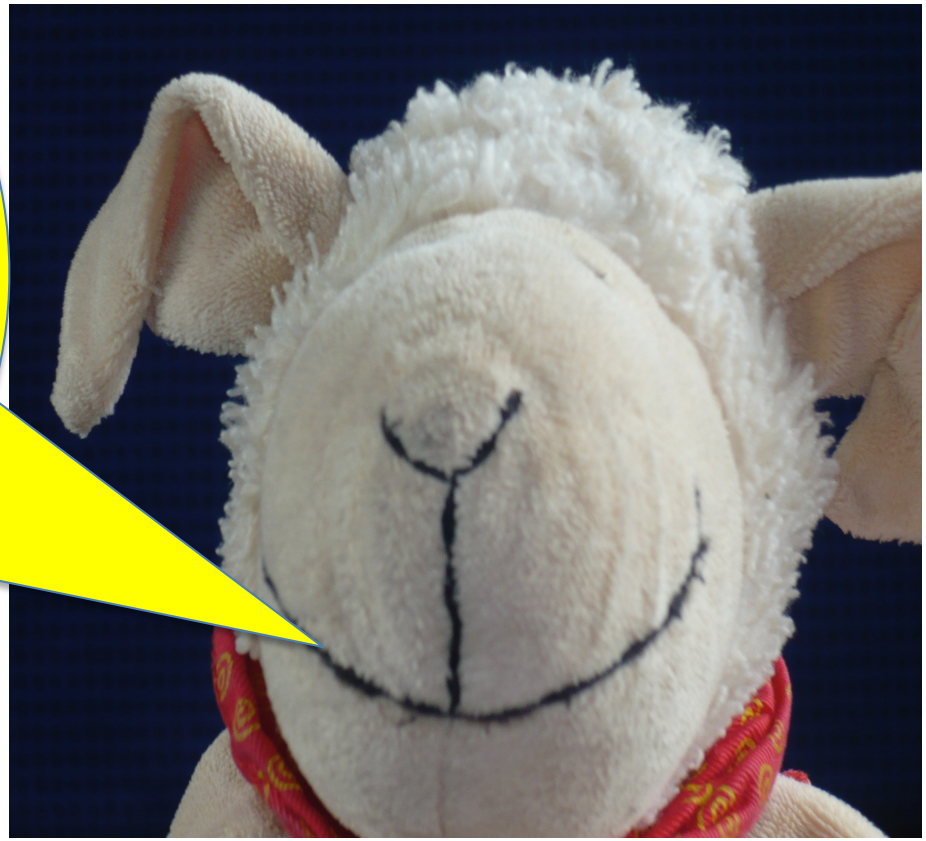
Eine datenschutzrechtliche Absicherung kann auch mittels eines **Codes of Conduct** erfolgen. Hierbei handelt es sich um die verbindliche Vereinbarung zwischen Unternehmen (z.B. konzernweite verbindliche **Verhaltenskondizies** / **Code of Conduct** für multinationale Konzerne) z.B. in Form von „**Binding Corporate Rules (BCR)**“.

Hierbei handelt es sich um die **Umsetzung** bzw. die **rechtliche Ausgestaltung** des sog. „***Konzernprivilegs***“, mit dem es **international agierenden Unternehmen** unter bestimmten Voraussetzungen ermöglicht werden soll, auf vereinfachte Art und Weise **unternehmensintern personenbezogene Daten** von **Unternehmensangehörigen** auszutauschen bzw. zu verarbeiten.

Ein Austausch innerhalb der Unternehmensgruppe bzw. des Konzerns **soll möglich sein**, **wenn es rechtsverbindliche interne Datenschutzvorschriften** gibt, die es dem Betroffenen ermöglichen seine der DS-GVO entsprechenden **Rechte erfolgreich durchzusetzen**.

Zu beachten ist, dass es im deutschen Datenschutzrecht **kein „*Konzernprivileg*“** gab, so dass **jede** Überlassung personenbezogener Daten an eine ausländische (z.B. US-) Konzernmutter, die für die Übermittlung personenbezogener Daten an Dritte geltenden datenschutzrechtlichen Anforderungen erfüllen musste. Bereits **die Ermöglichung des Zugriffs** reichte in diesem Zusammenhang aus, da gemäß **§ 3 Nr. 3b BDSG** der datenschutzrechtliche Begriff der „***Übermittlung***“ den Abruf personenbezogener Daten durch Dritte einschloss.

Natürlich nur unter ganz bestimmten und engen Voraussetzungen!



Ausnahmen für bestimmte Fälle, Art. 49 DS-GVO

Art. 49 DS-GVO enthält einen Katalog von **Ausnahmen** bei denen eine Übermittlung an Stellen bei denen **kein** angemessenes Datenschutzniveau gewährleistet ist, **auch ohne ausdrückliche Einwilligung dennoch zulässig ist**; dies ist der Fall, wenn:

- die Übermittlung **für die Erfüllung eines Vertrages** zwischen dem Betroffenen und der verantwortlichen Stelle **oder zur Durchführung von vorvertraglichen Maßnahmen** die **auf Veranlassung des Betroffenen** getroffen worden sind, erforderlich sind;*

- die Übermittlung **zum Abschluss oder zur Erfüllung eines Vertrages erforderlich ist** der **im Interesse des Betroffenen** von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll;**

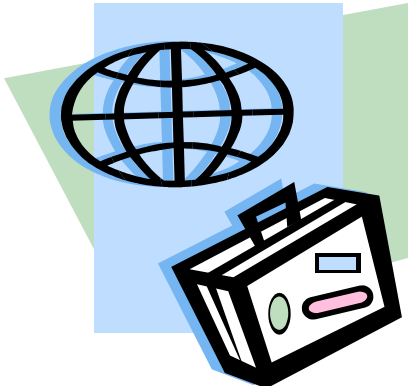
- die Übermittlung **zur Wahrung eines wichtigen öffentlichen Interesses** oder **zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** vor Gericht erforderlich ist;

- die Übermittlung **zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist** oder

- die Übermittlung **aus einem Register erfolgt, dass zur Information der Öffentlichkeit bestimmt ist** und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigten Interesses nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Übermittlung für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen die **auf Veranlassung des Betroffenen** getroffen worden sind:

Klassischer Beispielsfall ist die **Hotelbuchung** durch das Reisebüro im Ausland. Das Reisebüro darf nur die Kundendaten, in dem für die Buchung erforderlichen Umfang an das Ausland übermitteln.



Übermittlung zum Abschluss oder zur Erfüllung eines Vertrages, der **im Interesse des Betroffenen** von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossenen werden soll erforderlich:

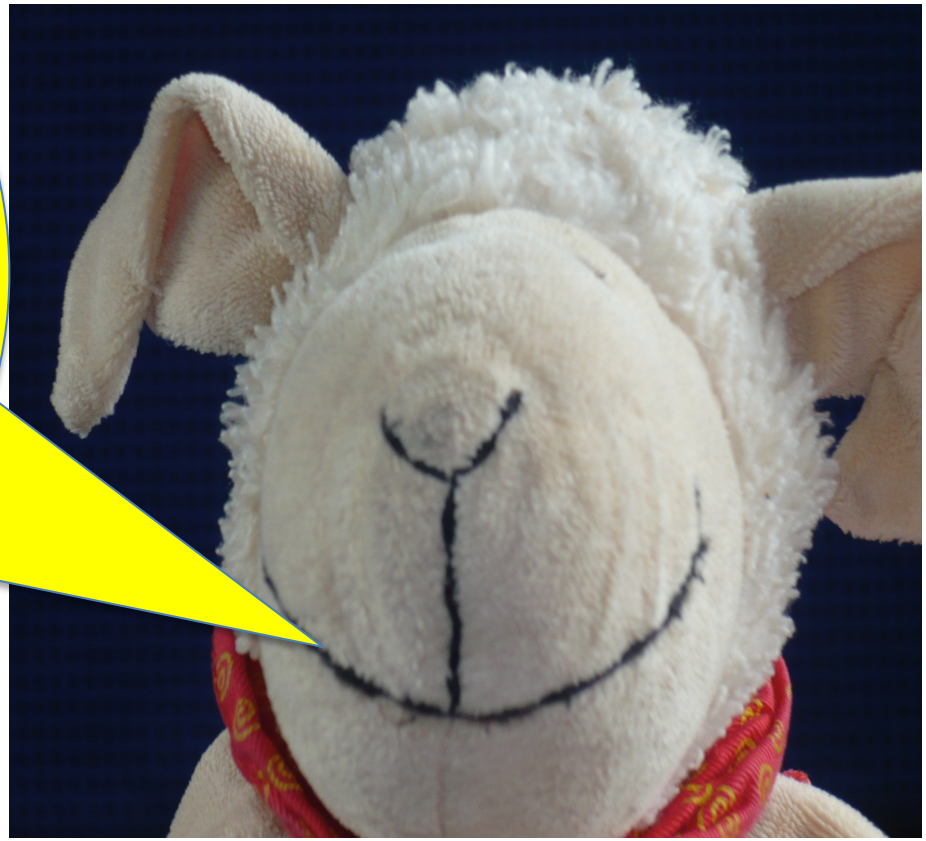
Hierher gehören z.B. **Buchungen des Hotels vor Ort, in Bezug auf weitere Aktivitäten des Gastes** (z.B.: Auto, Tauchschule, Golfclub, Surfen usw.)

In jedem Fall ist die Stelle an die die Daten übermittelt werden, darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden


Puuh, das nimmt ja kein Ende!
Was muss uns denn noch interessieren?

Na ist doch klar:

- **Kontrolle**
- **Rechtsbehelfe**
- **Haftung und**
- **Sanktionen**



Um die Anforderungen des Datenschutz auch **zielgerichtet durchsetzen** zu können, bedarf es selbstverständlich einiger **wirksamer Kontrollmechanismen** und **Durchsetzungsmöglichkeiten**.

Zu nennen sind zunächst die hierzu berufenen Institutionen:

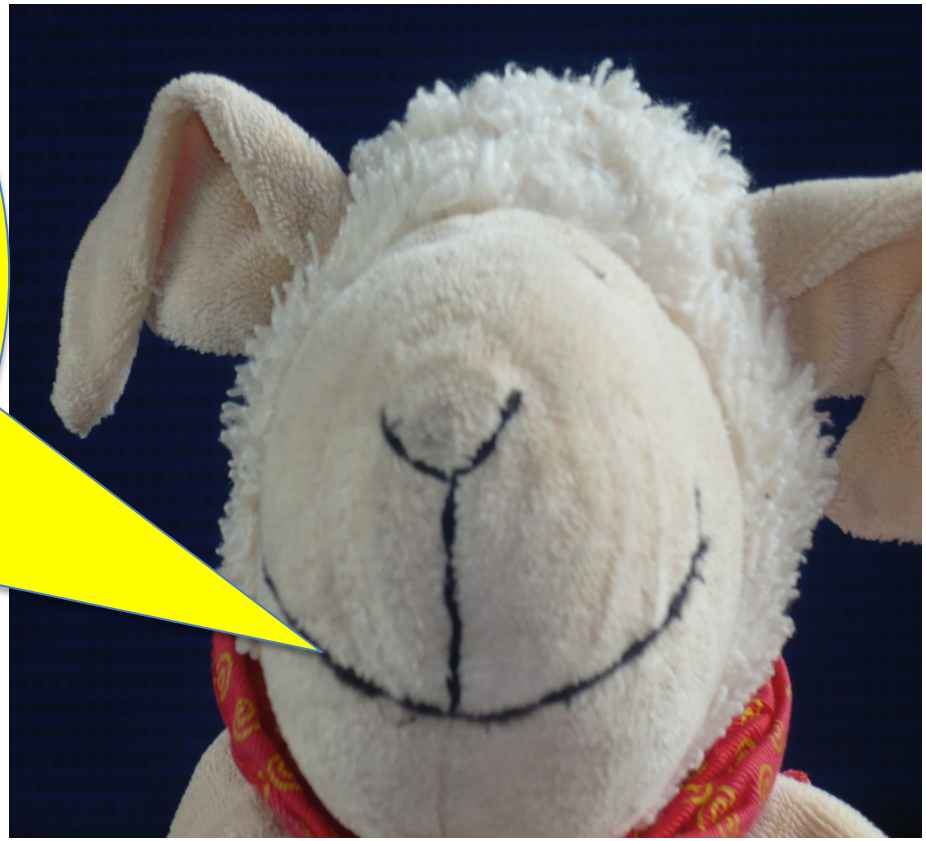
- der **Datenschutzbeauftragte**
- die **Aufsichtsbehörde(n)**
- die **Gerichte**

Zu nennen sind ferner die zur Verfügung gestellten Rechtsmittel:

- Das **Recht auf Beschwerde** bei einer **Aufsichtsbehörde** gem. **Art. 77 DS-GVO**
- Das **Recht auf gerichtlichen Rechtsbehelf** gegen eine **Aufsichtsbehörde** gem. **Art. 78 DS-GVO**
- Das **Recht auf gerichtlichen Rechtsbehelf** gegen **Verantwortliche** und **Auftragsverarbeiter** gem. **Art. 79 DS-GVO**

- Das **Recht auf Schadensersatz** gem. **Art. 82 DS-GVO**
- **Geldbußen** gem. **Art. 83 DS-GVO**
- **Sanktionen** gem. **Art. 84 DS-GVO**

Auf geht's mit dem
Datenschutzbeauftragten



Datenschutzbeauftragter, Art. 37 DS-GVO

Ein **Datenschutzbeauftragter** ist gem. **Art. 37 DS-GVO** insbesondere zu bestellen wenn:

- die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters **in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen**, oder
- die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters **in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9** oder **von personenbezogenen Daten über strafrechtliche Verurteilungen** und **Straftaten gemäß Artikel 10 besteht**.

Im Übrigen **können** der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, **einen Datenschutzbeauftragten benennen**; **falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen**.

Datenschutzbeauftragter, Art. 37 DS-GVO

Ein **Datenschutzbeauftragter** ist gem. **Art. 37 DS-GVO** insbesondere zu bestellen wenn:

- …rbeiters **in der Durchführung von** …Umfangs und/oder ihrer Zwecke …ung von betroffenen Personen

…rbeiters **in der umfangreichen** …r von personenbezogenen Daten **besteht**.

Das ist in der Bundesrepublik mit dem *Datenschutz-Anpassungs- und Umsetzungsgesetz EU*
– DSAnpUG-EU –
insbesondere im Rahmen des schon bestehenden *Bundesdatenschutzgesetz*
- BDSG -
Im Rahmen des § 38 BDSG erfolgt!
Es lautet dort:

„Ergänzend zu Art. 37 Abs. 1 b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsdatenverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.“

Stellung des Datenschutzbeauftragten, Art. 38 DS-GVO

Der Verantwortliche und der Auftragsverarbeiter sind gem. **Art. 38 Abs. 3 DS-GVO** verpflichtet, **sicherzustellen**, **dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält**. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben **nicht abberufen oder benachteiligt werden**. **Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters**.

Der **Datenschutzbeauftragte** ist gem. **Art. 38 Abs. 5 DS-GVO** nach dem Recht der Union oder der Mitgliedstaaten **bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden**.

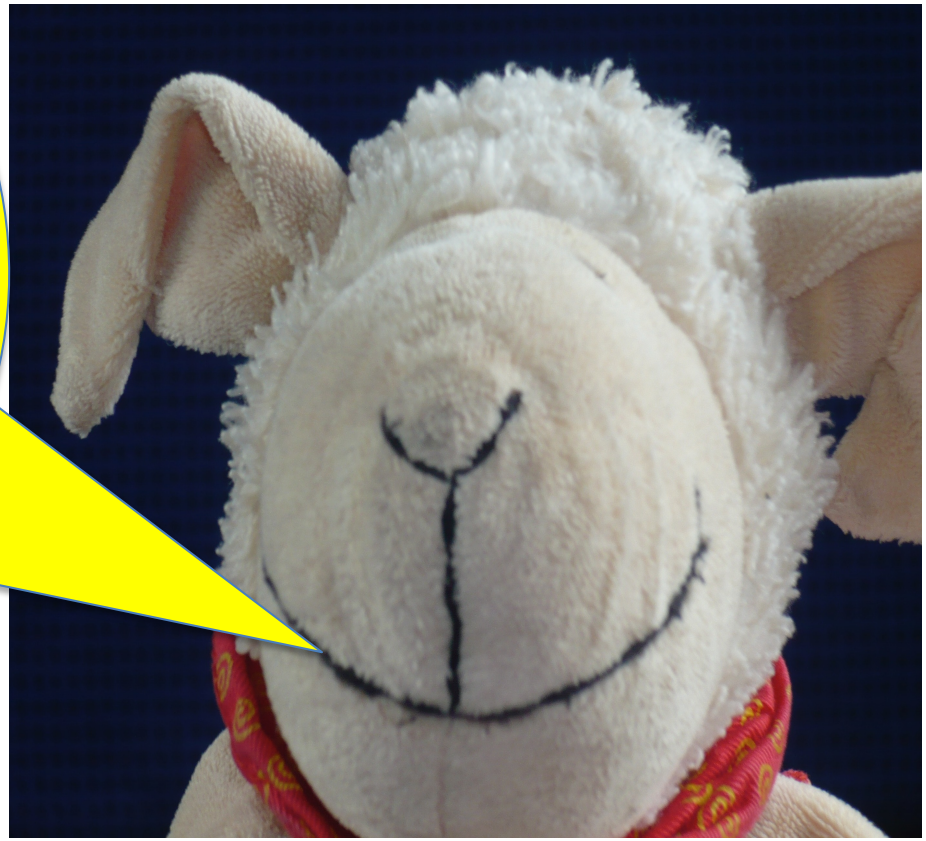
Der Datenschutzbeauftragte **kann** andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter sind gem. **Art. 38 Abs. 6 DS-GVO** verpflichtet **sicherzustellen**, **dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen**.

Aufgaben des Datenschutzbeauftragten, Art. 39 DS-GVO

Dem **Datenschutzbeauftragten** obliegen nach **Art. 39 DS-GVO** zumindest folgende **Aufgaben**:

- **Unterrichtung** und **Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- **Überwachung** der **Einhaltung** dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- **Beratung** — auf Anfrage — im Zusammenhang mit der **Datenschutz-Folgenabschätzung** und **Überwachung ihrer Durchführung** gemäß **Artikel 35**;
- **Zusammenarbeit** mit der **Aufsichtsbehörde**;
- **Tätigkeit als Anlaufstelle** für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß **Artikel 36**, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Jetzt kommen die
Rechtsmittel!



Recht auf Beschwerde bei einer Aufsichtsbehörde, Art. 77 DS-GVO

Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs, das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

In **Art. 77 DS-GVO** heißt es insoweit:

Recht auf Beschwerde bei einer Aufsichtsbehörde

*(1) **Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde**, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.*

*(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach **Artikel 78**.*

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde, Art. 78 DS-GVO

- Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.
- Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 55 und 56 DS-GVO zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 77 DS-GVO erhobenen Beschwerde in Kenntnis gesetzt hat.

Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde, Art. 78 DS-GVO

- Jede natürlich… anderweitigen verwaltungsr…cht auf einen wirksamen g…tsverbindlichen Beschluss ein…
- Jede betroffe…ungsrechtlichen oder außerg…n gerichtlichen Rechtsbehelf,…VO zuständige Aufsichtsbeh…roffene Person nicht innerha…emäß Artikel 77 DS-GVO erhobe…

Gemäß § 20 BDSG ist in Ergänzung der DS-GVO für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und einer Aufsichtsbehörde des Bundes oder eines Landes der Verwaltungsrechtsweg gegeben!

Örtlich zuständig ist das Verwaltungsgericht in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat.

Ein Vorverfahren findet nicht statt!

Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter, Art. 79 DS-GVO

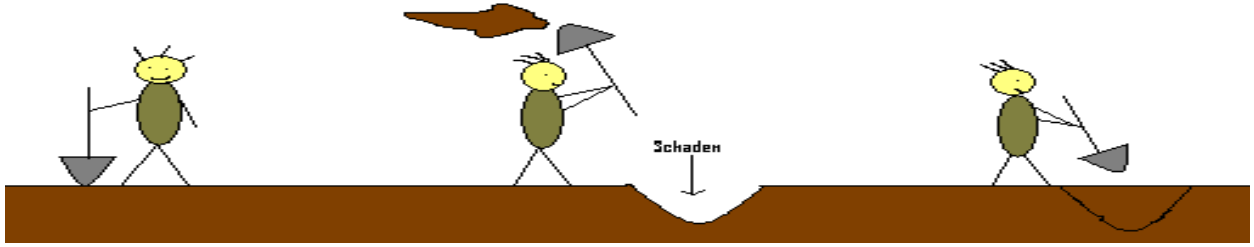
Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 DS-GVO das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat.

Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat.

Haftung und Recht auf Schadensersatz, Art. 82 DS-GVO

Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat gem. Art. 82 Abs. 1 DS-GVO Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.



Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für **den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde.**

Auch **Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden gem. Art. 82 Abs. 2 DS-GVO dann**, wenn er seinen, d.h. **speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist** oder **unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.**

Ist mehr als ein Verantwortlicher oder mehr als ein **Auftragsverarbeiter bzw. sowohl ein Verantwortlicher, als auch ein Auftragsverarbeiter** an derselben Verarbeitung beteiligt **und** sind sie gemäß den Absätzen 2 und 3 für **einen** durch die Verarbeitung verursachten Schaden verantwortlich, **so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.**

Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 DS-GVO

Jede Aufsichtsbehörde hat gem. Art. 83 Abs. 1 DS-GVO sicherzustellen, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung in jedem Einzelfall

- wirksam,
- verhältnismäßig und
- abschreckend ist.

Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 DS-GVO

Geldbußen werden gem. **Art. 83 Abs. 2 DS-GVO** je nach den Umständen des **Einzelfalls zusätzlich zu** oder **anstelle von** Maßnahmen nach **Artikel 58 Absatz 2 Buchstaben a** bis **h** und **i** (**Überprüfung und Abhilfe**) verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in **jedem Einzelfall Folgendes gebührend berücksichtigt**:

- die **Art**, **Schwere** und **Dauer des Verstoßes** unter Berücksichtigung der **Art**, des **Umfangs** oder des **Zwecks** der **betreffenden Verarbeitung** sowie der **Zahl** der von der Verarbeitung **betroffenen Personen** und des **Ausmaßes** des von ihnen **erlittenen Schadens**;
- **Vorsätzlichkeit** oder **Fahrlässigkeit des Verstoßes**;
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter **getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens**;
- der **Grad der Verantwortung** des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den **Artikeln 25** und **32** getroffenen **technischen** und **organisatorischen Maßnahmen**;
- etwaige **einschlägige frühere Verstöße** des Verantwortlichen oder des Auftragsverarbeiters;
- der **Umfang der Zusammenarbeit mit der Aufsichtsbehörde**, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
- die **Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind;
- die **Art** und **Weise**, **wie der Verstoß der Aufsichtsbehörde bekannt wurde**, insbesondere **ob** und gegebenenfalls **in welchem Umfang** der Verantwortliche oder der Auftragsverarbeiter **den Verstoß mitgeteilt hat**;
- die **Einhaltung** der **früher** gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter **in Bezug auf denselben Gegenstand angeordneten Maßnahmen**;
- die **Einhaltung** von **genehmigten Verhaltensregeln** oder **genehmigten Zertifizierungsverfahren und**
- jegliche **anderen erschwerenden** oder **mildernden Umstände** im jeweiligen Fall, wie **unmittelbar** oder **mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste**.

Allgemeine Bedingungen für die Verhängung von Geldbußen, Art. 83 DS-GVO

Bei **Verstößen** gegen die Bestimmungen der **DS-GVO** können **Geldbußen** von bis zu **10.000.000 €** oder **im Fall eines Unternehmens** von bis zu **2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist**.

Bei **schweren Verstößen** gegen die Bestimmungen der **DS-GVO** können **Geldbußen** von bis zu **20.000.000 €** oder **im Fall eines Unternehmens** von bis zu **4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.**

Bei **Verstößen** gegen die **Anweisung der Aufsichtsbehörde** können ebenfalls **Geldbußen** von bis zu **20.000.000 €** oder **im Fall eines Unternehmens** von bis zu **4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.**

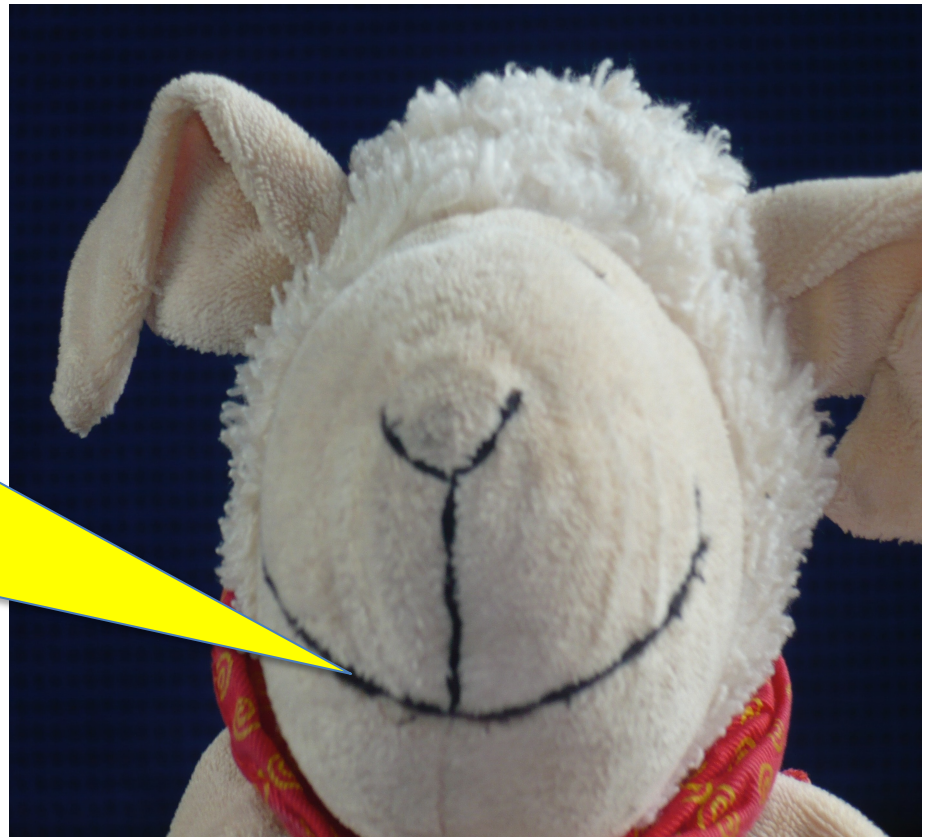
Sanktionen, Art. 84 DS-GVO

Die Mitgliedstaaten können Vorschriften über **andere Sanktionen für Verstöße gegen diese Verordnung — insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen — festlegen und treffen alle zu deren Anwendung erforderlichen Maßnahmen.**

Auch **diese Sanktionen müssen**

- **wirksam,**
- **verhältnismäßig und**
- **abschreckend sein.**

*„Nun stehen wir selbst und sehn betroffen, den Vorhang zu und viele Fragen offen!“**



*frei nach Berthold Brecht, Der gute Mensch von Sezuan

Herzlichen Dank für ihre Aufmerksamkeit!

Rechtsanwalt Prof. Wolfgang Müller
Fachanwalt für Informationstechnologierecht
Fachanwalt für Bau- und Architektenrecht
Schlichter nach SOBau
Honorarprofessor der TU Dortmund
Lehrbeauftragter der FH Dortmund

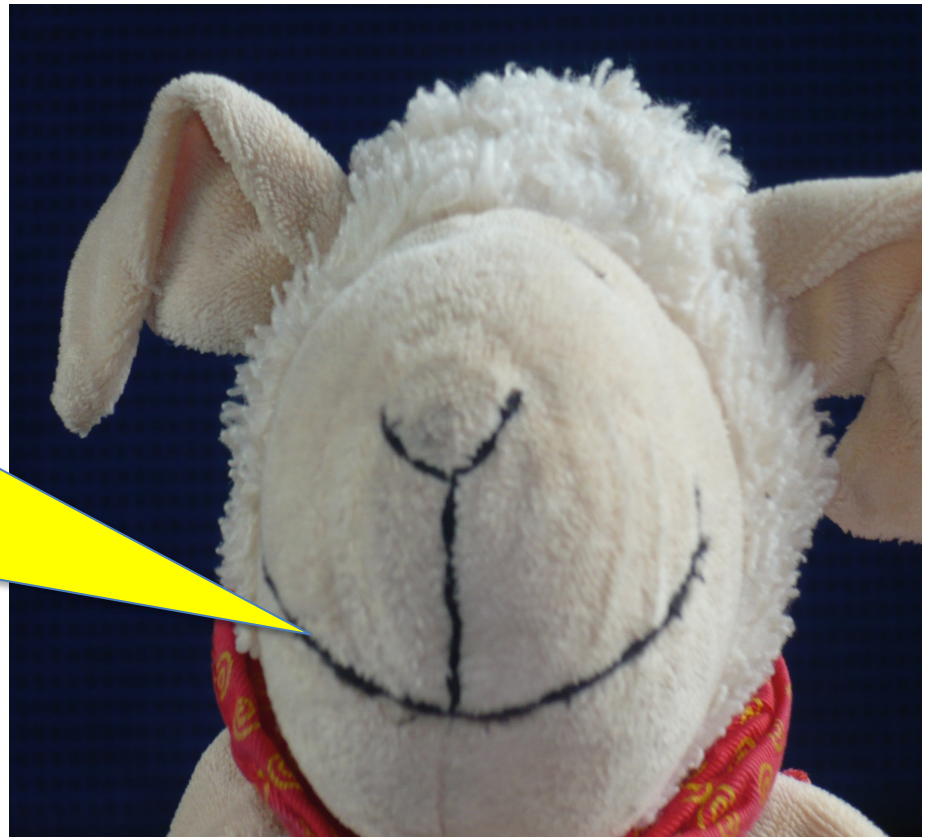
Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai

Herzlichen Dank für ihre Aufmerksamkeit!

Rechtsanwalt Prof. Wolfgang Müller
Fachanwalt für Informationstechnologierecht
Fachanwalt für Bau- und Architektenrecht
Schlichter nach SOBau
Honorarprofessor der TU Dortmund
Lehrbeauftragter der FH Dortmund

Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai

Die „wesentlichen“ Neuerungen nochmals im Überblick:



- Die DS-GVO gilt ab dem 25. Mai 2018 einheitlich in allen Staaten der EU!
- Auch unter der DS-GVO gilt das Verbotsprinzip mit Erlaubnisvorbehalt, d.h. jegliche Verarbeitung darf nur erfolgen soweit die Einwilligung des Betroffenen vorliegt oder ein Gesetz es erlaubt!
- Auch DS-GVO kennt die Verarbeitung von personenbezogenen Daten auf Weisung des Verantwortlichen durch einen Dritten, indes heißt dies nicht mehr *„Auftragsdatenverarbeitung“* sondern *„Auftragsverarbeitung“* und dies bedingt den Abschluss einer dementsprechenden neuen Vereinbarung! Den Auftragsverarbeiter treffen eigene Pflichten!
- Der Betroffene hat ein Recht auf *„Vergessenwerden“*!
- Der Betroffene hat ein Recht auf *„Datenübertragbarkeit“*!
- Der Schutz der Daten des Betroffenen ist vom Verantwortlichen und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik sicherzustellen!
- Der Datenschutz ist dabei insbesondere schon vorab d.h. vor der eigentlichen Erhebung/Verarbeitung von Daten bereits durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umzusetzen!
- Nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter die in der Union Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen beobachten, haben schriftlich einen Vertreter in der Union zu benennen!
- Durch den Verantwortlichen und den Auftragsverarbeiter ist ein *„Verarbeitungsverzeichnis“* zu führen!

- Der Verantwortliche ist verpflichtet, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten des Betroffenen zur Folge hat, vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten („*Datenschutz-Folgenabschätzung*“) durchzuführen !

- Sind z.B. im Rahmen eines Wirtschaftskreises – mehrere an der Verarbeitung bzw. der Festlegung der Kriterien der Verarbeitung und der Nutzung beteiligt, sind auch alle gemeinsam verantwortlich und kann der Betroffene seine Ansprüche auch jedem gegenüber geltend machen! Der Auftragsverarbeiter haftet nun für unterlassene Hinweise!

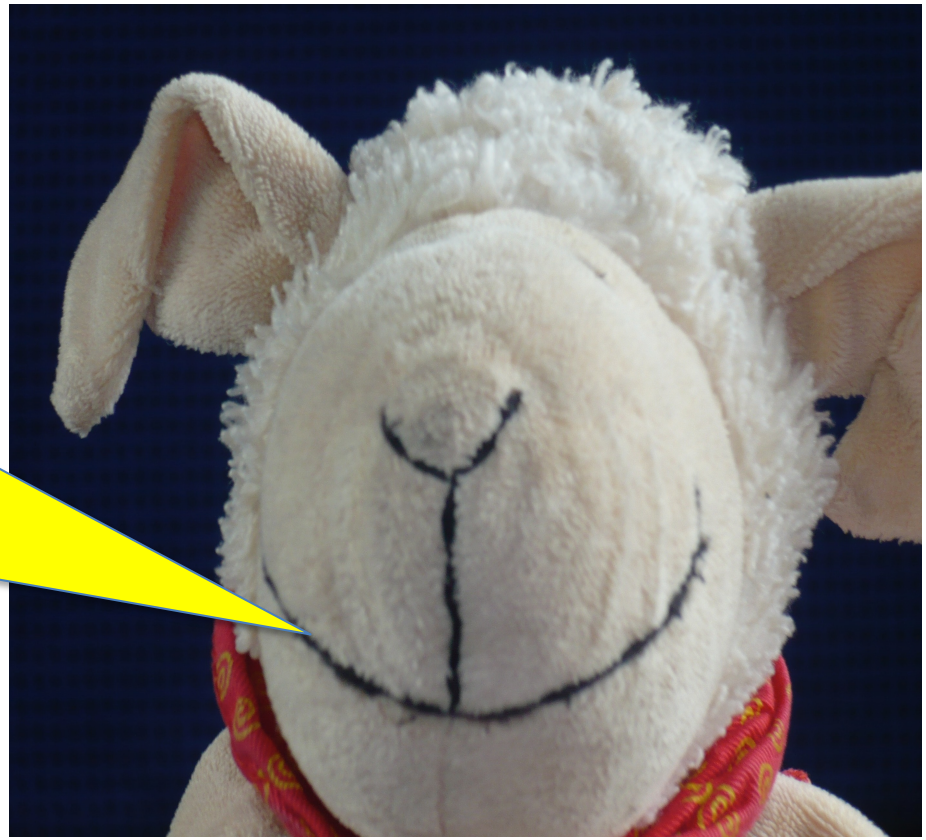
- Jeder Betroffene hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Diese Aufsichtsbehörde ist dann - ggfls. gemeinsam mit der Aufsichtsbehörde die für den Verantwortlichen zuständig ist – gehalten, dem Vorwurf nachzugehen und diesen soweit er sich als zutreffend herausstellt, auch zu ahnden!

- Jede Aufsichtsbehörde hat sicherzustellen, dass die Verhängung von Geldbußen für Verstöße gegen die Verordnung in jedem Einzelfall:
  - wirksam
  - verhältnismäßig und
  - abschreckend ist!

- Bei Verstößen gegen Bestimmungen der DS-GVO können Geldbußen von bis zu 10 Mio. € oder Fall eines Unternehmens von bis zu 2% seines gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher der Beträge höher ist!

- Bei schweren Verstößen gegen Bestimmungen der DS-GVO oder Anweisungen der Aufsichtsbehörde können Geldbußen von bis zu 20. Mio. € oder Fall eines Unternehmens von bis zu 4% seines gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher der Beträge höher ist!

So das war´s jetzt aber endgültig!



Herzlichen Dank für ihre Aufmerksamkeit!

Rechtsanwalt Prof. Wolfgang Müller
Fachanwalt für Informationstechnologierecht
Fachanwalt für Bau- und Architektenrecht
Schlichter nach SOBau
Honorarprofessor der TU Dortmund
Lehrbeauftragter der FH Dortmund

Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai