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 und
Lehrbeauftragter der Fachhochschule Dortmund

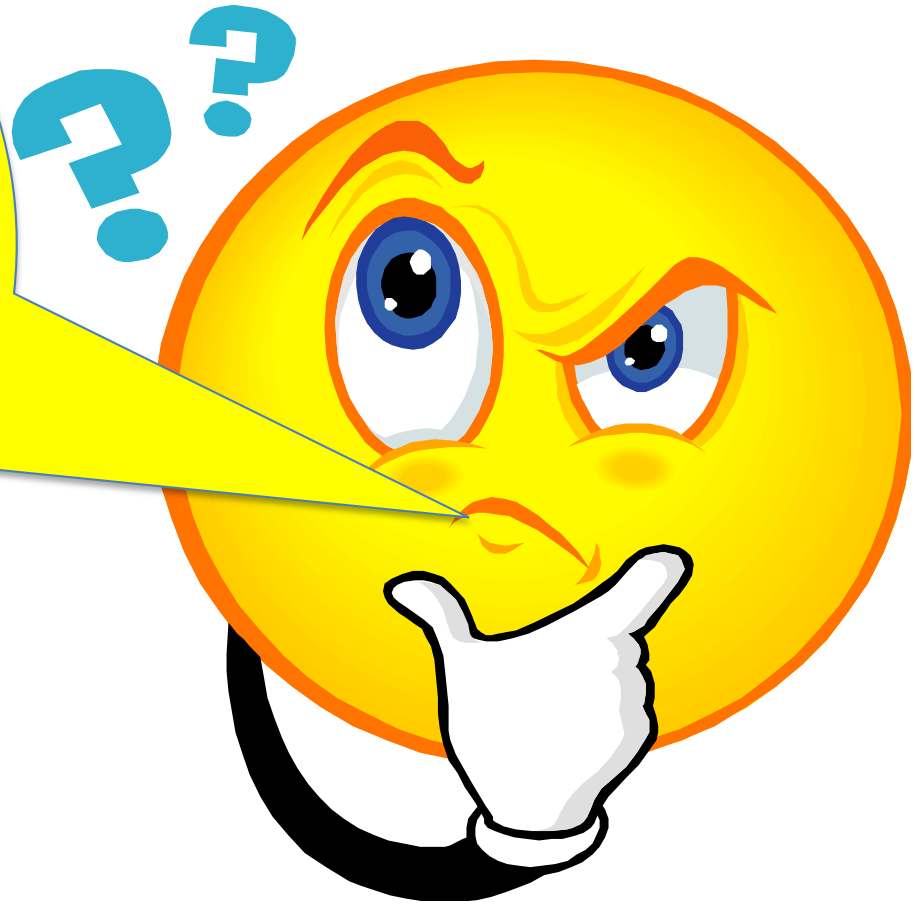
Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai

Das „*IT-Sicherheitsgesetz*“!
„*Ob das denn so wirklich so sicher ist?*“

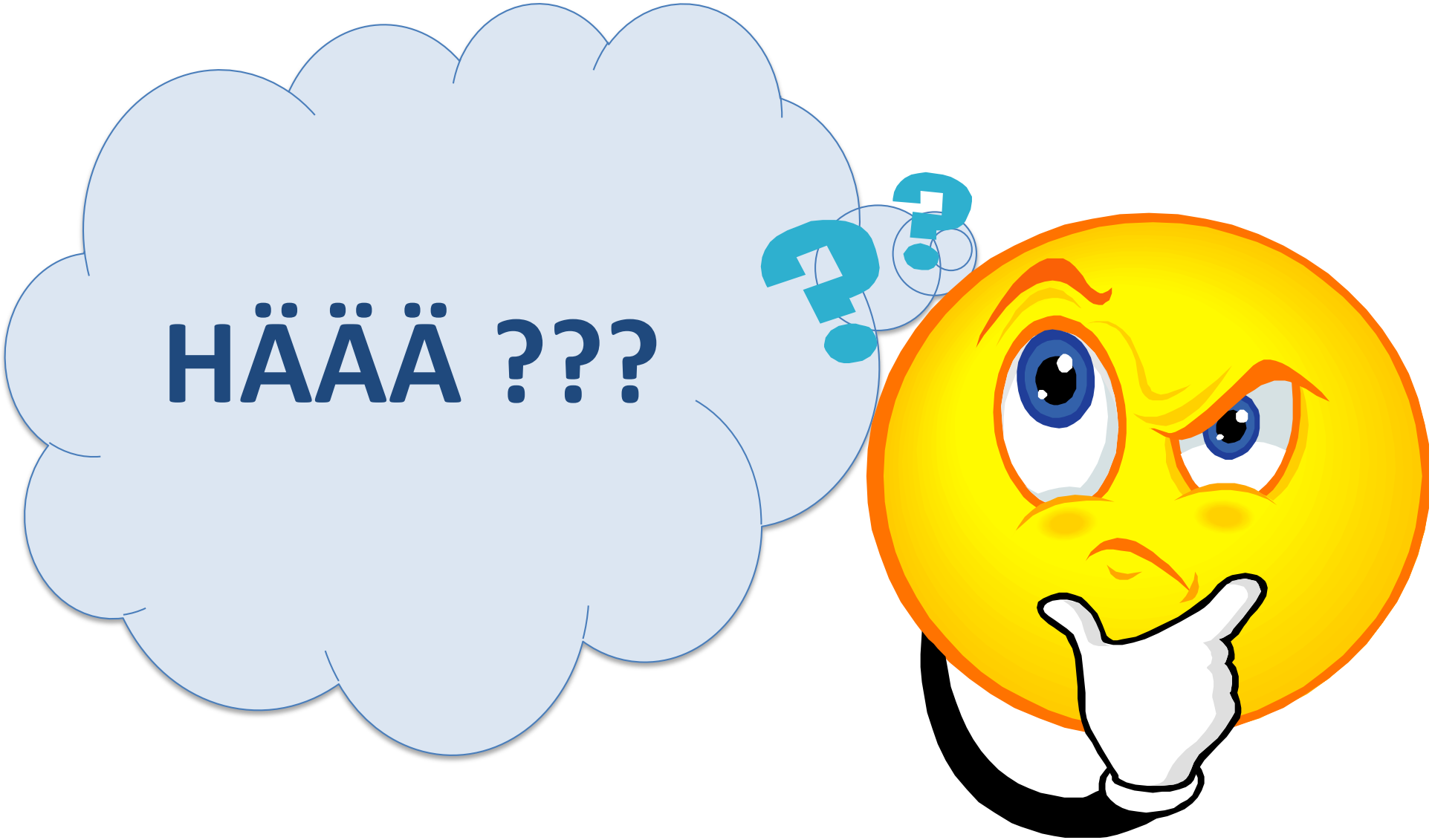
oder

„*Wer kann das denn wirklich (schon) umsetzen*?“
???

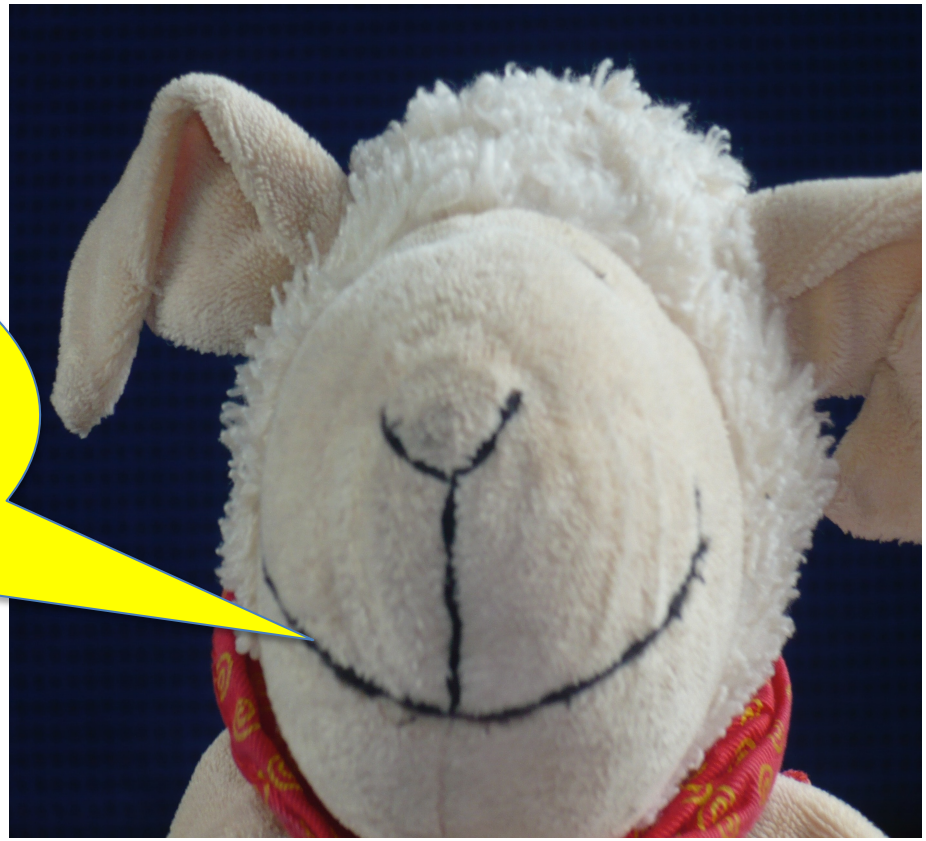
War da nicht noch irgendwas mit einem „IT-Sicherheitsgesetz“ ???



Na ja, nicht so richtig!!!

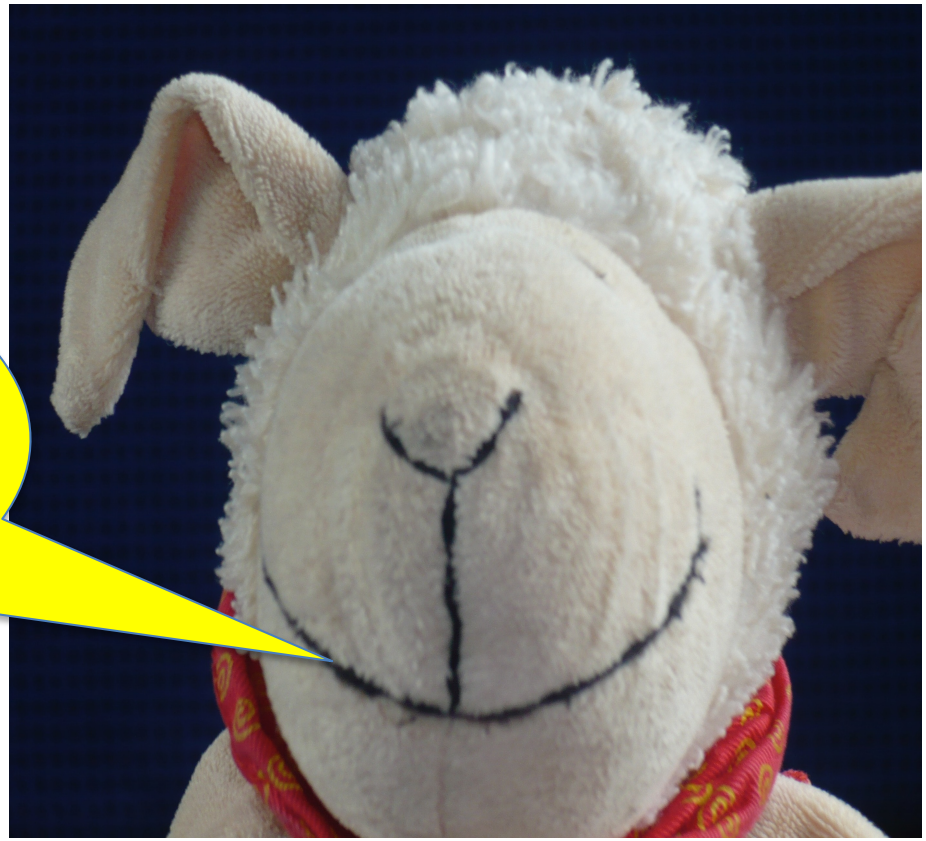

HÄÄÄ ???

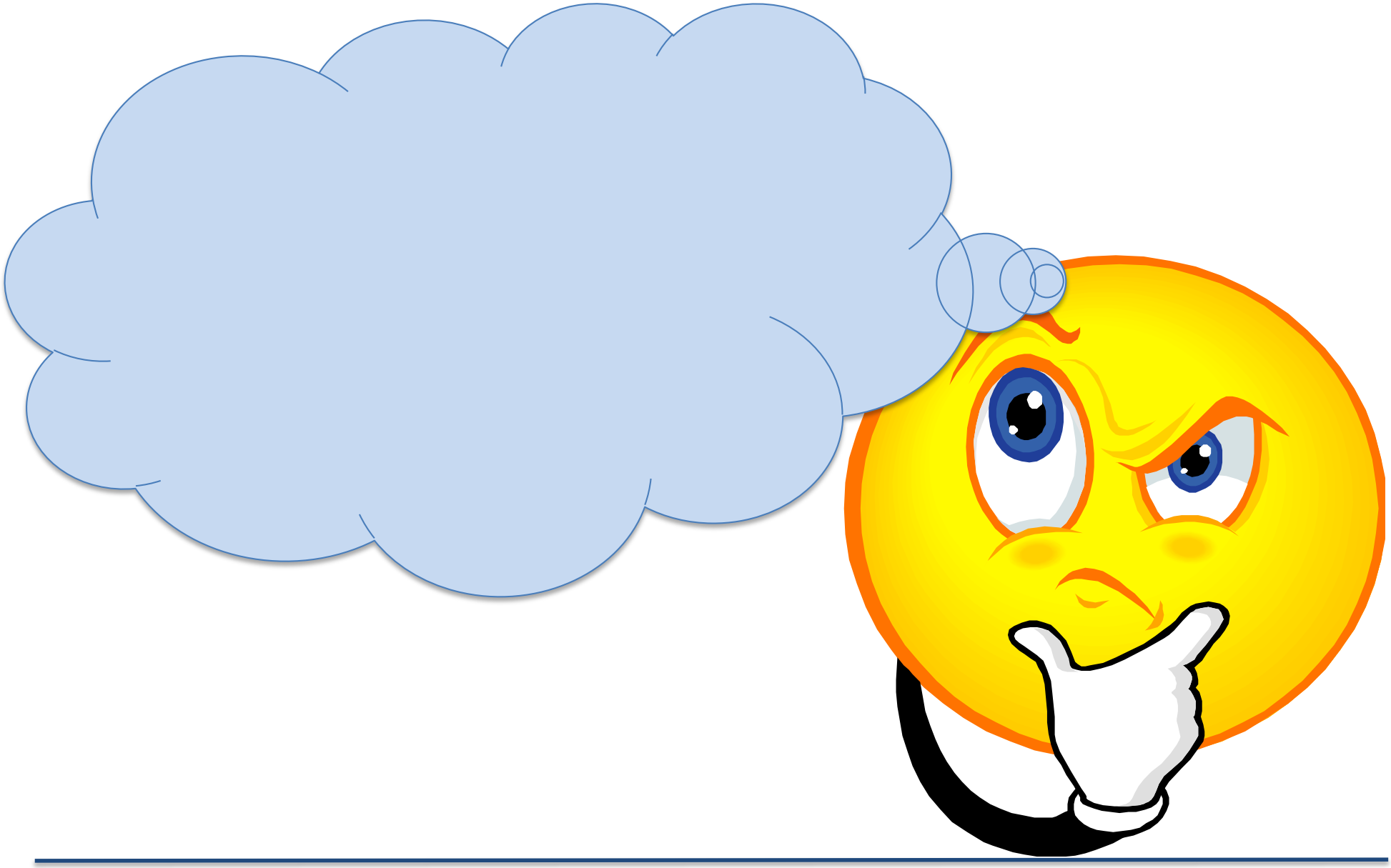
Eigentlich gibt es gar
kein
„IT-Sicherheitsgesetz“
!!!



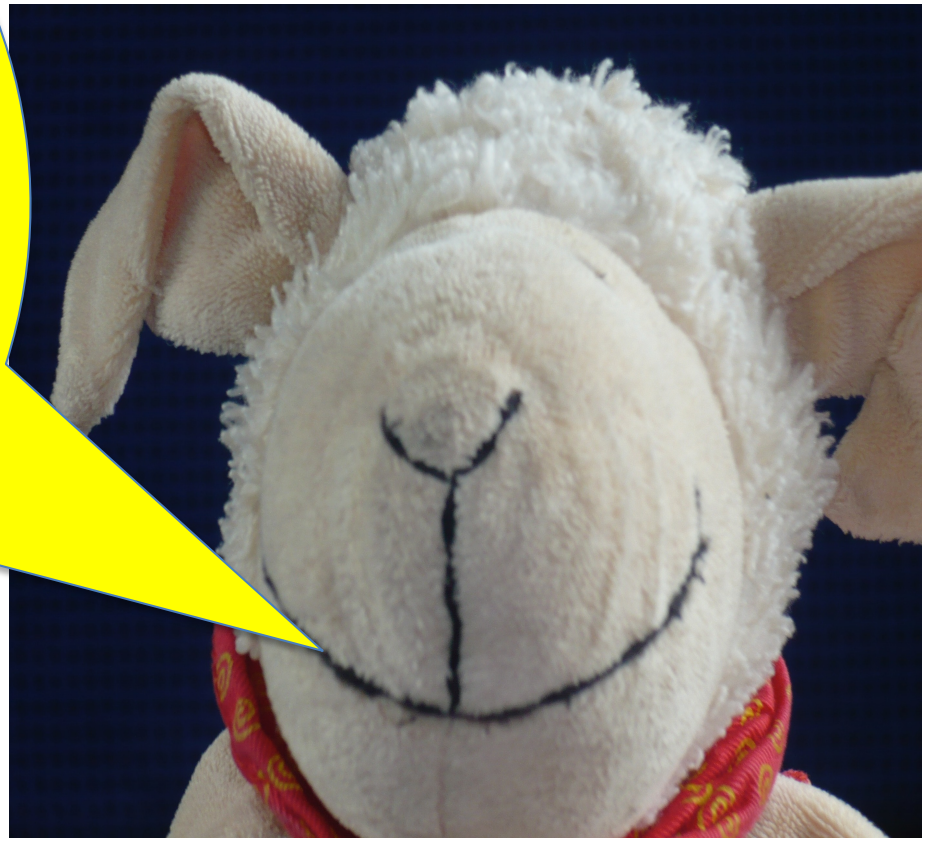
So ein Blödmann! Der spinnt doch! Jede Zeitung ist doch voll davon!

Na eigentlich gibt es es und eigentlich gibt es es auch wieder nicht!





Das IT-Sicherheitsgesetz ist ein sog. „*Artikelgesetz*“, also eigentlich kein Gesetz wie man es sich normalerweise vorstellt, sondern ein Gesetz was quasi „*Transportbehälter*“ für Gesetzesänderungen an anderen Gesetzen ist und diese zum Teil auch gar nichts mit „*IT-Sicherheit*“ zu tun haben!



Das (1.) **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme** (sog. „*IT-Sicherheitsgesetz*“) vom 17.07.2015 bestand aus **11 Artikeln**, von denen **9 Artikel** die Änderung anderer Gesetze beinhalten, von denen wiederum einige **nichts** mit **IT** zu tun hatten:

Artikel 1: Änderung des **BSI-Gesetzes** (IT +)
Artikel 2: Änderung des **Atom-Gesetzes** (IT +)
Artikel 3: Änderung des **Energiewirtschaftsgesetzes** (IT +)
Artikel 4: Änderung des **Telemediengesetzes** (IT +)
Artikel 5: Änderung des **Telekommunikationsgesetzes** (IT +)

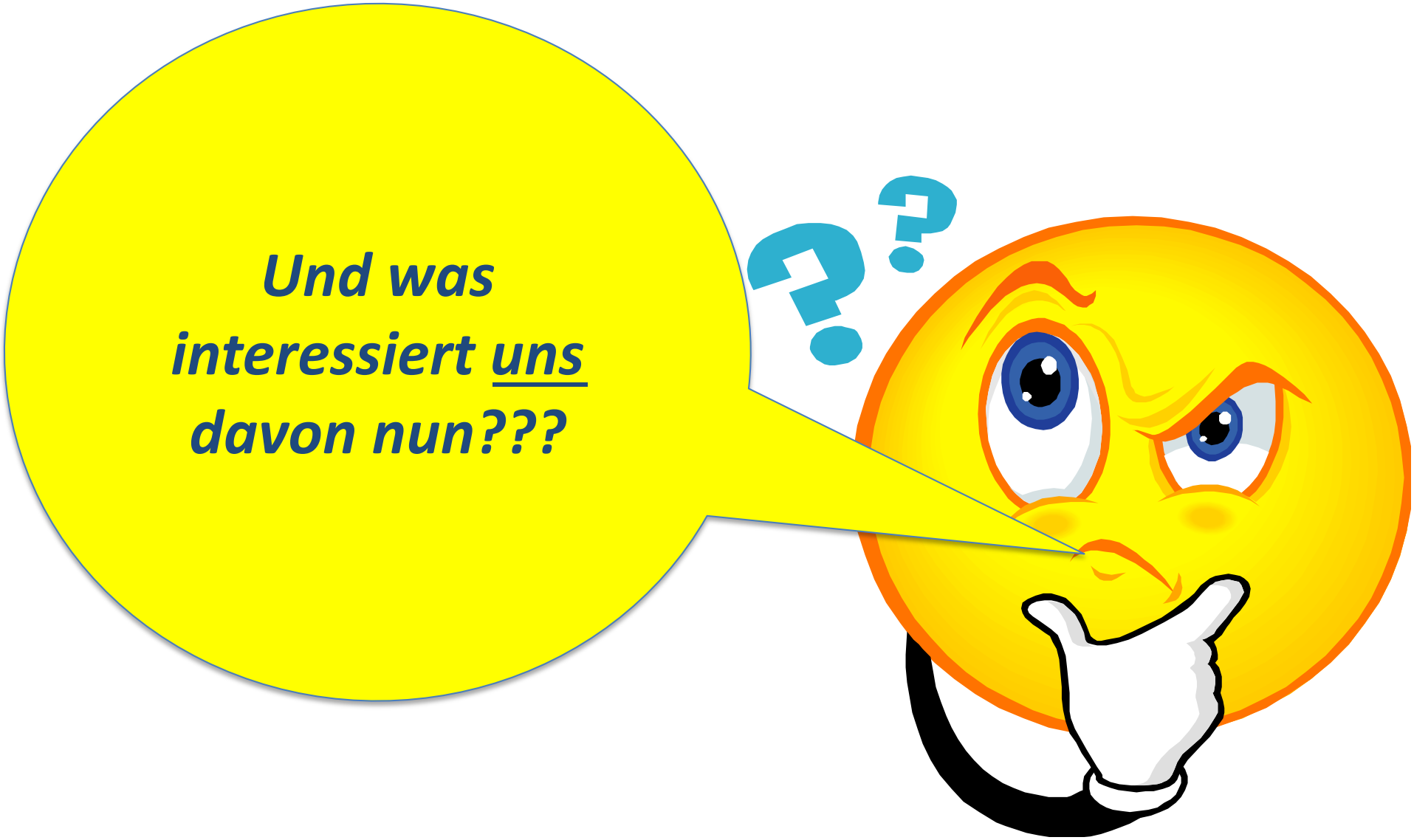
Artikel 6: Änderung des Bundesbesoldungsgesetzes (IT -)
Artikel 7: Änderung des Bundeskriminalamtsgesetzes (IT -)
Artikel 8: Weitere Änderung des BSI-Gesetzes (Gebühren) (IT -)
Artikel 9: Änderung des Gesetzes zur Strukturreform des Gebührenrechts des Bundes (IT -)

Artikel 10: Evaluierung
Artikel 11: Inkrafttreten der gesetzlichen Neuregelungen

Das (2.) **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme** (sog. „**IT-Sicherheitsgesetz**“) vom 28.05.2021 besteht aus **7 Artikeln**, von denen **2 Artikel** die Änderung anderer Gesetze beinhalten, von denen wiederum einige **nichts** mit **IT** zu tun haben:

Artikel 1: Änderung des **BSI-Gesetzes** (IT +)
Artikel 2: Änderung des **Telekommunikationsgesetzes** (IT +)
Artikel 3: Änderung des **Energiewirtschaftsgesetzes** (IT +)
Artikel 4: Änderung der **Außenwirtschaftsverordnung** (IT +)
Artikel 5: Änderung des **Zehnten Buches Sozialgesetzbuch** (IT +)

Artikel 6: Evaluierung (IT -)
Artikel 7: Inkrafttreten (IT -)


Und was interessiert uns davon nun???

Die **Regelungen** im

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)

Telekommunikations-gesetz (TKG)

Die **Regelungen** im

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)

Telekommunikations-gesetz (TKG)

Durch das **1.** und **2. IT-Sicherheitsgesetz sind** am **BSI-Gesetz** an zahlreichen Punkten Veränderungen vorgenommen worden.


Was habe ich denn mit dem „BSI-Gesetz“ zu tun???

Gute Frage!
Eigentlich Nichts,
jetzt aber doch!

Das **BSI-Gesetz** ist eigentlich ein Gesetz zur **Sicherstellung der IT-Sicherheit** des **Bundes** bzw. der **Bundesbehörden**.

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.

→ Achtung: Alte Fassung!!!

Neue Fassung v. 18. Mai 2021:

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

Das **BSI-Gesetz** ist eigentlich ein Gesetz zur **Sicherstellung der IT-Sicherheit** des **Bundes** bzw. der **Bundesbehörden**.

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.

→ **Achtung: Alte Fassung!!!**

Neue Fassung v. 18. Mai 2021:

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

Damit wird deutlich, dass der **Anwendungsbereich ein anderer als üblich ist**!

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

Na Klar!

§ 9a Nationale Behörde für die Cybersicherheitszertifizierung

*(1) Das Bundesamt ist die **nationale Behörde für die Cybersicherheitszertifizierung** im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881.*

§ 9c Freiwilliges IT-Sicherheitskennzeichen

*(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien **ein einheitliches IT-Sicherheitskennzeichen** ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.*

Durch das **1.** und das **2. IT-Sicherheitsgesetz** ist auch im Weiteren am **BSI-Gesetz** an zahlreichen Punkten eine Veränderung vorgenommen worden, die über den ursprünglichen Anwendungsbereich hinausgehen und nunmehr auch **Dritte** bzw. die **Privatwirtschaft** betreffen können.

Im Einzelnen hierzu wie folgt:

In **§ 2 Abs. 2 BSI-Gesetz** heißt es nun **ausdrücklich**:

*(**2**) Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele.*
Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder

2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber **Kritischer Infrastrukturen** sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, **angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind**. Dabei soll der **Stand der Technik** eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

*(**1a**) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 **auch den Einsatz von Systemen zur Angriffserkennung**. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.*

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

Dann mal im Einzelnen:

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber **Kritischer Infrastrukturen*** *sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

Kritische Infrastrukturen sind nach **§ 2 Abs. 10 BSIG**
Einrichtungen, **Anlagen** oder **Teile davon**, die

1. den **Sektoren**
   - **Energie**,
   - **Informationstechnik** und **Telekommunikation**,
   - **Transport** und **Verkehr**,
   - **Gesundheit**,
   - **Wasser**,
   - **Ernährung**
   - **Finanz-** und **Versicherungswesen**
   - **Siedlungsabfallentsorgung** angehören **und**

2. **von hoher Bedeutung für das Funktionieren des Gemeinwesens sind**, weil durch ihren **Ausfall** oder ihre **Beeinträchtigung erhebliche Versorgungs-engpässe** oder **Gefährdungen für die öffentliche Sicherheit** eintreten würden.

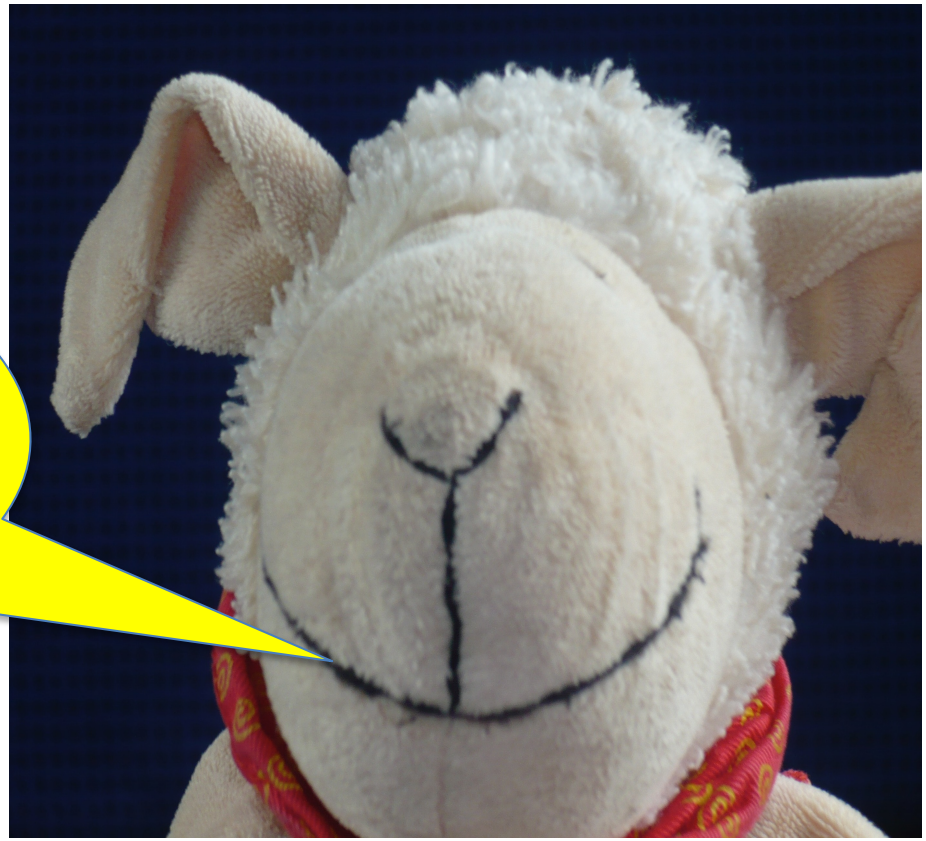
**Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSI-Gesetz näher bestimmt (z.B. Banken, Krankenhäuser, Wasser-/Energieversorger, Bahn usw).*

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

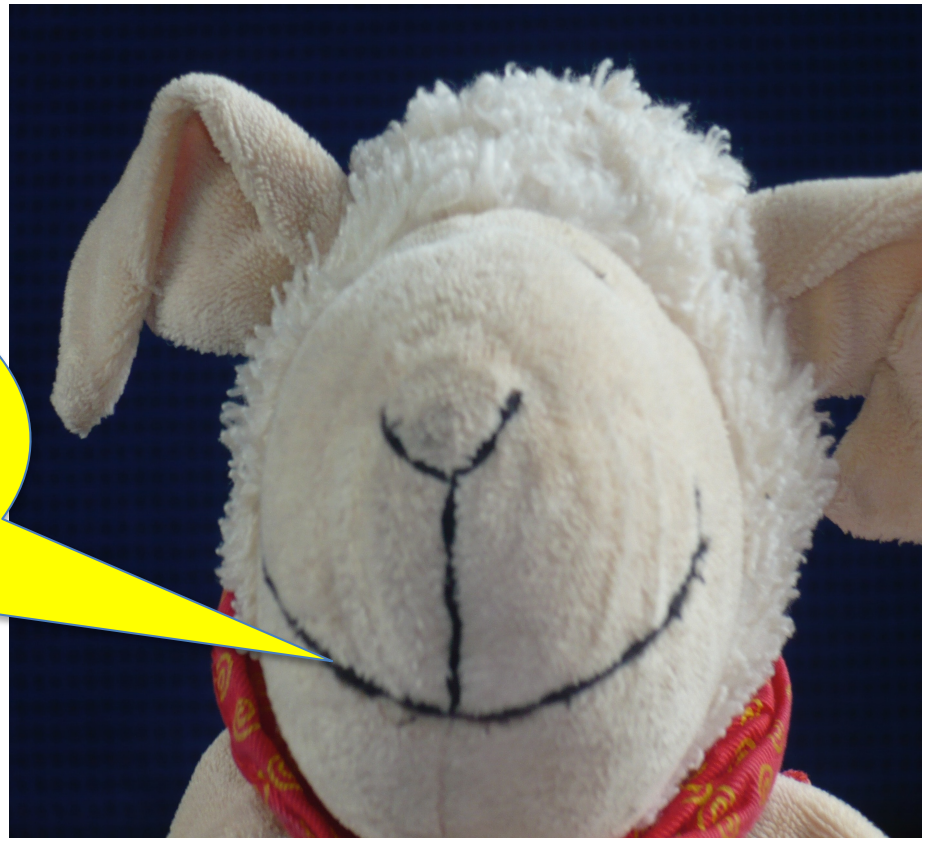
*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten,* ***angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.*** *Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*


Und wie geht dies???

Das muss der Betreiber schon selber wissen!



Nein Spaß beiseite!



§ 3 Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Hierzu nimmt es folgende Aufgaben wahr:

1. – 20.

(2)

(3) Das Bundesamt ***kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen****.*

§ 3 Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Hierzu nimmt es folgende Aufgaben wahr:

1. – 20.

(2)

(3) Das Bundesamt ***kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen****.*

... und dann gibt es dann noch den **§ 8a BSIG Absatz 2**!!!

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

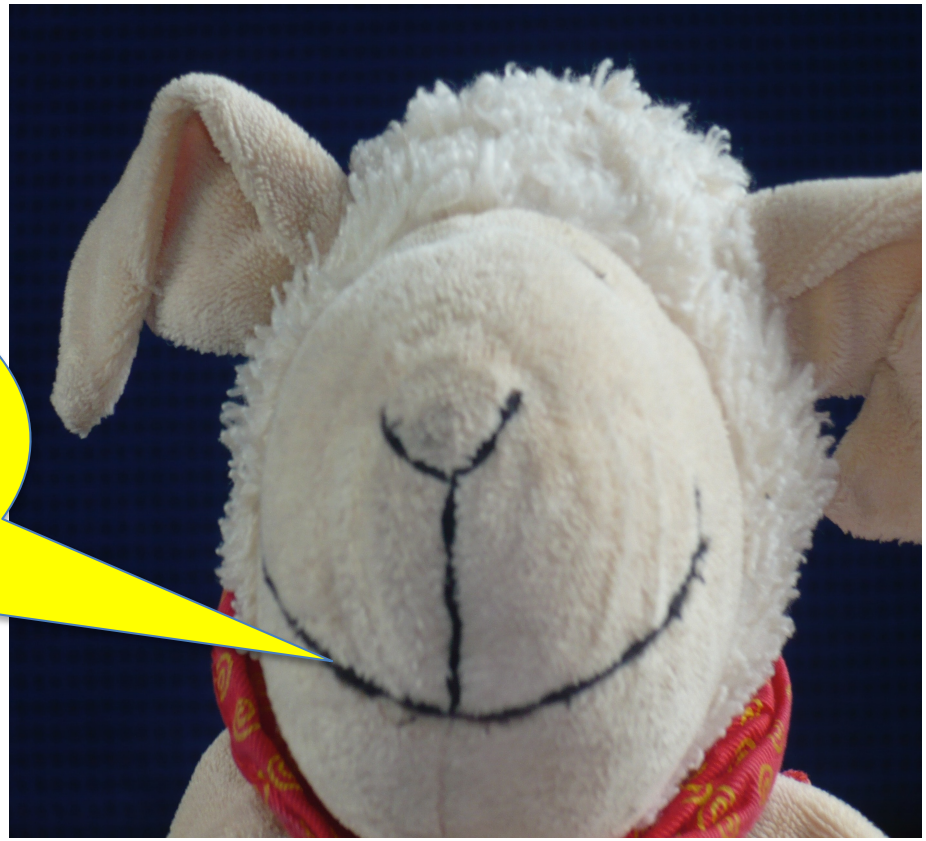
*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

*(**2**) **Betreiber Kritischer Infrastrukturen und** ihre **Branchenverbände** können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. **Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten**. Die Feststellung erfolgt*

1. *im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*
2. *im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*


Und wenn es hier nichts gibt???

Dann ist der Betreiber eben selbst verantwortlich!

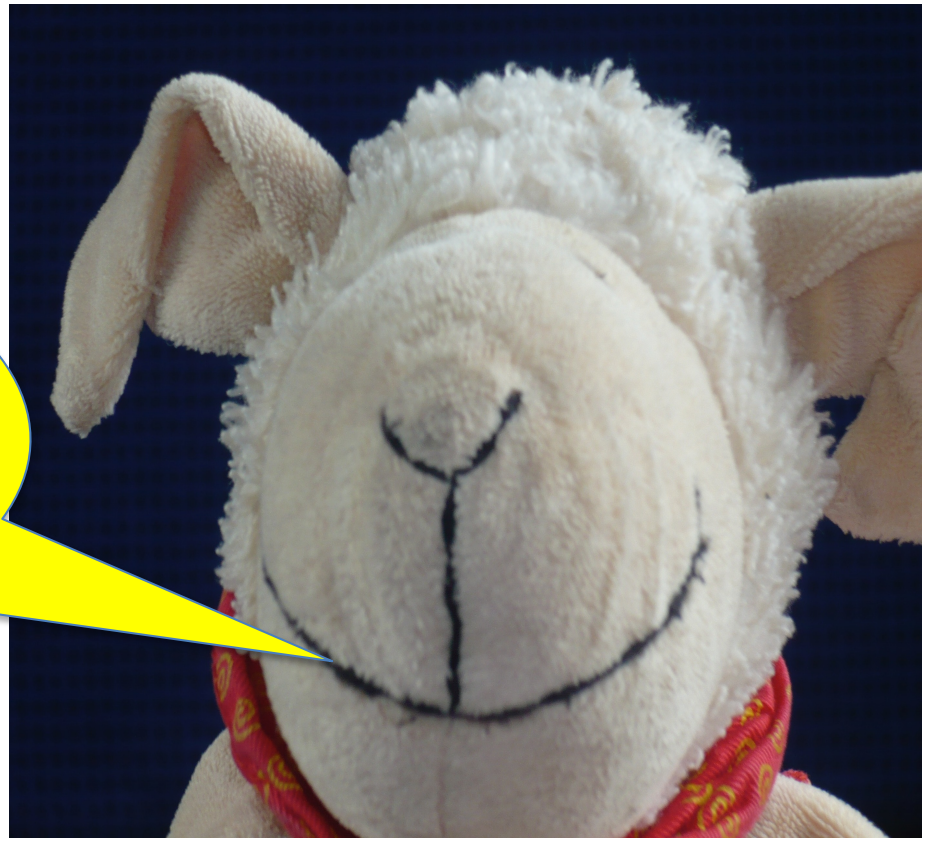


d.h. er hat selber Sorge zu tragen für:

… angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.


Jetzt bin ich genauso schlau wie vorher!!!

Na dann schau Dich doch mal um! Die Begriffe sind doch nicht unbekannt!



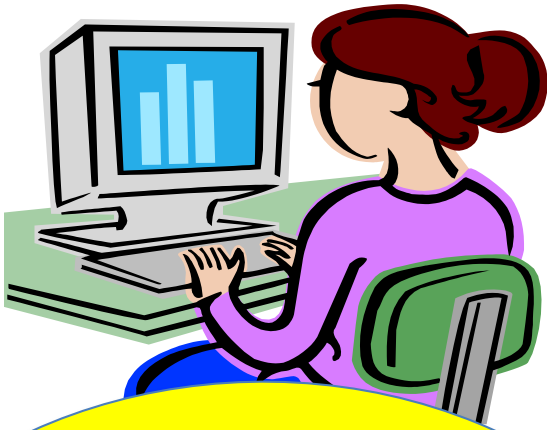
Allgemeine Grundsätze des Datenschutzes

§ 9 BDSG (alt) Technische und organisatorische Maßnahmen

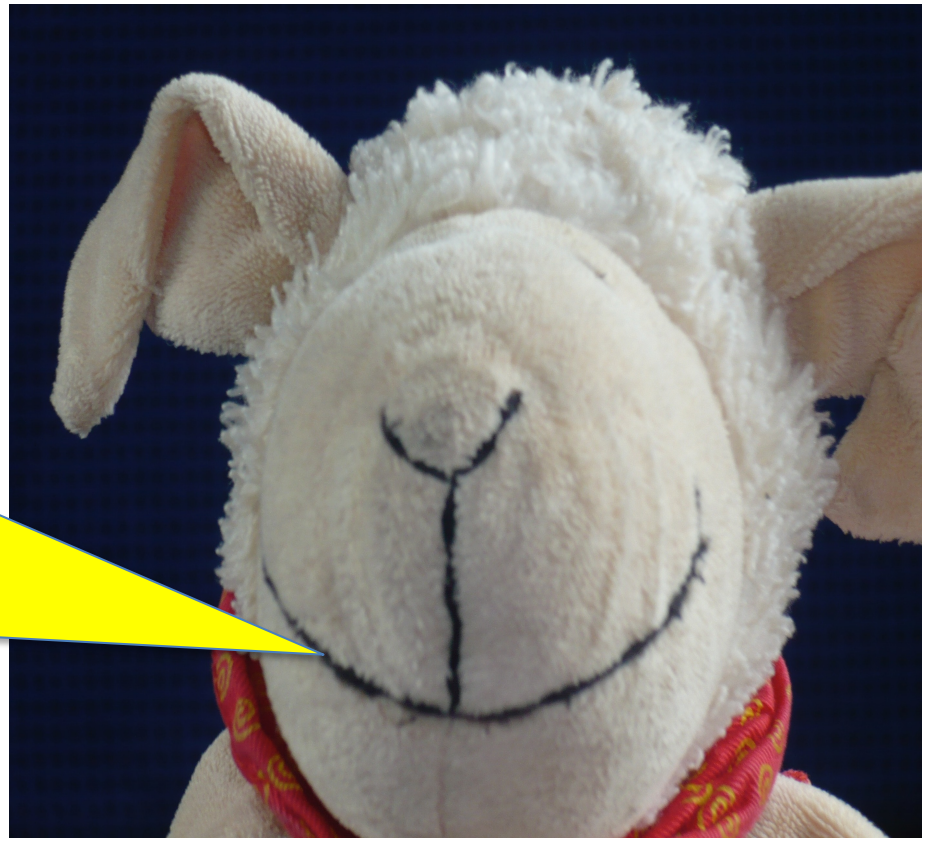
[1]Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben **die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage 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 (alt)

- 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;

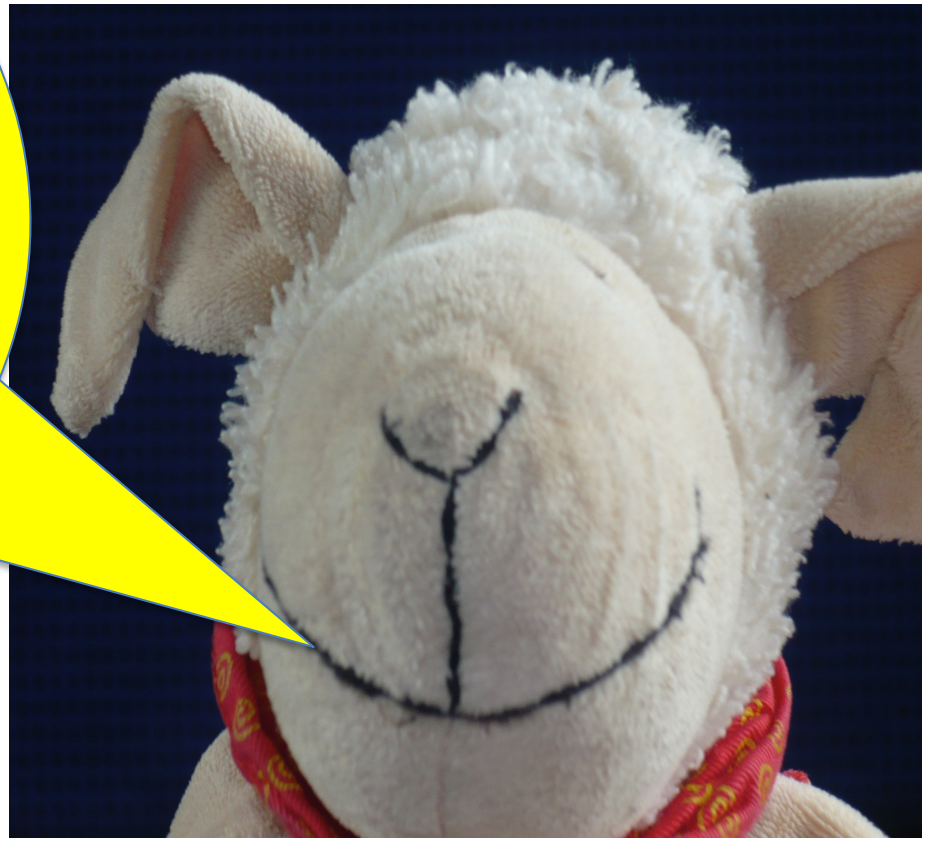
Die zu vereinbarenden technischen und **organisatorischen** Maßnahmen i.S.d. **Anlage zu § 64 BDSG** beinhalten:

- **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 müsstest Du eigentlich schon im Rahmen des Schutzes von personenbezogenen Daten einhalten! Nichts anderes gilt jetzt für alle Daten



d.h. er hat selber Sorge zu tragen für:

… angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.

und

*Dabei soll der „**Stand der Technik**“ eingehalten werden.*

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. **Dabei soll der Stand der Technik eingehalten werden**. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

Die *Technik* das „unbekannte Wesen“

„Stand der Wissenschaft und Technik“

„Allgemein anerkannte Regeln der Technik“ - **aaRdT**

„Stand der Technik“

„GMP oder cGMP“

„beste verfügbare Technik“

„technische Regelwerke“

„DIN-Normen“

„*Allgemein anerkannte Regeln der Technik*“ - aaRdT

Allgemein anerkannte Regeln der Technik sind diejenigen technischen Regeln für den **Entwurf** und die **Ausführung von (baulichen) Anlagen**, die **in der technischen Wissenschaft als theoretisch richtig erkannt sind und feststehen sowie** insbesondere **in dem Kreise der für die Anwendung der betreffenden Regeln maßgeblichen, nach dem neuesten Erkenntnisstand vorgebildeter Techniker durchweg bekannt und** aufgrund fortdauernder praktischer Erfahrung **als technisch geeignet, angemessen und notwendig anerkannt** sind.

Der Begriff der **allgemein anerkannten Regeln der Technik** umfasst alle überbetrieblichen Normen, zu denen insbesondere die **DIN-Normen**, die **ETB** (Einheitliche Technische Baubestimmungen des Instituts für Bautechnik), die **Richtlinien des Vereins Deutscher Ingenieure (VDI)**, die **VDE-Bestimmungen des Verbandes Deutscher Elektriker** und auch mündlich überlieferte technische Regeln gehören.*

Im medizinischen Bereich finden sich vielfach schriftlich fixierte „**Leitlinien**“, „**Richtlinien**“ oder „**Empfehlungen**“; auch diese können geeignet sein, rechtliche Gegebenheiten des medizinischen Bereichs zu konkretisieren. Hierzu gehören z.B. die **GMP** oder **cGMP**.**

→ Ein **Verstoß** gegen die allgemein anerkannten Regeln der Technik liegt vor, wenn der **Auftragnehmer** solche technischen Regeln **nicht** beachtet, **die sich in der Wissenschaft als richtig durchgesetzt und die sich in der (Bau-)Praxis als richtig bewährt haben**!

*Knifka/Koeble *Kompendium des Baurechts*, 4. Aufl. 2014, 6. Teil Rdn. 32;

**Good Manufacturing Practices „Gute Herstellungspraxis“;

„*Stand der Technik*“

Der ***Stand der Technik*** beschreibt die Verfahrensweisen, die **nach den gegenwärtigen technischen Gegebenheiten erreichbar sind.** Er spiegelt die **machbaren technischen Spitzenleistungen** wider, die zum maßgeblichen Zeitpunkt – i.d.R. bei Abnahme – erreichbar sind.

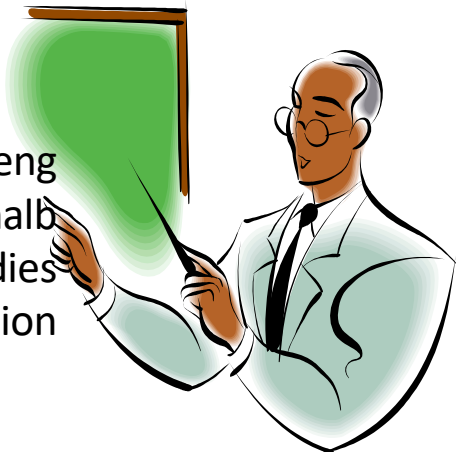
Mit der Verpflichtung zur Einhaltung des ***Standes der Technik*** ist – worauf auch Streitz* zu Recht verweist, insbesondere bei länger laufenden Projekten ein **hohes Risiko** für den **Auftragnehmer** verbunden.

→ Allerdings ist dies auch für den **Auftraggeber** insbesondere im Anlagenbau nicht ohne Risiko, da eine Erstellung nach dem ***Stand der Technik*** auch das Risiko fehlerhafter Konstruktionen birgt. Solche Konstruktionen sind häufig **Versuchsmodelle**, so dass eine dementsprechende Erstellung **insbesondere in der laufenden Produktion abgelehnt werden sollte**!

*Streitz, *Beck´sches Mandatshandbuch IT-Recht*, 1. Aufl. 2011, § 35 Rdn. 42;

„*Stand der Wissenschaft und Technik*“

Der „***Stand der Wissenschaft und Technik***“ beschreibt über das momentan praktisch-technisch Erreichte hinaus **auch die neusten Ergebnisse des derzeitigen wissenschaftlichen Erkenntnisstandes**.*



→ Software und Anlagen die dieser Definition unterliegen sollen, sind streng genommen dem **Entwicklungs- bzw. Labormaßstab** zu zu ordnen. Dies sollte deshalb nur dann **vereinbart und** auch **vertraglich besonders abgesichert** werden, wenn dies allen Beteiligten klar ist und beide Parteien sich in einer „***Entrepreneur***“** Position sehen!

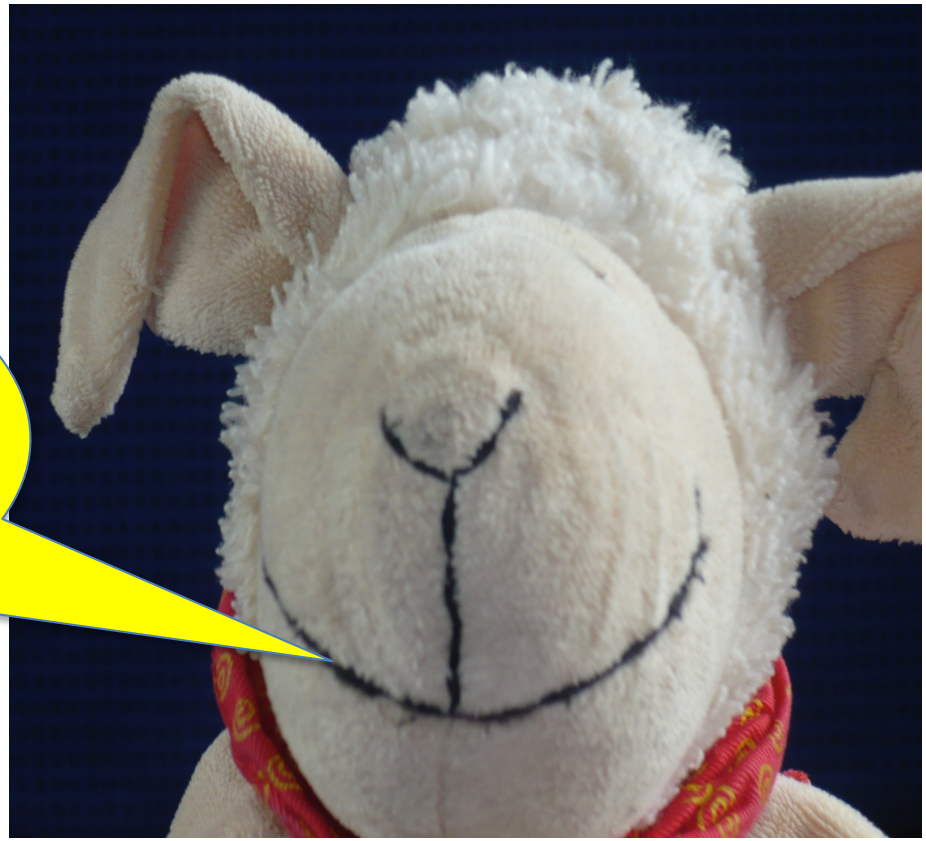
→ Mittlerweile findet sich auch noch das aus dem in § 3 Abs. 6 BImSchG bestimmten Beurteilungsmaßstab abgeleitete Kriterium „***beste verfügbare Technik***“ unter diesem Begriff wird die **in der Europäischen Gemeinschaft vorhandene optimale Technik verstanden**.

*Ulrich, *Der gerichtliche Sachverständige*, 12. Aufl. 2006, Rdn. 291;

**Im Englischen beschreibt das ursprünglich französische Wort „*Entrepreneur*“ eine Persönlichkeit, die bereit dazu ist, hohe Verantwortung und hohes Risiko zu tragen!


Der Teufel steckt bekanntermaßen im Detail!

Wir sind noch nicht fertig!




Was denn nun noch???

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach § 10 Absatz 1 gelten, angemessene organisatorische und Technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

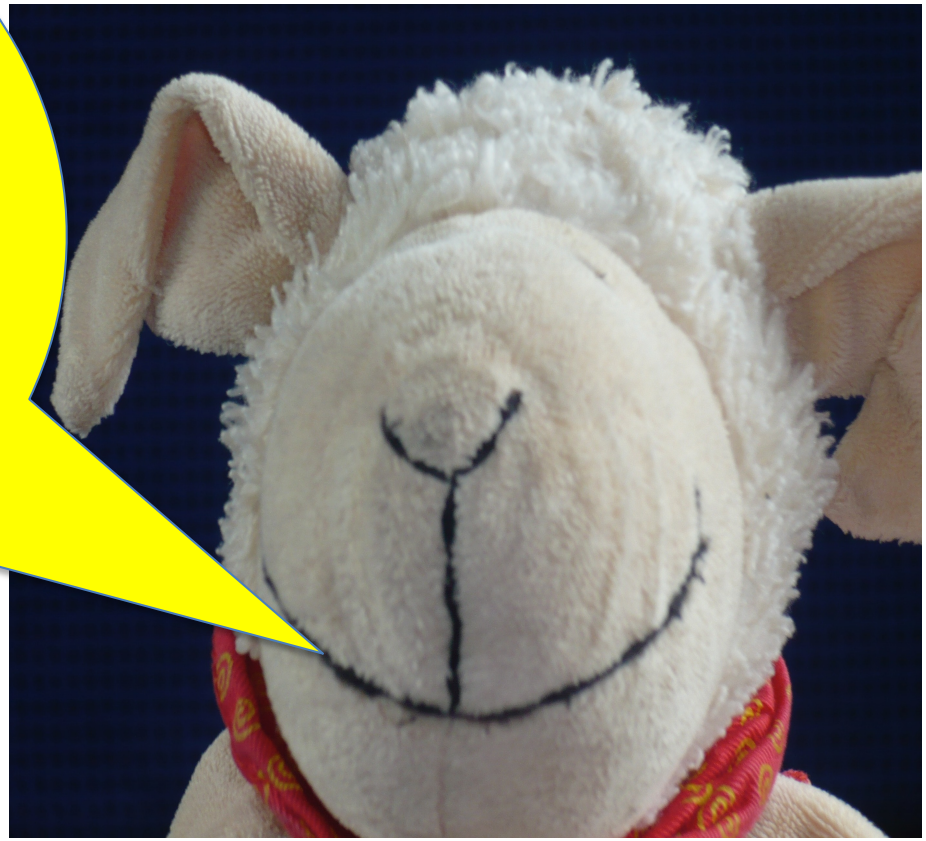
(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale us dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.

*(**2**) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt*

1. *Im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*
2. *Im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*

*(**3**) Betreiber Kritischer Infrastrukturen haben **die Erfüllung der Anforderungen** nach Absatz 1 und 1a **spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre** dem Bundesamt **nachzuweisen**. Der Nachweis kann durch **Sicherheitsaudits**, **Prüfungen** oder **Zertifizierungen** erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.*

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




Mir schwant Übles!!!

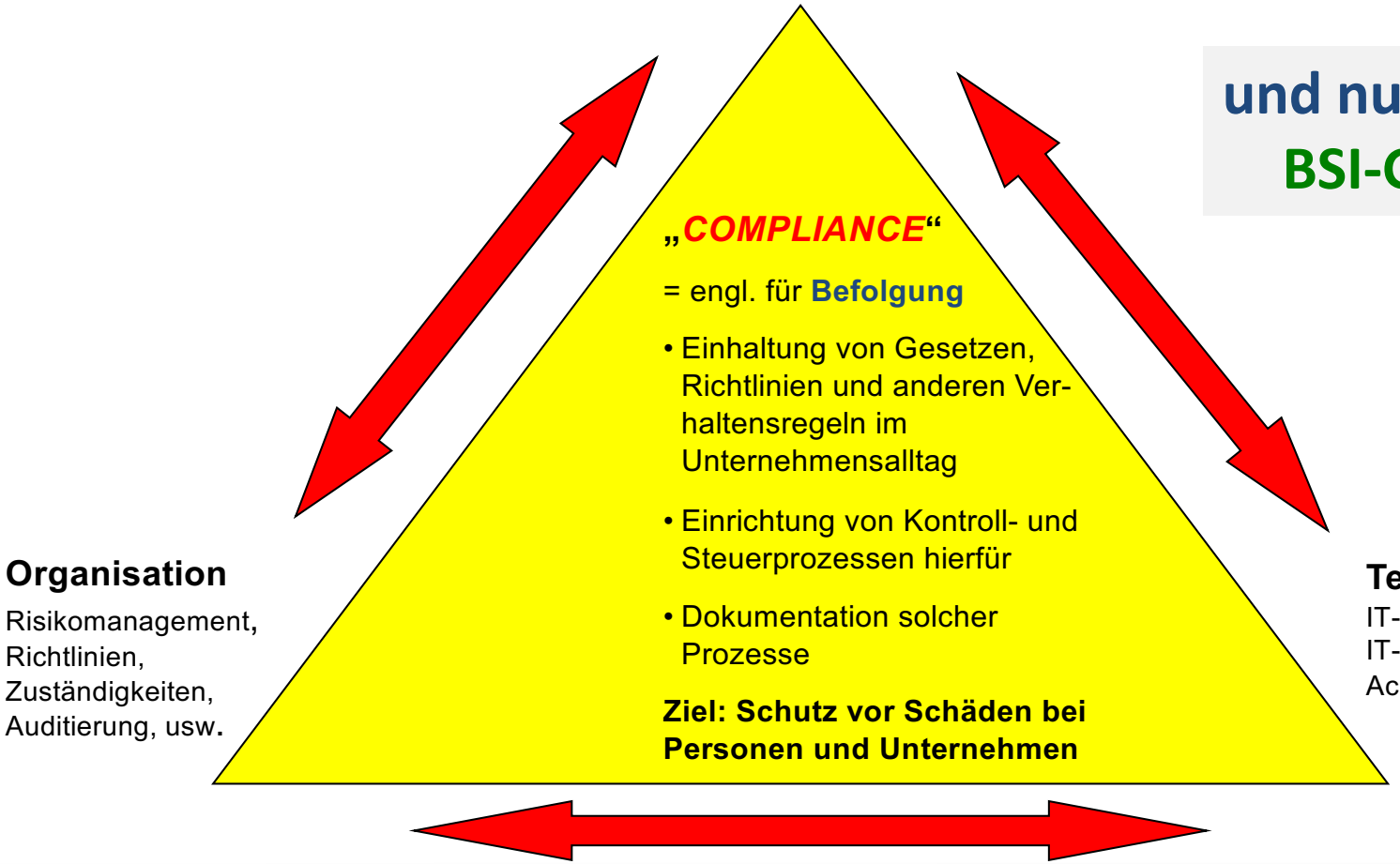
Mit dem **BSI-Gesetz** wird nunmehr erstmals das, was an den verschiedensten Stellen hinsichtlich der **IT-Sicherheit** geregelt ist und durch **Richterrecht** unter dem Begriff Verletzung der (**IT-**) **Compliance** z.B. im Rahmen von Schadensersatzansprüchen gegen den Vorstand oder die Geschäftsführung des Unternehmens angewendet wurde, **als zentrale Bestimmung/Forderung gegenüber den betroffenen Unternehmen kodifiziert**.

Das **BSI-Gesetz** ist für Betreiber Kritischer Infrastrukturen nichts anderes als der **Obersatz**, unter dem nunmehr die **verschiedensten Handlungspflichten** für eine ordnungsgemäße **IT-Compliance** - verschärft - zusammengefasst werden.

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

gesetzliche Anforderungen

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



Organisation
Risikomanagement, Richtlinien, Zuständigkeiten, Auditierung, usw.

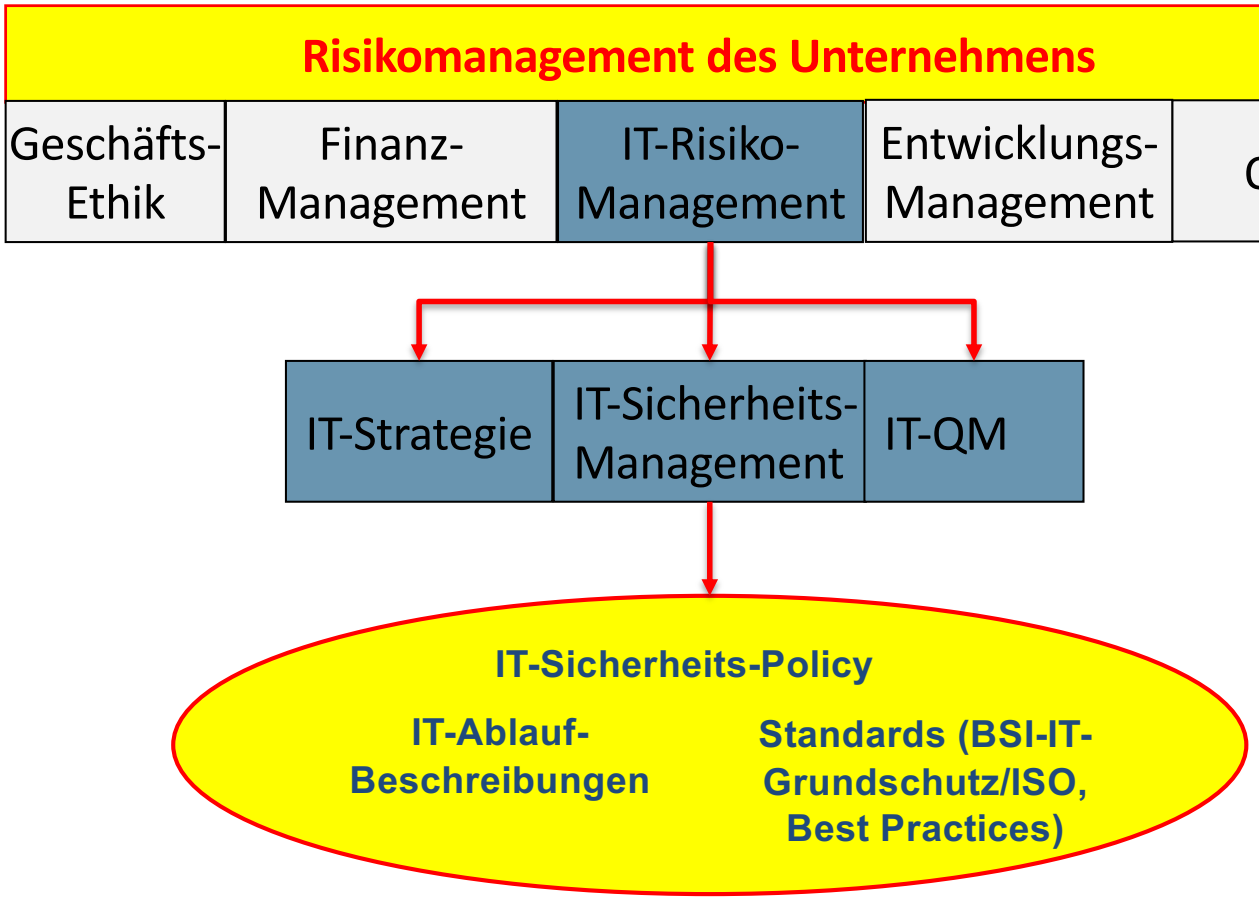
Technik
IT-Security, IT-Risikoanalyse, Achivierung usw.

und nun auch das BSI-Gesetz!!!

*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.

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!!!???

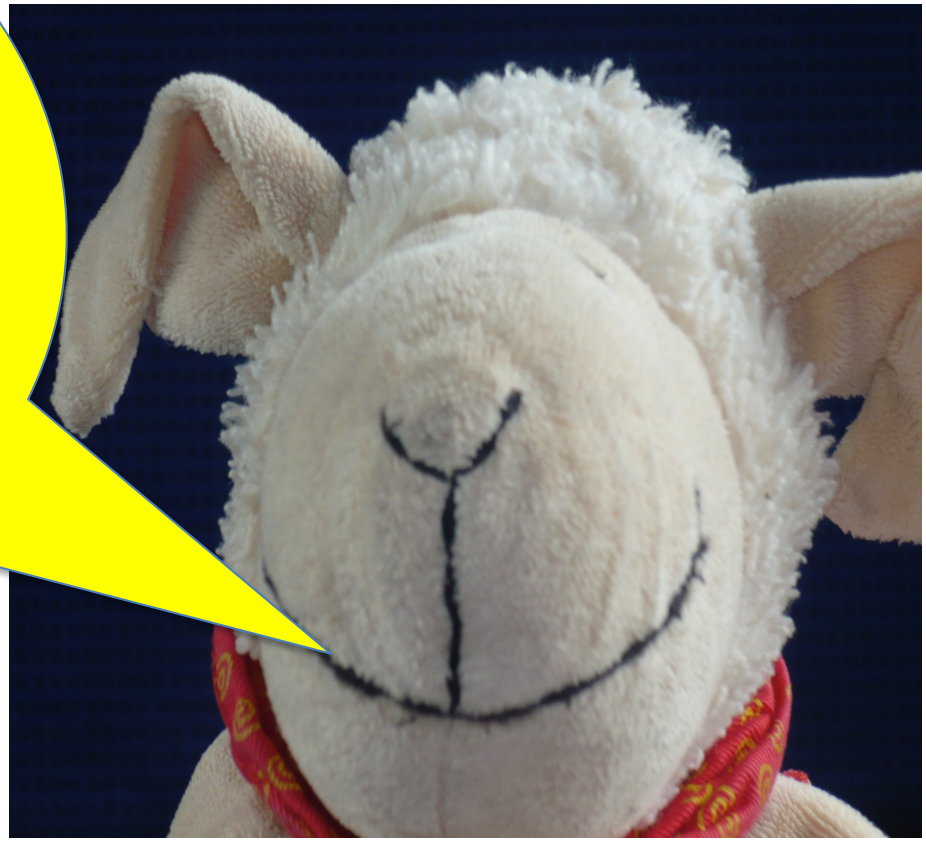
Beispielhafter Aufbau eines Regelwerkes zur IT-Security als „*Brandschutzmauer*“ des Unternehmens:

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 i.S.d. Anlage zu § 9 BDSG (alt)
IT-Security („*Security-Policy*“)		


Na herzlichen Glückwunsch!!!


Und gibt's da noch was???

Na klar! Den § 8b BSIG!



§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(1) Das **Bundesamt** ist die **zentrale Meldestelle** für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der Informationstechnik.*

*(2) Das **Bundesamt** hat zur Wahrung dieser Aufgabe …*

*(3) Die **Betreiber Kritischer Infrastrukturen sind verpflichtet**, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1* gelten, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt **zu registrieren** und eine **Kontaktstelle** zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht nicht erfüllt. Nimmt das Bundesamt eine solche registrierung selbst vor, informiert es die zuständige Aufsichtbehörde des Bundes darüber. **Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind**. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.*

*(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 **nicht erfüllt**, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung **aus Sicht des Bundesamtes** erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen entgegenstehen.*

**Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSI-Gesetz näher bestimmt (z.B. Banken, Krankenhäuser, Wasser-/Energieversorger, Bahn usw).*

(4) Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1. *Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,*
2. *erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.*

Die Meldung muss Angaben zu der Störung zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder den Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse sind befugt dem Bundesamt auf verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 erforderlich ist.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. …

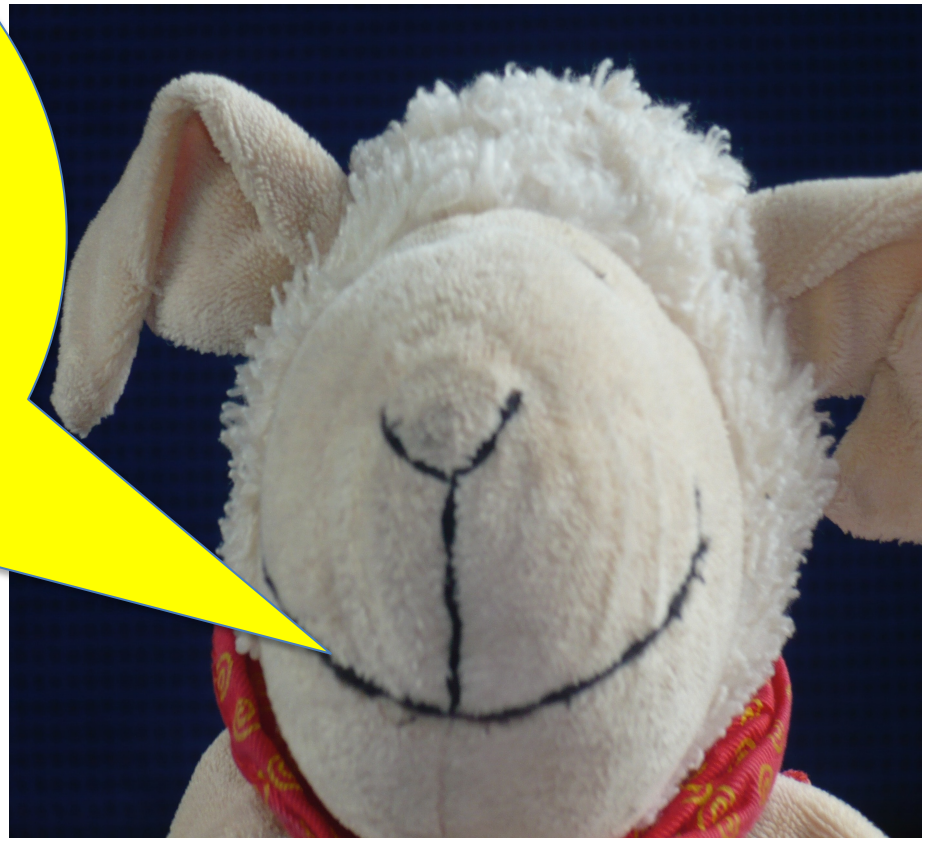
(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

(7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regeln des Bundesdatenschutzgesetzes anzuwenden.

§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

(1) Unternehmen im besonderen öffentlichen Interesse …

Na das ergibt sich aus § 2 Abs. 14 BSI-Gesetz!



§ 2 Begriffsbestimmungen
(1) - (13)

(14) *Unternehmen* ***im besonderen öffentlichen Interesse*** *sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und*

1. *die* ***Güter nach § 60 Außenwirtschaftsverordnung*** *in der jeweils geltenden Fassung herstellen oder entwickeln,*
2. *die nach* ***ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören*** *und daher* ***von erheblicher volkswirtschaftlicher Bedeutung*** *für die Bundesrepublik sind oder die für solche Unternehmen als* ***Zulieferer*** *wegen ihrer Alleinstellungsmerkmale* ***von wesentlicher Bedeutung sind*** *oder*
3. *die Betreiber eines Betriebsbereichs der oberen Klasse* ***im Sinne der Störfall-Verordnung*** *diesen gleichgestellt sind.*

Die Unternehmen im besonderen öffentlichen Interesse nach Satz 1 Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.

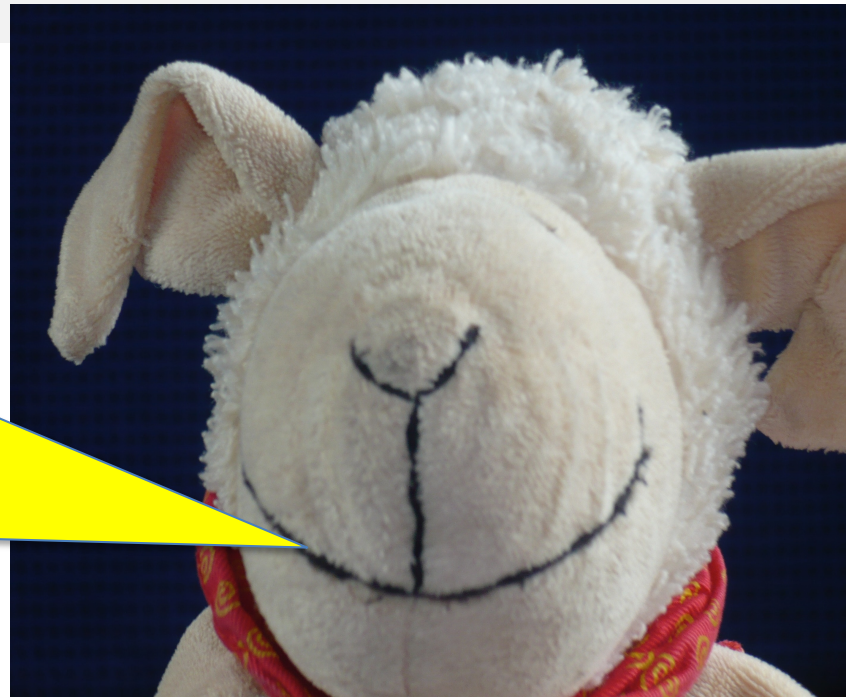
§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

*(1) **Unternehmen im besonderen öffentlichen Interesse** nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Unternehmen im besonderen öffentlichen Interesse nach § 2Absatz 14 Satz 1 Nummer 1 oder 2 gelten, und danach mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen, aus der hervorgeht,*

1. *Welche **Zertifizierungen** im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche **Prüfungsgrundlage** und welcher **Geltungsbereich** hierfür festgelegt wurden,*
2. *Welche **sonstigen Sicherheitsaudits** oder **Prüfungen** im Bereich der der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche **Prüfungsgrundlage** und welcher **Geltungsbereich** hierfür festgelegt wurden oder*
3. ***Wie sichergestellt wird**, dass die für das Unternehmen besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden und ob dabei der **Stand der Technik** eingehalten wird.*

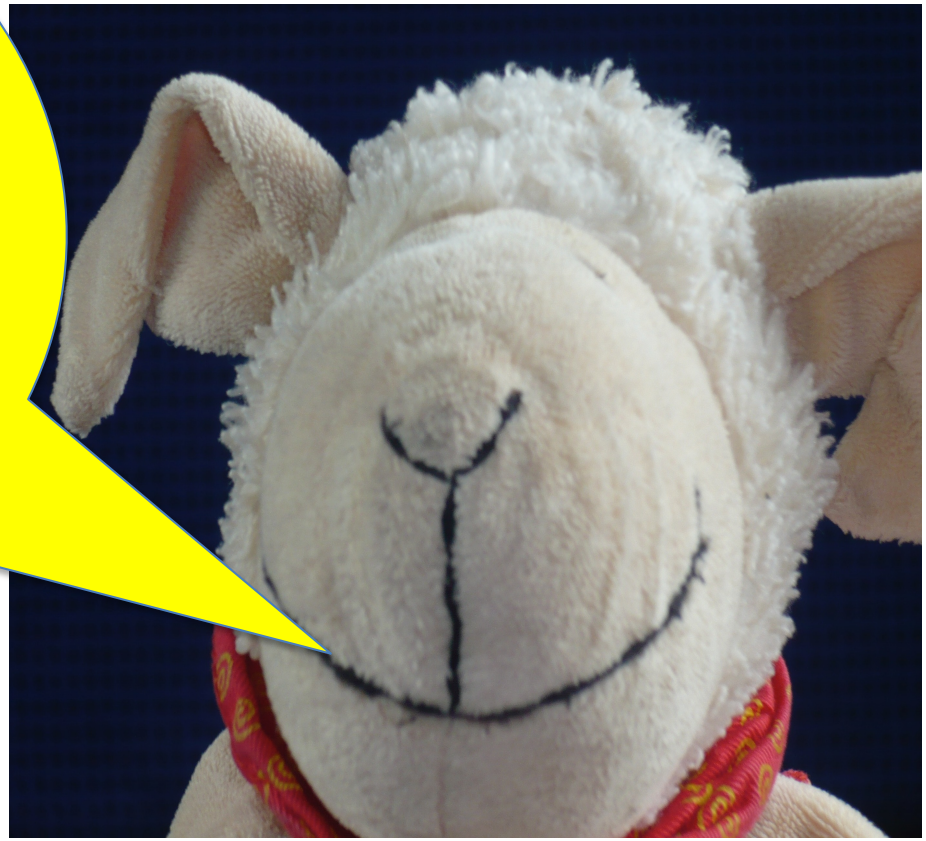
(2) – (8)

Auch diese Unternehmen trifft nach § 8f Abs. 7 und Abs. 8 eine umfassende Meldepflicht!




Und das muss ich nun
Alles umsetzen???

ja und nein!
oder besser:
nein und ja!!!



§ 8d Anwendungsbereich

*(1) Die §§ 8a und 8b sind **nicht** anzuwenden auf **Kleinstunternehmen** im Sinne der Empfehlung **2003/361/EC** der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleineren und mittleren Unternehmen (Abl. L 124 vom 20.05.2003, S. 36). Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anzuwenden.*

***Artikel 2** (Empfehlung 2003/361/EC v. 6.5.2003)*

Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen

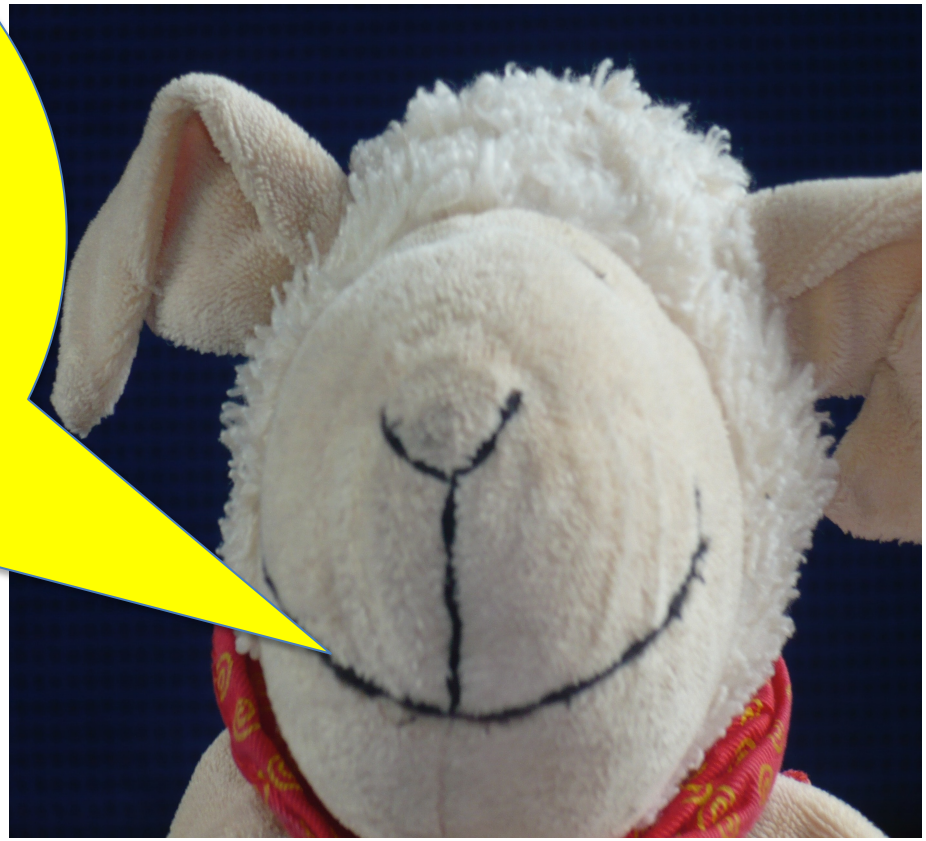
(**1**) Die Größenklasse der **Kleinstunternehmen** sowie der **kleinen und mittleren Unternehmen (KMU)** setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 42 Mio. EUR beläuft.

(**2**) Innerhalb der Kategorie der KMU wird ein **kleines Unternehmen** als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. dessen Jahresbilanz 10 Mio. EUR nicht übersteigt.

(**3**) Innerhalb der Kategorie der KMU wird ein **Kleinstunternehmen** als ein Unternehmen definiert, das **weniger als 10 Personen beschäftigt** und **dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet**.


Na Gott-sei-Dank, dann bin ich ja aus Allem raus!!!???

Du selbst vielleicht ja, aber wahrscheinlich Deine Kunden bzw. deren Kunden nicht! Und die geben es nach „unten“ weiter!!!



Denn:

Sicherheit in der Informationstechnik im Sinne des **BSI-Gesetzes** bedeutet nach **§ 2 BSIG**:

Die Einhaltung bestimmter **Sicherheitsstandards**, die

1. die **Verfügbarkeit**, **Komponenten** oder **Prozesse** oder
2. bei der Anwendung von informationstechnischen **Systemen**, **Komponenten** oder **Prozessen**

betreffen.

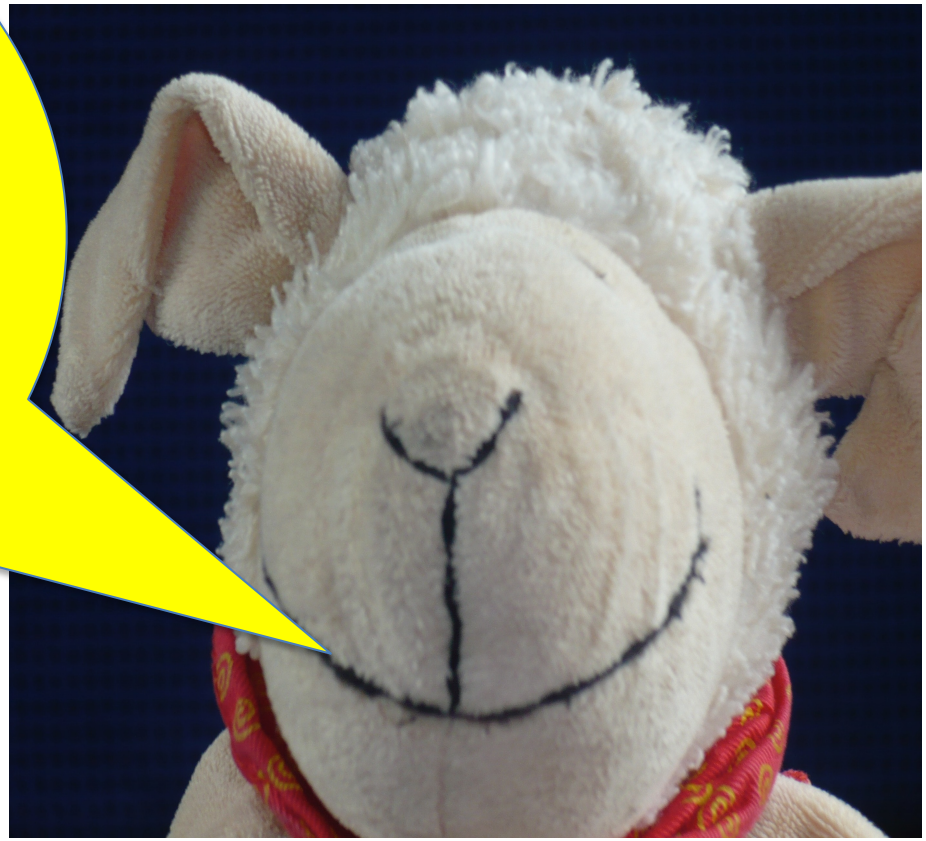
Fazit:

Selbst die Unternehmen die nicht **unmittelbar** betroffen sind, sind es aber zumindest **mittelbar**, weil über kurz oder lang diese Anforderungen an sie weitergeleitet werden, soweit sie

„***Dienstleistungen***“ (wie **Pflege**, **Wartung**, **Service**, **Rechenzentrums-/Clouddienste**, **Hardware-/Softwarelieferung)**

für betroffene Unternehmen **erbringen** bzw. **erbringen wollen** und damit in Verbindung mit deren **Netzwerken** kommen!

Im Übrigen gibt es dann auch noch den § 9b BSI-Gesetz!!!



§ 9b Untersagen des Einsatzes kritischer Komponenten

*(1) Der **Betreiber einer kritischen Infrastruktur** hat den **geplanten erstmaligen Einsatz einer kritischen Komponente** gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz **anzuzeigen**. In der Anzeige sind die **kritische Komponente** und **die geplante Art ihres Einsatzes** anzugeben. Satz 1 gilt nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.*

*(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt **bis zum Ablauf von zwei Monaten nach Eingang der Anzeige** nach Absatz 1 **untersagen** oder **Anordnungen erlassen**, **wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt**. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob*

1. ***der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird**,*
2. ***der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedsstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten,** oder*
3. ***der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht**.*

***Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet**. Das Bundesministerium des Innern, für bau und Heimat kann die Frist gegenüber dem Betreiber **um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist**.*

*(3) Kritische Komponenten gemäß § 2 Absatz 13 **dürfen nur eingesetzt werden**, **wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Infrastruktur abgegeben hat**. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, **wie** der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.*

(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt ***untersagen*** *oder* ***Anordnungen erlassen****,* ***wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.***

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann ***nicht vertrauenswürdig sein****, wenn hinreichende Anhaltspunkte dafür bestehen, dass*

1. ***er gegen die in der Garantieerklärung eingegangenen Verpflichtungen verstoßen hat,***
2. ***in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,***
3. ***er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,***
4. ***Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,***
5. ***die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotential aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken können oder***
6. ***die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.***

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

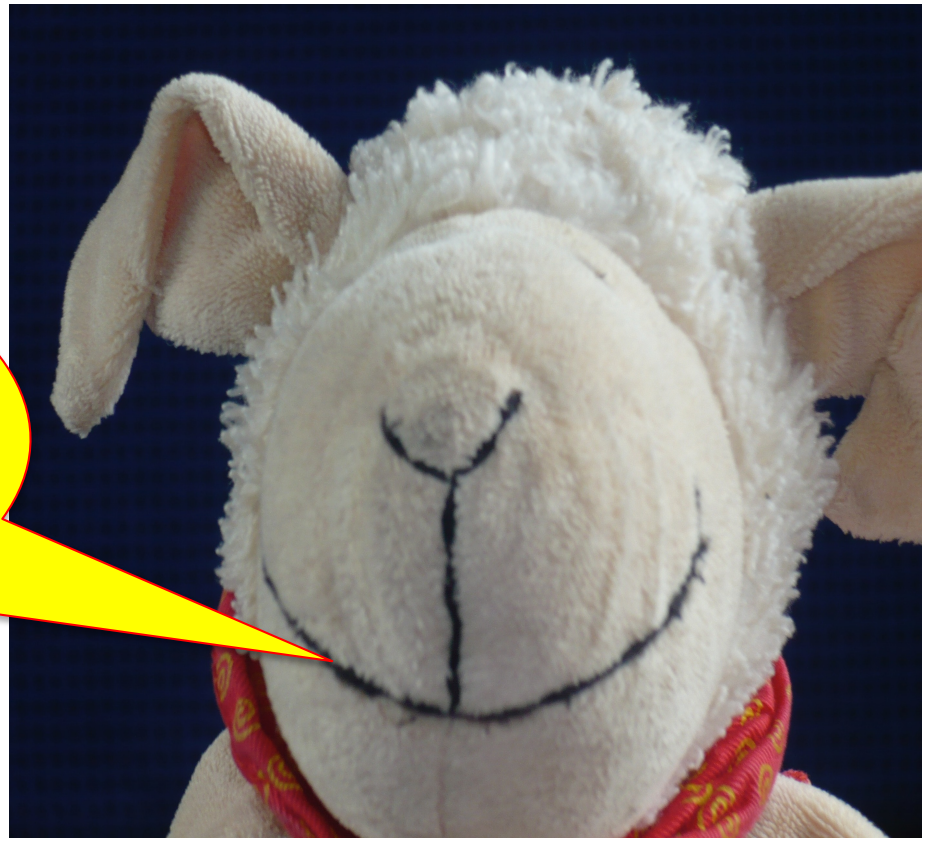
1. *den geplanten Einsatz* ***weiterer*** *kritischer Komponenten desselben Typs und desselben Herstellers untersagen und*
2. *den* ***weiteren Einsatz*** *kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.*

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz ***aller*** *kritischen Komponenten des Herstellers im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.*


Alle Achtung!!!


Und was hat sich im Telekommunikations-gesetz geändert???

Na da schaun wir mal, dann sehn wir schon!*



* *Zitat eines abgedankten Kaisers eines auch Heute noch gesellschaftlich gepflegten Ballspiels!*

Im **Telekommunikationsgesetz** sind durch das IT-Sicherheitsgesetz (**nur!?**) die Vorschriften des

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

§ 165 Technische und organisatorische Schutzmaßnahmen

§ 169 Daten- und Informationssicherheit

geändert worden.

Im **Telekommunikationsgesetz** sind durch das IT-Sicherheitsgesetz (nur!?) die Vorschriften des

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

§ 165 Technische und organisatorische Schutzmaßnahmen

§ 169 Daten- und Informationssicherheit

geändert worden.

§ 165 Technische und organisatorische Schutzmaßnahmen

(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz des Fernmeldegeheimnisses und

2. gegen die Verletzung des Schutzes personenbezogener Daten

*Dabei ist der **Stand der Technik** zu berücksichtigen.*

*(2) Wer ein **öffentliches Telekommunikationsnetz** **betreibt** oder **öffentlich zugängliche Telekommunikationsdienste** **erbringt**, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen*

1. *zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und –diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und*
2. *zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und –diensten.*

*Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei den Maßnahmen nach Satz 2 ist der **Stand der Technik** zu berücksichtigen.*

(3) …

*(4) Kritische Komponenten im Sinne von § 2 Absatz 13 des **BSI-Gesetzes** dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotential nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.*

....


Und was ist das schon wieder???

Ein **„*öffentliches Telekommunikationsnetz*“** ist ein Telekommunikationsnetz, das ganz oder überwiegend **der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste dient**, die **die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen**, **§ 3 Nr. 42 TKG.**

„*öffentlich zugängliche Telekommunikationsdienste*“ sind **einem unbestimmten Personenkreis zur Verfügung stehende Telekommunikationsdienste**, **§ 3 Nr. 44 TKG.**

„*öffentlich zugängliche Telekommunikationsdienste*“ sind einem unbestimmten Personenkreis zur Verfügung stehende Telekommunikationsdienste,
§ 3 Nr. 44 TKG.

„*Telekommunikationsdienste*“ sind in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und –dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen:

a) Internetzugangsdienste
b) interpersonelle Telekommunikationsdienste
c) Dienste die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste , die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden,

§ 3 Nr. 61 TKG.

Ja, ja ist ja schon gut! Ein Blick ins Gesetz erleichtert die Rechtsfindung:

Im **Telekommunikationsgesetz** sind durch das IT-Sicherheitsgesetz (**nur!?**) die Vorschriften des

- § 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten
- § 165 Technische Schutzmaßnahmen
- **§ 169 Datensicherheit**

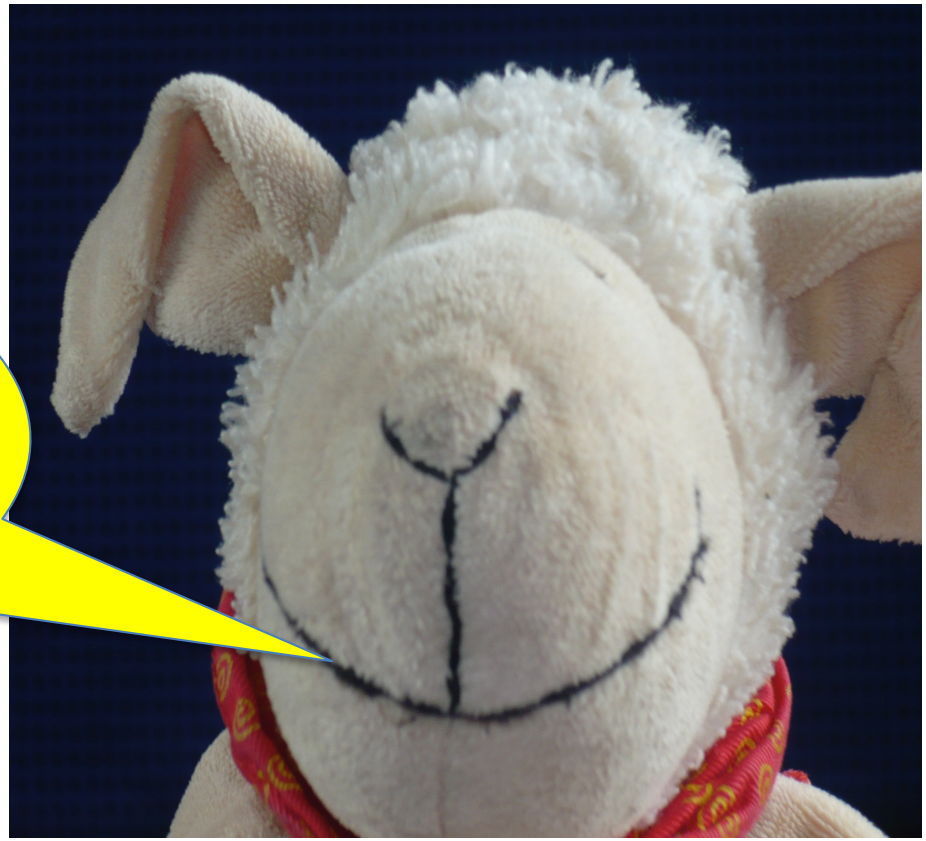
geändert worden.

Im **§ 169 TKG** hat sich neben der Überschrift, die anstelle von „***Datensicherheit***“ nunmehr „***Daten- und Informationssicherheit***“ lautet, im Wesentlichen nur eine Änderung durch einen neuen Absatz 4 ergeben.

*(**4**) Werden dem Anbieter des Telekommunikationsdienstes nach Absatz 1 Satz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. …*


Wenn ich das richtig verstanden habe, sind die Regelungen im TKG mindestens genauso hart wie im BSI-Gesetz???

Na klar Du Schnellmerker, das TKG ist lediglich ein Spezialgesetz!



Im **Telekommunikationsgesetz** sind durch das IT-Sicherheitsgesetz (**nur!?**) die Vorschriften des

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

§ 165 Technische und organisatorische Schutzmaßnahmen

§ 169 Daten- und Informationssicherheit

geändert worden.

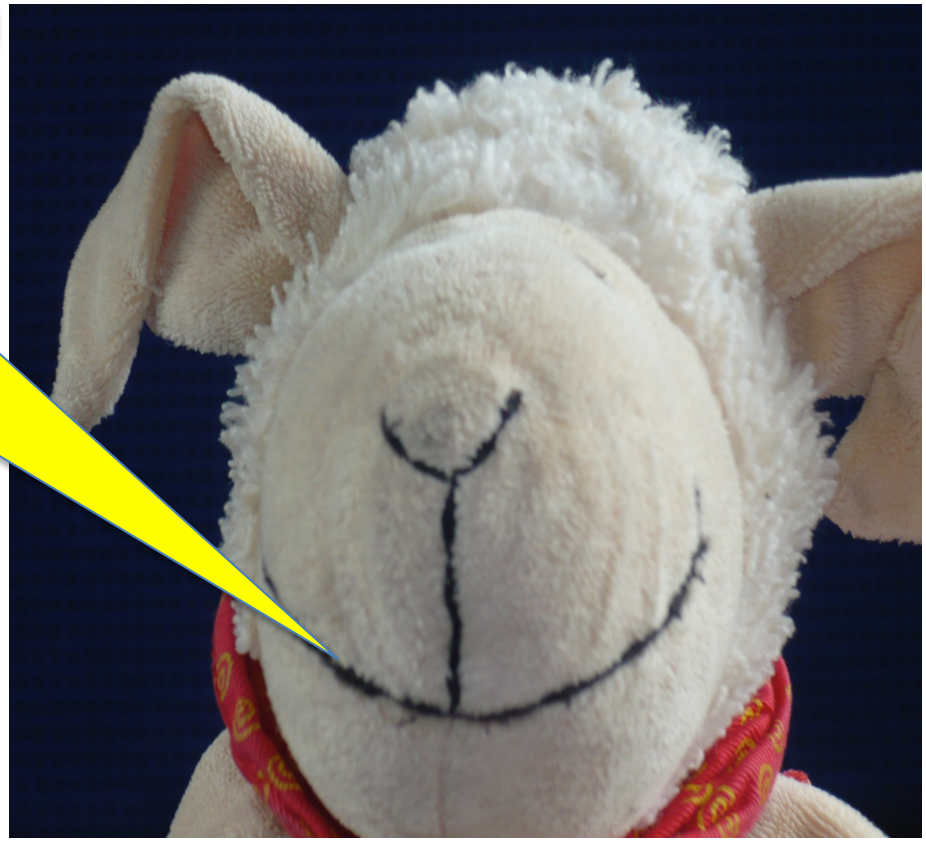
§ 100 TKG in der **bislang** geltende Fassung:

§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, darf der Diensteanbieter zum **Erkennen**, **Eingrenzen** oder **Beseitigen** von **Störungen** oder **Fehlern** an Telekommunikationsanlagen die **Bestandsdaten** und **Verkehrsdaten** der Teilnehmer und Nutzer erheben und verwenden.

(2) ...

Den gibt's nicht mehr!
Das ist jetzt
§ 12 TTDSG*



*Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)

§ 12 TTDSG in der geltenden Fassung:

§ 12 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, dürfen Verpflichtete nach § 3 Absatz 2 Satz 1 **Verkehrsdaten** der Endnutzer sowie die **Steuerdaten** eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, verarbeiten um **Störungen** oder **Fehler** an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Eine Verarbeitung der Verkehrsdaten zu anderen Zwecken ist unzulässig. …

(2) Die **Verkehrsdaten** und **Steuerdaten** sind unverzüglich zu löschen, sobald sie für die Beseitigung der **Störung** nicht mehr erforderlich sind.

Achtung!!!

Die Regelungen des **§ 12 TTDSG** greifen - soweit sie das „***Erheben***“ und „***Verwenden***“ von **Verkehrs- und Steuerdaten** legitimieren - **immer**

in den **Anspruch des einzelnen Nutzers auf Wahrung des Fernmeldegeheimnisses** (**§ 3 TTDSG (neu), § 88 TKG (alt), Art. 10 Abs. 1 GG**) und

sein **Grundrecht auf Informelle Selbstbestimmung** (**Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG**) **ein!!!**

Daneben ist auch **Artikel 6** der **Richtlinie 2002/58/EG** des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (**Datenschutzrichtlinie für elektronische Kommunikation**) zu beachten, der **grundsätzlich die Löschung von Verkehrsdaten vorschreibt, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden**.

Gemäß **Artikel 15 Abs. 1 RL 2002/58/EG** können die Mitgliedsstaaten unter bestimmten Voraussetzungen Rechtsvorschriften erlassen, welche **Artikel 6 RL 2002/58/EG zum Schutz** der nationalen Sicherheit, der Landesverteidigung, der öffentlichen Sicherheit sowie der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen **beschränken**.

Nach der deutschen Übersetzung des Erwägungsgrund **29 RL 2002/58/EG** kann der Diensteanbieter

Verkehrsdaten in Bezug auf Teilnehmer und Nutzer **in Einzelfällen** verarbeiten,

- ***„um technische Versehen“*** **oder**
- ***„Fehler bei der Übertragung von Nachrichten“*** zu ermitteln.

Für Fakturierungszwecke notwendige Verkehrsdaten ebenfalls verarbeiten, ***„um Fälle von Betrug“*** **ermitteln und abstellen zu können**, die in der Nutzung von elektronischen Kommunikations-diensten **„ohne entsprechende Bezah-lung“** liegen.

Normadressat des **§ 12 TTDSG** – also der, der was machen muss oder darf ist der **Anbieter von Telekommunikationsdiensten**

Erfasst sind von der Vorschrift des **§ 12 TTDSG** die **Verkehrs- und Steuerdaten** der Teilnehmer und Nutzer
→ Diese dürfen **erhoben** und **verwendet**, also

- **gespeichert**,
- **verändert**,
- **übermittelt**,
- **gesperrt**,
- **gelöscht**,
- **in sonstiger Weise genutzt werden**.

Wenn es dem

„*Erkennen*“ „*Eingrenzen*“ „*Beseitigen*“

von „***Störungen***“ oder „***Fehlern***“ an **Telekommunikationsanlagen*** dient!

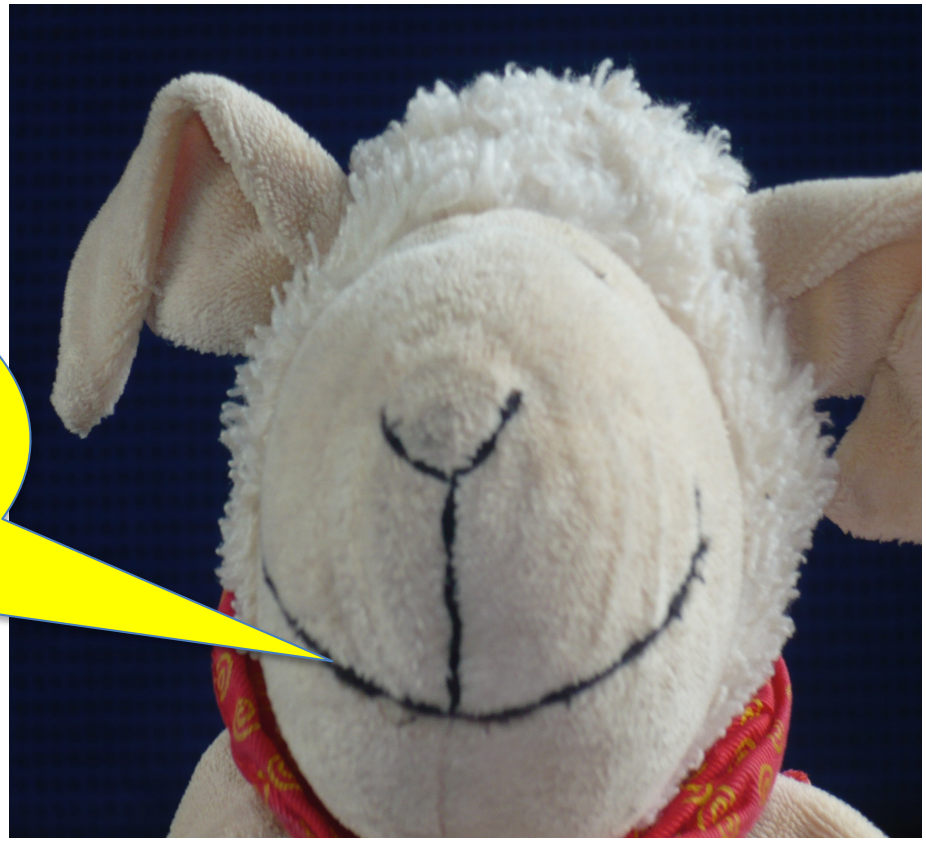
Das „*Eingrenzen*“ oder „*Beseitigen*“ setzt (jedenfalls) **begrifflich** voraus, dass bereits ein „***Fehler***“ **aufgetreten ist**, oder eine „***Störung***“ **ausgemacht wurde**!

Aber Achtung: Dies kann anders gesehen werden, soweit es das **„*Erkennen*“** betrifft!

*Telekommunikationsanlagen sind gemäß § 3 Nr. 60 TKG technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (s.o.).
Der Begriff der „Telekommunikationsanlagen“ umfasst nicht nur die Systeme, welche die Nachrichten transportieren, sondern auch die Systeme, die das Netzmanagement sichern, etwa Überwachungs-, Steuerungs-, Qualitätssicherungs- und Lenkungssysteme (Beck´scher TKG Kommentar § 100. Rdn. 5, BGH, NJW 2011,1509 (1511))


Und was sind nun
„Störungen“ oder
„Fehler“???

Na da scheiden sich nun die (juristischen) Geister!



Man könnte einen „***Fehler***“ einer Telekommunikationsanlage bereits dann bejahen, wenn diese – in welcher Hinsicht auch immer – **irgendwie** nicht ordnungsgemäß funktioniert (z.B. ein Sekundärsystem nicht ordnungsgemäß arbeitet, was sich auf die eigentliche Signalübertragung gar nicht auswirkt).

Aber:

Nach Erwägungsgrund **29 RL 2002/58/EG** kann der Diensteanbieter indes

Verkehrsdaten in Bezug auf Teilnehmer und Nutzer (**nur**) verarbeiten, „**um technische Versehen oder Fehler bei der Übertragung von Nachrichten**“ zu ermitteln.

Für Fakturierungszwecke notwendige Verkehrsdaten ebenfalls verarbeiten, „**um Fälle von Betrug“ ermitteln und abstellen zu können**, die in der Nutzung von elektronischen Kommunikations-diensten „**ohne entsprechende Bezah-lung**“ liegen.

→ Dieser *„enge“* Fehlerbegriff (*„bei“*) ist ist nach den Grundsätzen der unionsrechtlichen Auslegung nationalen Rechts auch für das deutsche Recht maßgebend*

*BeckTKG-Komm/Braun, 4. Aufl., § 100, Rn. 8 mwN

Umstritten ist, ob das Erheben und Verwenden von Daten zum „***Erkennen***“ von „***Störungen***“ es erfordert,

dass bereits **tatsächliche Anhaltspunkte** für das Vorliegen solcher Störungen gegeben sind

oder

ob die Datenerhebung und –verwendung auch **ohne** das Vorliegen **solcher Anhaltspunkte** zulässig ist.

Zum Teil wird unter Verweis auf Satz 1 des **Erwägungsgrundes 29** der **RL 2002/58/EG** die Möglichkeit einer solchen Datenerhebung abgelehnt.

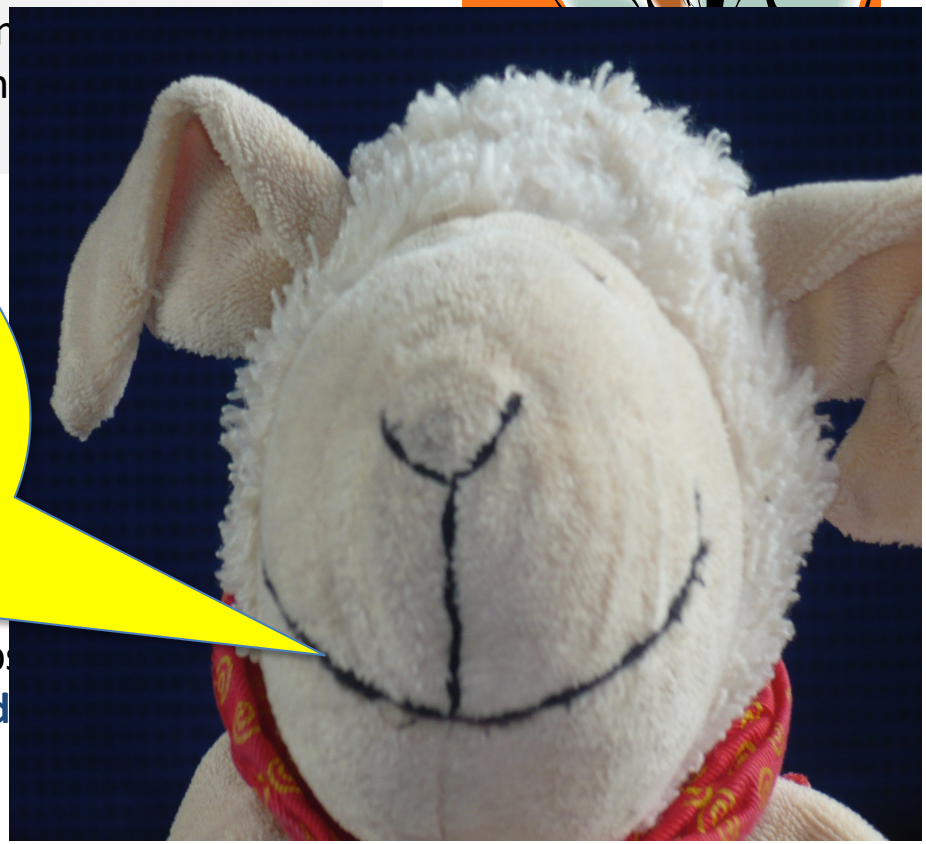
Der Begriff der „***Störung***“ wird zum Teil in der juristischen Literatur in Umsetzung der Richtline, umfassend als **jede** vom Diensteanbieter **nicht gewollte Veränderung** der von ihm für sein Telekommunikationsangebot genutzten technischen Einrichtungen verstanden; d.h. die **Störung** wird auf Grund des Wortlauts der deutschen Übersetzung der **RL 2002/58/EG nicht in Verbindung mit der Nachrichtenübermittlung** gesehen!
Dabei soll der Diensteanbieter sogar berechtigt sein, auch **abstrakten Gefahren** für die Funktionstüchtigkeit des Telekommunikationsbetriebes entgegenzuwirken.

!!!

Da zwar das „***Eingrenzen***“ oder „***Beseitigen***“ (jedenfalls) **begrifflich** voraussetzt, dass bereits ein „***Fehler***“ **aufgetreten ist**, oder eine „***Störung***“ **ausgemacht wurde**, dies aber für das „***Erkennen***“ von Störungen nicht gegeben ist, wurde bislang zum Teil argumentativ versucht insoweit auch „***putative generelle Maßnahmen***“ als mit **§ 100 TKG (alt) bzw. § 12 TTDSG (neu)** vereinbar darzustellen!
Das würde bedeuten, dass im Rahmen **§ 12 TKG** um abstrakte Störungen / Gefahren zu „**Erkennen**“ auch das vorbeugende („***ansatzlose***“) Speichern von **Verkehrsdaten** erlaubt wäre.

Der Begriff der „***Störung***“ wird zum Teil in der Literatur in Umsetzung der Richtline umfassend als **jede** vom Diensteanbieter **nicht gewollte Veränderung** der von ihm für sein Telekommunikationsangebot genutzten technischen Einrichtungen verstanden; d.h. die Störung wird auf Grund des Wortlauts der deutschen Übersetzung der **RL 2002/58/EG nicht in Verbindung mit der Nachrichtenübermittlung** gesehen!
Dabei soll der Diensteanbieter sogar berechtigt sein
Gefahren für die Funktionstüchtigkeit des Telekomm
entgegenzuw

Die zeitliche Grenze des „*Erhebens*“ oder „*Verwendens*“ wird vom BHG im Einzelfall zur Zeit noch bei 7 Tagen gesehen!



ni
Maß
Das würd G um abs
das vorbeugende (von **Verkehrsd**

Der Begriff der „***Störung***“ wird zum Teil in Umsetzung der Richtline umfassend al… …ter nicht gewollte Veränderung der von ihm… …gebot genutzten technischen Einri… …rd auf Grund des Wortlauts de… …cht in Verbindung mit der M…

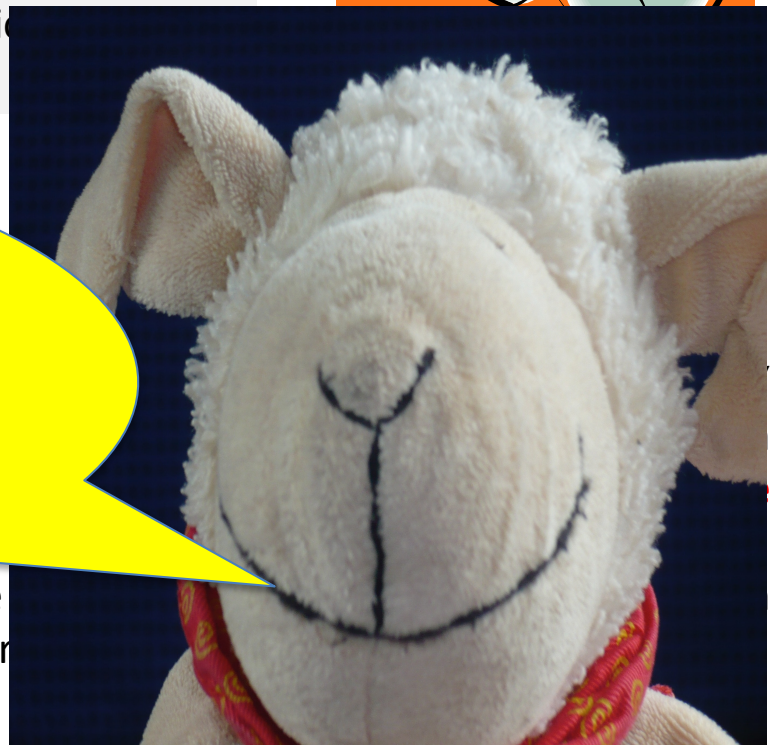
…ein… …h abstrakten …nik… …onspet…

Müsste ich das mit diesem „Speichern“ nicht schon von Irgendwo kennen???

Da… …nfalls) **begrif**… …**r**“ **aufge**… …**cht wurde**, dies … …gen nicht geg… … argumentativ versuc… …**trelle Maßnahmen** … …bar darzustellen!
Das würde bedeuten, dass im Rahmen **§ 100 TKG** um abstrakte Stö…nge… …**hmen**“ auch das vorbeugende („**ansatzlose**“) Speichern von **Verkehrsdaten** erlaub… …äre.

Der Begriff der „**Störung**“ wird zum Teil in Umsetzung der Richtline umfassend als **jede** vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telekommunikationsangebot genutzten technischen Einrichtungen verstanden; d.h. die Störung wird auf Grund des Wortlauts der deutschen Übersetzung der **RL 2002/58/EG nicht in Verbindung mit der Nachrichtenübermittlung** gesehen!
Dabei soll der Diensteanbieter sogar berechtigt sein, auch **abstrakten Gefahren** für die Funktionstüchtigkeit des Telekommunikati
entgegenzuwirken.

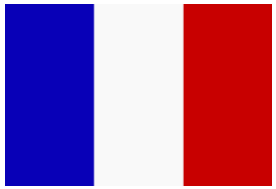
Genau!!!
Das hieß an anderer Stelle
„*Vorratsdatenspeicherung*“
!!!



ni
Maßnah
Das würde bedeute abstrakte
das vorbeugende („**ansatzlose**“) Speichern von **Verkehrsdaten** er

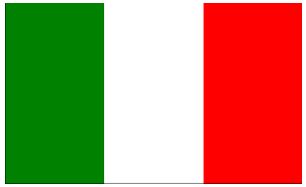
Erhebliche **Zweifel** an einer derartigen Interpretationsmöglichkeit u.a. des Begriffs „***Störung***“ ergeben sich aber, worauf insbesondere *Braun** hinweist auch im Hinblick auf den Wortlaut des **Erwägungsgrundes 29 RL 2002/58/EG** aus der Gegenüberstellung der deutschen Übersetzung mit den Übersetzungen anderer Staaten.

(**29**) Der Diensteanbieter kann Verkehrsdaten in Bezug auf Teilnehmer und Nutzer in Einzelfällen verarbeiten, um **technische Versehen oder Fehler bei der Übertragung von Nachrichten zu ermitteln**.



(**29**) Au besoin, et au cas par, le fournisseur d´un service peut traiter des données relatives au trafic qui concernent des abonnés ou des utilisateurs s´il s´agit de déceler **une défaillance technique ou une erreur dans la transmission des communications**.

(**29**) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect **technical failure or errors in the transmission of communication**.

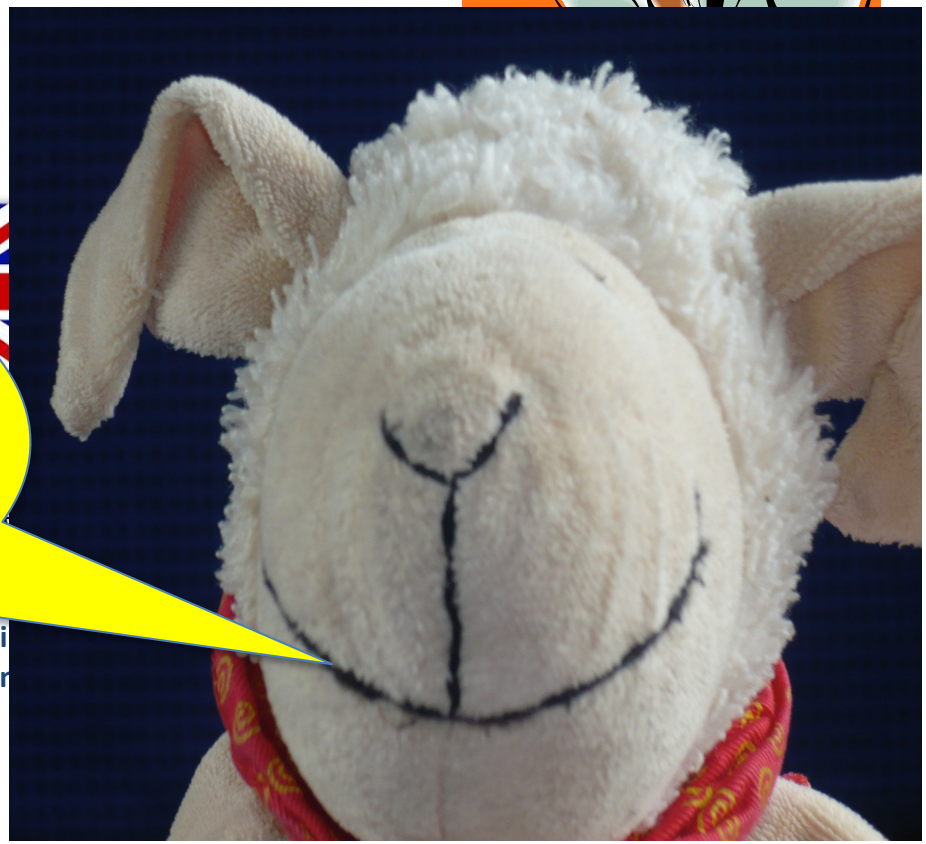


(**29**) Il fornitore di servici può trattare I dati sul traffcio relativi agli abbonati ed agli utenti ove neccario in singoli casi per individuare **problemi tecnici od errori materiali nella trasmissione delle comunicazioni**.

(**29**) De ser necesario, el proveedor del servicio puede tratar, en casos concretos, los datos de tráficio relacionados con los abonados yusarios, a fin **de detectar fallos o errores tècnicos en la transmisión de las comunicaciones**.

BeckTKG-Komm/Brau, 4. Aufl., § 100, Rn. 11

Erhebliche **Zweifel** an einer derartigen Interpretationsmöglichkeit u.a. des Begriffs „***Störung***“ ergeben sich aber, worauf insbesondere *Braun** hinweist auch im Hinblick auf den Wortlaut des **Erwägungsgrundes 29 RL 2002/58/EG** aus der Gegenüberstellung der deutschen Übersetzung mit den Übersetzungen anderer Staaten.



In allen anderen Sprachen wird auch die *„Störung“* auf die konkrete Übertragung von Nachrichten bezogen !

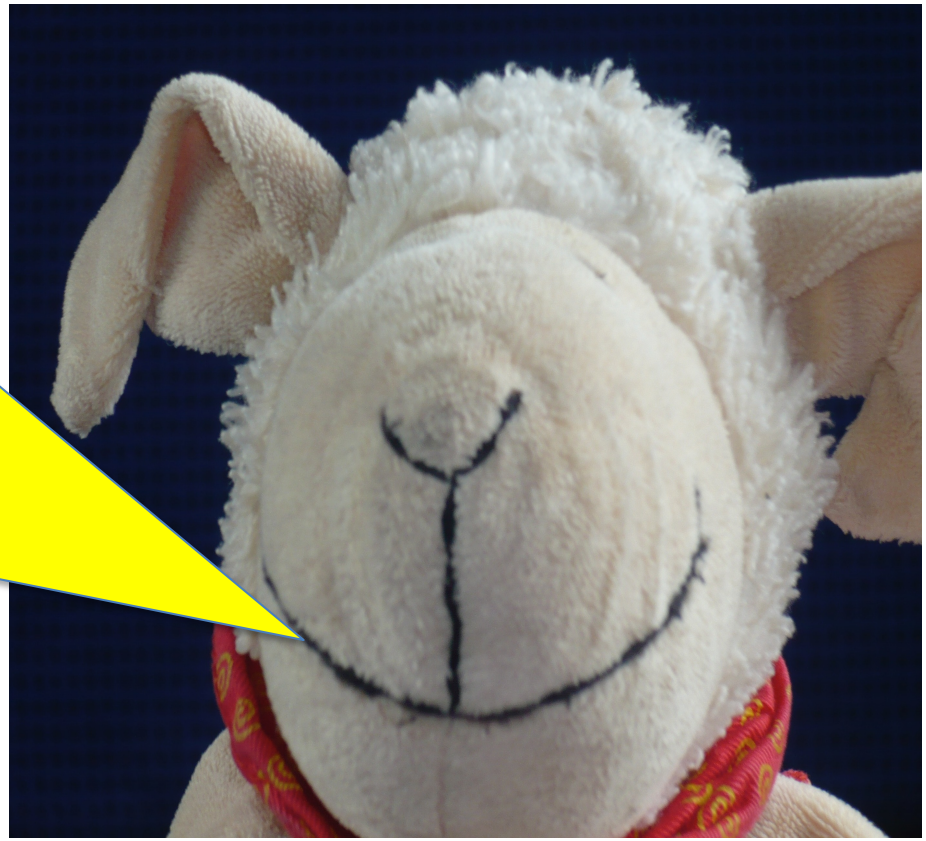
(
k
Be
Nutze
verarbeite
**technische Vers
Fehler bei der
Übertragung von
Nachrichten zu ermitteln.**

**t technical fai
errors in the transr
of communication.**

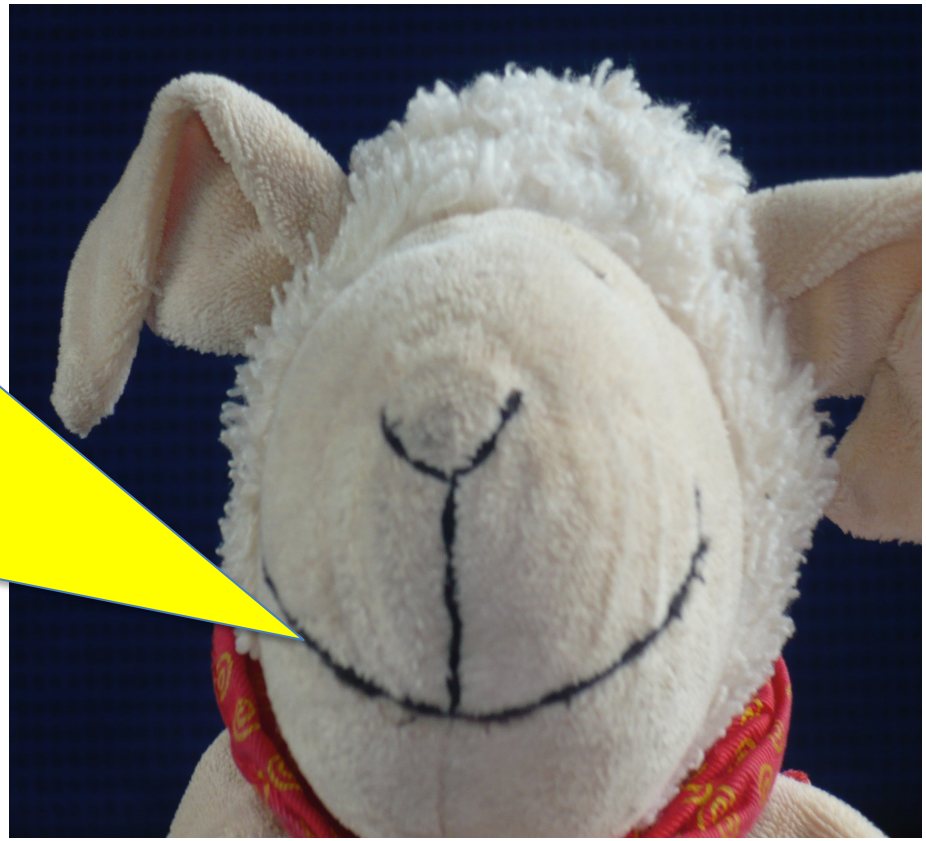
déceler une défaillance technique ou une erreur dans la transmission des communications.

BeckTKG-Komm/Brau, 4. Aufl., § 100, Rn. 11

Es spricht deshalb viel dafür, das der Unionsgesetzgeber eine Daten-*„Erhebung“* und – „Verwendung“ allenfalls in Bezug auf das Ermitteln von *„Störungen“* oder *„Fehlern“* ***„bei der Übertragung von Nachrichten“*** erlauben wollte.



Darüber hinaus spricht der Unionsgesetzgeber ausdrücklich von *„Verarbeitung“* (*„Erhebung“* und *„Verwendung“*) im Einzelfall.



Ergebnis zu **§ 12 Abs. 1 TKG** dürfte deshalb wohl sein, dass der Diensteanbieter in

- **Grundgesetz** und
- **Unionsrecht**

konformer Weise

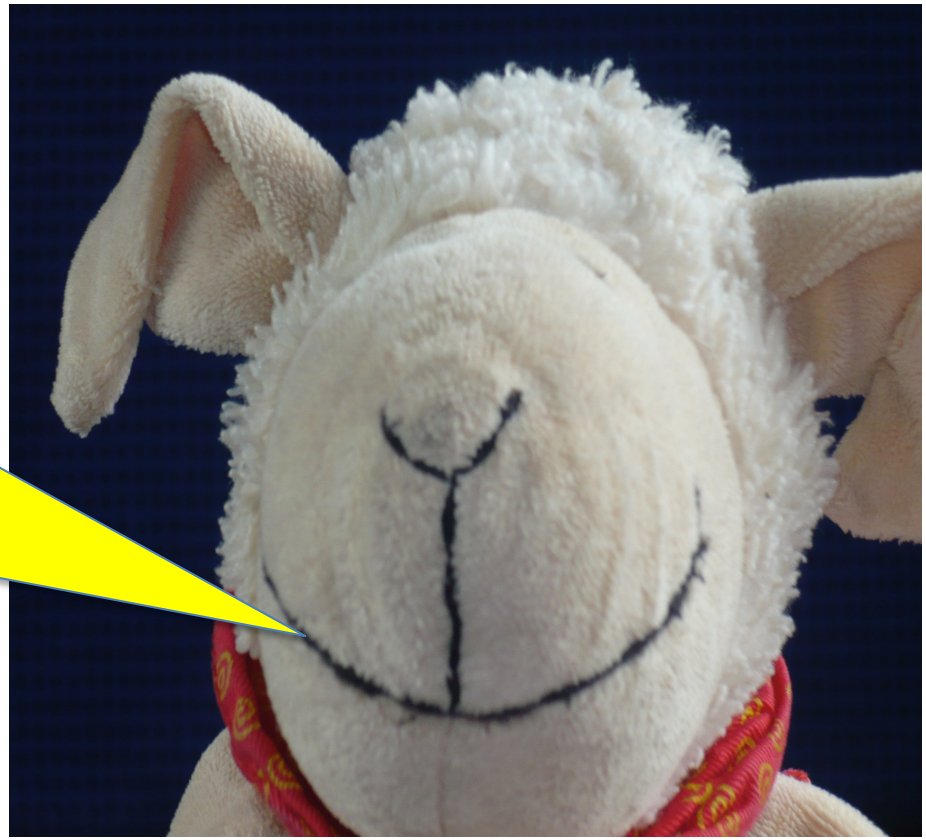
soweit erforderlich, zum **Erkennen**, **Eingrenzen** oder **Beseitigen** von „***aufgetretenen***“ **Störungen** oder **Fehlern** an Telekommunikationsanlagen „***im Einzelfall***“ die **Bestandsdaten** und **Verkehrsdaten** der Teilnehmer und Nutzer erheben und verwenden darf.

§ 12 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten

(1) Soweit erforderlich, dürfen Verpflichtete nach § 3 Absatz 2 Satz 1 **Verkehrsdaten** der Endnutzer sowie **Steuerdaten** eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, („***im Einzelfall***“) verarbeiten, um („***aufgetretene***“) Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

(2) ...

Das war es
oder:
„Nun stehen wir selbst und sehn betroffen, den Vorhang zu und viele Fragen offen!“*



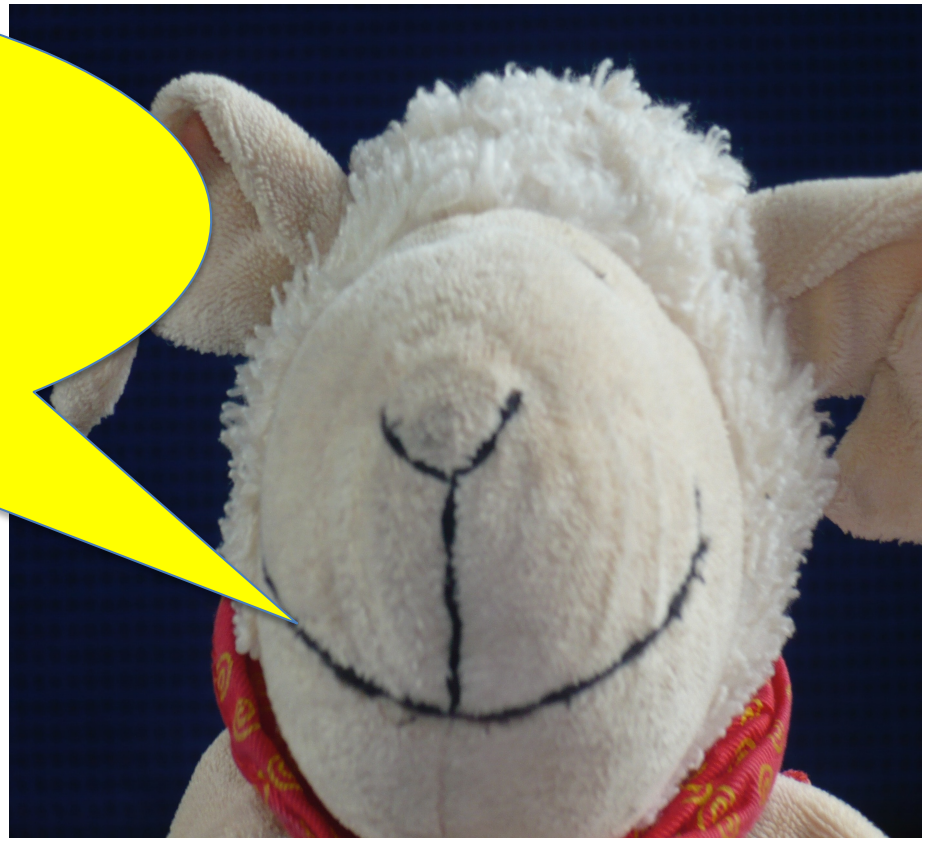
*frei nach Berthold Brecht, Der gute Mensch von Sezuan

Herzlichen Dank für Ihre Aufmerksamkeit!

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

Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai

Anhang!!!



§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

*(**1**) Betreiber **Kritischer Infrastrukturen*** *sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass ig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zu von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihr stechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähig nen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der T lten werden. Organisatorische und technische Vorkehrungen sind angemessen, wen orderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeintr betroffenen Kritischen Infrastruktur steht.*

Kritische Infrastru ch **§ 2 Abs. 10 BSIG**

Einrichtungen, An e davon, die

1. den **Sektoren**
   - **Energie**,
   - **Informationst Telekommuni**
   - **Transport** und
   - **Gesundh**
   - **Wasser**,
   - **Ernährung**
   - **Finanz-** und **Versi gswesen**
   - **Siedlungsabfallentso gung** angehören **und**

2. **von hoher Bedeutung für das Funktionieren des Gemeinwesens sind**, weil durch ihren **Ausfall** oder ihre **Beeinträchtigung erhebliche Versorgungs-engpässe** oder **Gefährdungen für die öffentliche Sicherheit** eintreten würden.

**Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSI-Gesetz näher bestimmt (z.B. Banken, Krankenhäuser, Wasser-/Energieversorger, Bahn usw).*

Kritische Infrastrukturen sind nach **§ 3 Abs. 10 BSIG**

Einrichtungen, **Anlagen** oder **Teile davon**, die

1. den **Sektoren**
   - **Energie**,
   - **Informationstechnik** und **Telekommunikation**,
   - **Transport** und **Verkehr**,
   - **Gesundheit**,
   - **Wasser**,
   - **Ernährung** sowie
   - **Finanz-** und **Versicherungswesen**

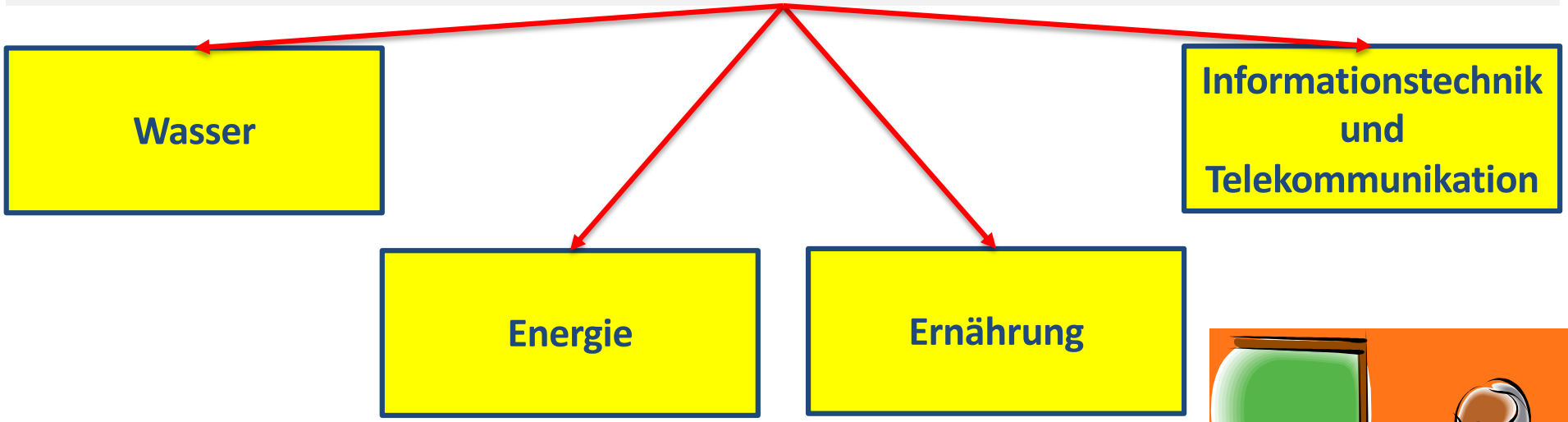
   angehören **und**

2. **von hoher Bedeutung für das Funktionieren des Gemeinwesens sind**, weil durch ihren **Ausfall** oder ihre **Beeinträchtigung erhebliche Versorgungsengpässe** oder **Gefährdungen für die öffentliche Sicherheit** eintreten würden.

**Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSI-Gesetz näher bestimmt (z.B. Banken, Krankenhäuser, Wasser-/Energieversorger, Bahn usw).*

Grundlage ist die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (**BSI-Kritisverordnung – BSI-KritisV**) vom **22. April 2016** (BGBl. I S. 958) geändert durch die „***Erste Verordnung zur Änderung der BSI-Kritisverordnung***“ vom **21. Juni 2017** (BGBl. I S. 1903), nochmals geändert durch die „***Zweite Verordnung zur Änderung der BSI-Kritisverordnung***“ aus dem Jahre 2021.

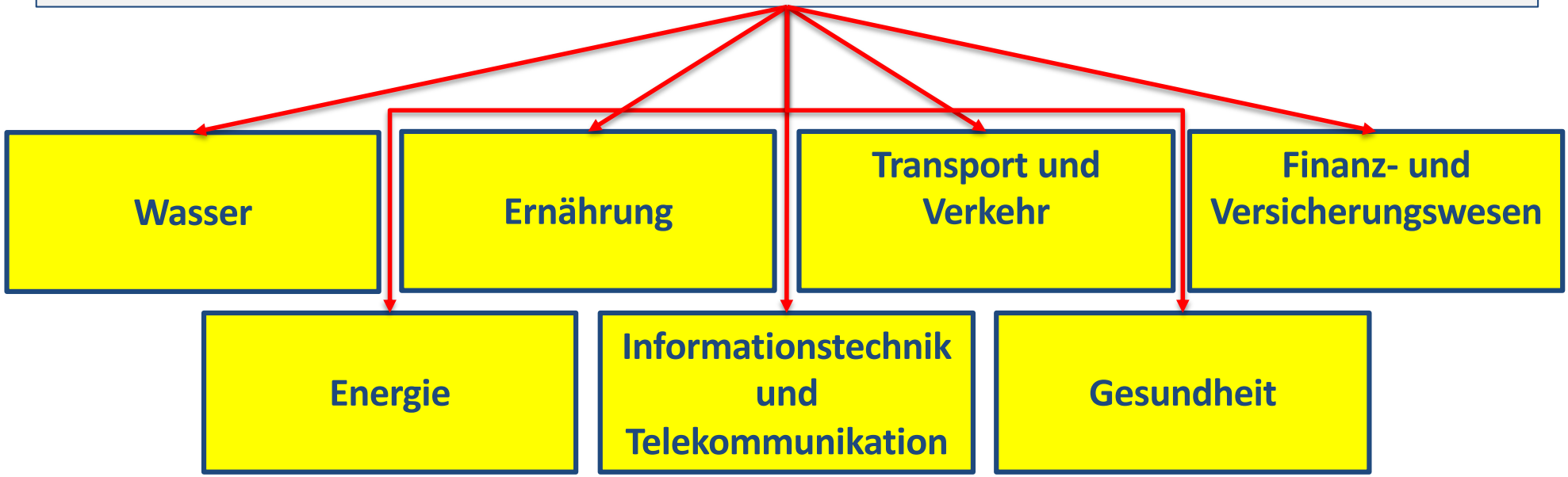
In einem **ersten Schritt** hat die Bundesregierung zunächst durch die **BSI-Kritisverordnung – BSI-KritisV** vom 22. April 2016 Regelungen im Hinblick auf die Bestimmung **Kritischer Infrastrukturen** für bestimmte **Teilbereiche** erstellt. Definiert wurden solche **zunächst für die Bereiche**:



Mit der „*Ersten Verordnung zur Änderung der BSI-Kritisverordnung*“ vom 21.06.2017 erfolgte auch eine Regelung für die **Sektoren**:

- **Transport und Verkehr**
- **Gesundheit**
- **Finanz- und Versicherungswesen**

Damit waren dann sämtliche im Rahmen des **ersten** Schrittes zu identifizierenden **Kritischen Anlagen definiert**:



In einem **zweiten Schritt** werden diejenigen **Kategorien von Anlagen** identifiziert, die für die Erbringung der kritischen Dienstleistungen erforderlich sind.

In einem **dritten Schritt** werden hiervon ausgehend von den identifizierten Anlagenkategorien **konkrete Anlagen** oder **Anlagen Teile** davon bestimmt, die einen **aus gesamtgesellschaftlicher Sicht** bedeutenden „***Versorgungsgrad***“ für die Allgemeinheit aufweisen.

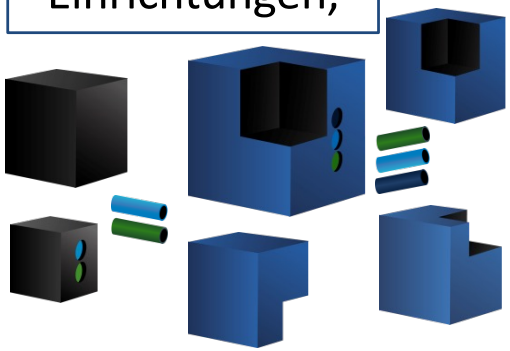
Die Bestimmung erfolgt dabei anhand eines **Schwellenwertes**, der **einer jeden Anlagenkategorie** durch den Verordnungsgeber d.h. dem Bund beigemessen wird.

In **§ 1 der Verordnung** werden zunächst die **Begrifflichkeiten** weiter definiert. Definiert werden:

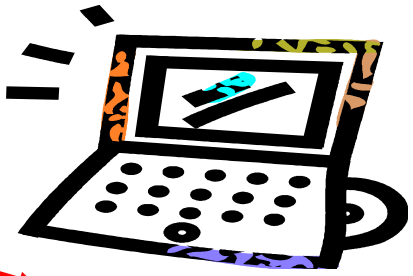
- **Anlagen**
- **Betreiber**
- **kritische Dienstleistung**
- **Versorgungsgrad**
- **Schwellenwert**

Anlagen
i.S.d. Verordnung sind

Betriebsstätten und sonstige **ortsfeste** Einrichtungen,



Maschinen, Geräte und sonstige **ortsveränderliche** technische Einrichtungen



Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind

die zur Erbringung einer kritischen Dienstleistung erforderlich sind; wobei einer Anlage **alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen sind, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen**, die mit den Anlagenbauteilen und Verfahrensschritten **in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung von Bedeutung sein können**. Mehrere Anlagen, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als **gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind**.

Betreiber
i.S.d. Verordnung sind

natürliche oder juristische Personen, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der Anlage oder Teilen davon ausüben**.
Betreiben zwei oder mehr Personen **gemeinsam** eine Anlage, **so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich**.

kritische Dienstleistung
i.S.d. Verordnung ist

eine Dienstleistung **zur Versorgung der Allgemeinheit in den benannten Sektoren**, deren Ausfall oder Beeinträchtigung zu **erheblichen Versorgungsengpassen oder** zu **Gefährdungen der öffentlichen Sicherheit oder zu vergleichbaren Folgen** führen würde.

Für den Sektor
Energie
sind gemäß **§ 2** der Verordnung entsprechende **kritische Dienstleistungen**:

- **1. die Versorgung der Allgemeinheit mit Elektrizität;**
- **2. die Versorgung der Allgemeinheit mit Gas;**
- **3. die Versorgung der Allgemeinheit mit Kraftstoff und Heizöl;**
- **4. die Versorgung der Allgemeinheit mit Fernwärme.**

Für den Sektor
Wasser
sind gemäß **§ 3** der Verordnung entsprechende **kritische Dienstleistungen**:

- **1. die Versorgung der Allgemeinheit mit Trinkwasser;**
- **2. die Beseitigung von Abwasser der Allgemeinheit.**

Für den Sektor
Ernährung
ist gemäß § 4 der Verordnung entsprechende **kritische Dienstleistung**:

die Versorgung der Allgemeinheit mit Lebensmitteln.

Für den Sektor Informationstechnik und Telekommunikation sind gemäß **§ 5** der Verordnung entsprechende **kritische Dienstleistungen**:

die **Sprach- und Datenübertragung** in den Bereichen **Zugang**, **Übertragung**, **Vermittlung** und **Steuerung**

die **Datenspeicherung und Datenverarbeitung** in den Bereichen **Housing**, **IT-Hosting** und **Vertrauensdienste**

Für den Sektor Gesundheit sind gemäß § 6 der Verordnung entsprechende **kritische Dienstleistungen**:

1. die stationäre medizinische Versorgung;
2. die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten die Verbrauchsgüter sind;
3. die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zu Anwendung im oder am menschlichen Körper;
4. die Laboratoriumsdiagnostik.

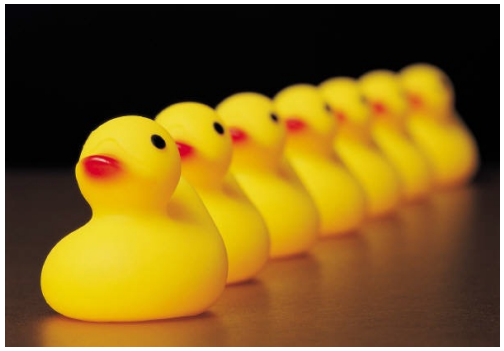
Für den Sektor
Finanz- und Versicherungswesen
sind gemäß § 7 der Verordnung entsprechende kritische Dienstleistungen:

1. die Bargeldversorgung;
2. der kartengestützte Zahlungsverkehr;
3. der konventionelle Zahlungsverkehr;
4. Der Handel mit Wertpapieren und Derivaten sowie die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften;
5. Versicherungsdienstleistungen und Sozialleistung sowie der Grundsicherung für Arbeitssuchende.

Für den Sektor
Transport und Verkehr
ist gemäß § 8 der Verordnung entsprechende **kritische Dienstleistung**:

die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern.

Versorgungsgrad
i.S.d. Verordnung ist



ein Wert mittels dessen **der Beitrag einer Anlage oder Teilen davon im jeweiligen benannten Sektor zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung** bestimmt wird.

Schwellenwert
i.S.d. Verordnung ist

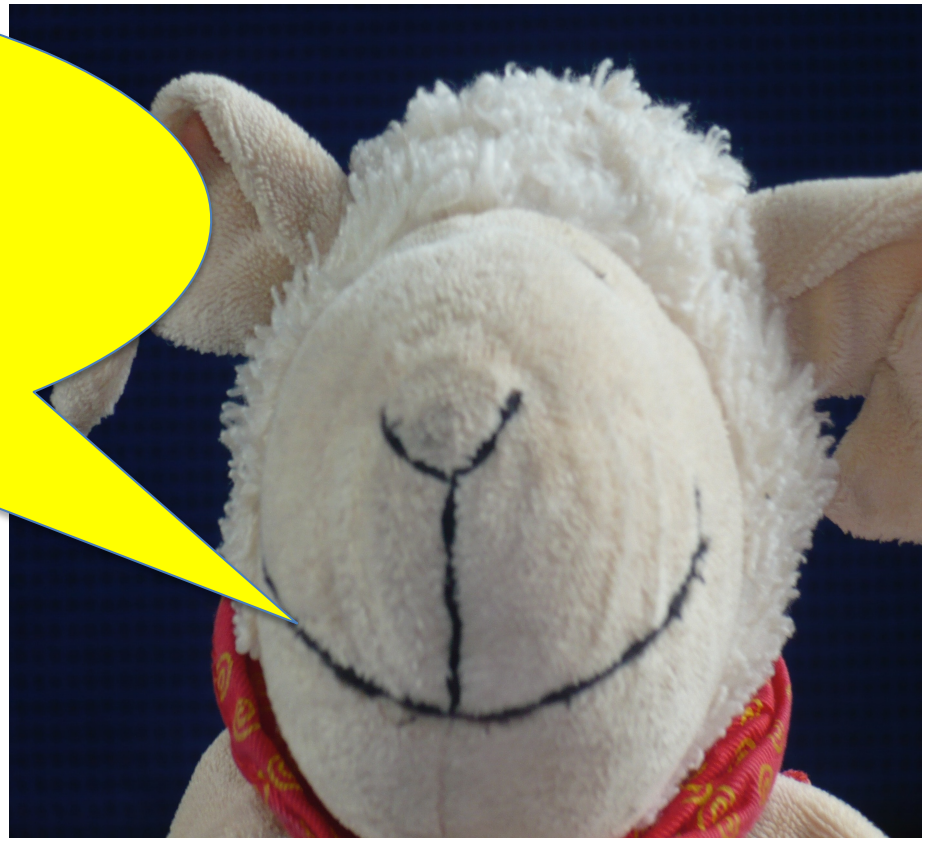
ein Wert, bei dessen **Erreichen** oder dessen **Überschreitung** der **Versorgungsgrad einer Anlage oder Teilen davon als bedeutend** im Sinne von **§ 10 Abs. 1 S.1** des **BSI-Gesetzes** anzusehen ist.

Anlagenkategorie	Bemessungskriterium	Schwellenwert
1. Sprach- und Datenübertragung		
1.1 Zugang		
1.1.1 Zugangsnetz	Teilnehmeranschlüsse nach § 3 Nr. 58 TKG	100.000
1.2 Übertragung		
1.2.1 Übertragungsnetz	Vertragspartner des jeweiligen Dienstes	100.000
1.3 Vermittlung		
1.3.1 IPX	Anzahl angeschl. autonomer Systeme (⌀/J)	100
1.4 Steuerung		
1.4.1 DNS-Resolver	Anzahl d. Vertragsp. d. Zugangsnetzes	100.000
1.4.2 Autoritativer DNS-Server	Anzahl d. Domains f. d. d. Servers autoritativ ist	250.000
1.4.3 Top-Level-Domain-Name-Registry	Anzahl d. Domains d. verwaltet o. betrieben werden	250.000
2. Datenspeicherung- u. Verarb.		
2.1 Housing		

2. Datenspeicherung und Datenverarbeitung		
2.1 Housing		
2.1.1 Rechenzentrum (Housing)	vertragl. vereinb. Leistung in MW	3,5
2.2 IT-Housting		
2.2.1 Serverfarm (Housting)	Anz. d. f. Nutzer betr. physischen Instanzen	10.000
	Anz. d. f. Nutzer betr. virtuellen Instanzen	15.000
2.2.2 Content Delivery Networks	ausgelief. Datenvolumen (Tbyte/J)	75.000
2.3 Vertrauensdienste		
2.3.1 Anl. z. Erbringung v. Vertrauensdiensten	Anz. d. ausgegebenen qualifizierten Zertifikate	500.000
	Anz. d. Zertifikate z. Authentifizierung öfftl. Zugänglicher Server (z.B. TLS/SSL-Zertifikate)	10.000


Und gibt es da jetzt noch was?

Ja, die „*NIS-Richtlinie*“!



Die „*NIS-Richtlinie*“ oder genauer die „*Richtlinie über Maßnahmen zur Gewährung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union*“ wurde am 07.02.2013 von der EU-Kommissarin Neelie Kroes vorgeschlagen und soll die Mitglieder der Europäischen Union zur Erhöhung ihrer IT-Sicherheit d.h. die Sicherheit bei der Nutzung des Internets durch öffentliche und private Nutzer auf einem gemeinsamen Mindeststandard verpflichten.

Die EU-Mitgliedsstaaten haben am 18.12.2015 der zuvor zwischen dem Parlament und dem Rat verhandelten Fassung zugestimmt. Nach Konsolidierung der Texte ist der Entwurf durch den Rat und das Parlament angenommen worden und im August 2016 in Kraft getreten. Danach hatten die einzelnen Mitgliedsstaaten dann 21 Monate Zeit um die Richtlinie in nationale Gesetze umzusetzen und weitere 6 Monate um die entsprechenden Institutionen zu schaffen.

Die „*NIS-Richtlinie*“ „*Richtlinie über Maßnahmen* *samen Netz- und Info* 02.2013 von d ll die Mit IT-Sic öff Mi Die L chen dem P timmt. Nach Kons n Rat und das Parlament a gust 2016 in Kraft getreten. Danach haben die einzelnen Mitgliedsstaaten dann 21 Monate Zeit um die Richtlinie in nationale Gesetze umzusetzen und weitere 6 Monate um die entsprechenden Institutionen zu schaffen.

Der deutsche Gesetzgeber hat seine Hausaufgaben schon erledigt und die entsprechende Umsetzung im Rahmen des BSI-Gesetzes vorgenommen!

Die „*NIS-Richtlinie*“ … „*Richtlinie über Maßnahmen … samen Netz- und Infor… 7.02.2013* von de… soll die Mitg… IT-Sich… öff… Mi… Die … hen dem … hmt. Nach k… at und das Parla… 16 in Kraft getreten. Dana… daten dann 21 Monate Zeit um die … Gesetze umzusetzen und weitere 6 Monate um die entsprechenden Institutionen zu schaffen.

So wurde am 29.06.2017 das „*Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (Nis-Richtlinie)*“ verkündet.

Vor dem Hintergrund der schon bestehenden Regelungen im BSI-Gesetz erweitert das Gesetz auf der Basis der NIS-Richtlinie deshalb im Wesentlichen (nur) die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern und schafft ferner (neu) Regelungen für Anbieter Digitaler Dienste, die ab dem 10.05.2018 Anwendung finden.

So wurde insbesondere in § 8a nach Absatz 3 ein neuer Absatz 4 eingefügt und der bisherige Absatz 4 zu Absatz 5!

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

...

*(4) Das Bundesamt kann **beim Betreiber Kritischer Infrastrukturen** die Einhaltung der Anforderungen nach Abs. 1 **überprüfen**; **es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen**. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zwecke der Überprüfung **das Betreten der Geschäftsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren**. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach den Absätzen 1 und 1a begründeten.*

Und nach § 8b wurde ein (neuer) § 8c eingefügt, wodurch der der § 8c zu § 8d wurde!

§ 8c Besondere Anforderungen an Anbieter digitaler Dienste. (1) [1]Anbieter **digitaler Dienste** haben **geeignete** und **verhältnismäßige technische** und **organisatorische Maßnahmen** zu treffen, **um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen**. [2]Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste **vorzubeugen** oder **die Auswirkungen so gering wie möglich zu halten**.

(2) [1]Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des **Stands der Technik** ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. [2]Dabei ist folgenden Aspekten Rechnung zu tragen:

1. **der Sicherheit der Systeme und Anlagen**,
2. **der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen**,
3. **dem Betriebskontinuitätsmanagement**,
4. **der Überwachung, Überprüfung und Erprobung**,
5. **der Einhaltung internationaler Normen**.

[3]Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.

(3) [1]Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der **erhebliche Auswirkungen** auf die **Bereitstellung** eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. [2]Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:

1. die **Zahl der von dem Sicherheitsvorfall betroffenen Nutzer**, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
2. die **Dauer des Sicherheitsvorfalls**,
3. das von dem Sicherheitsvorfall betroffene **geographische Gebiet**,
4. das **Ausmaß der Unterbrechung der Bereitstellung des Dienstes**,
5. das **Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten**.

[3]Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. [4]Für den Inhalt der Meldungen gilt § 8b Absatz 3 entsprechend, soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. [5]Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedstaats zu unterrichten.

(4) [1]Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 **nicht erfüllt**, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:

1. **die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen**,
2. **die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen**.

[2]Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.

(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaats zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen.

Und in § 8d ehemals § 8c wurde ein (neuer) Absatz 4 eingefügt!

§ 8d Anwendungsbereich

*(1) Die §§ 8a und 8b sind **nicht** anzuwenden auf **Kleinstunternehmen** im Sinne der Empfehlung **2003/361/EC** der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleineren und mittleren Unternehmen (Abl. L 124 vom 20.05.2003, S. 36). Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anzuwenden.*

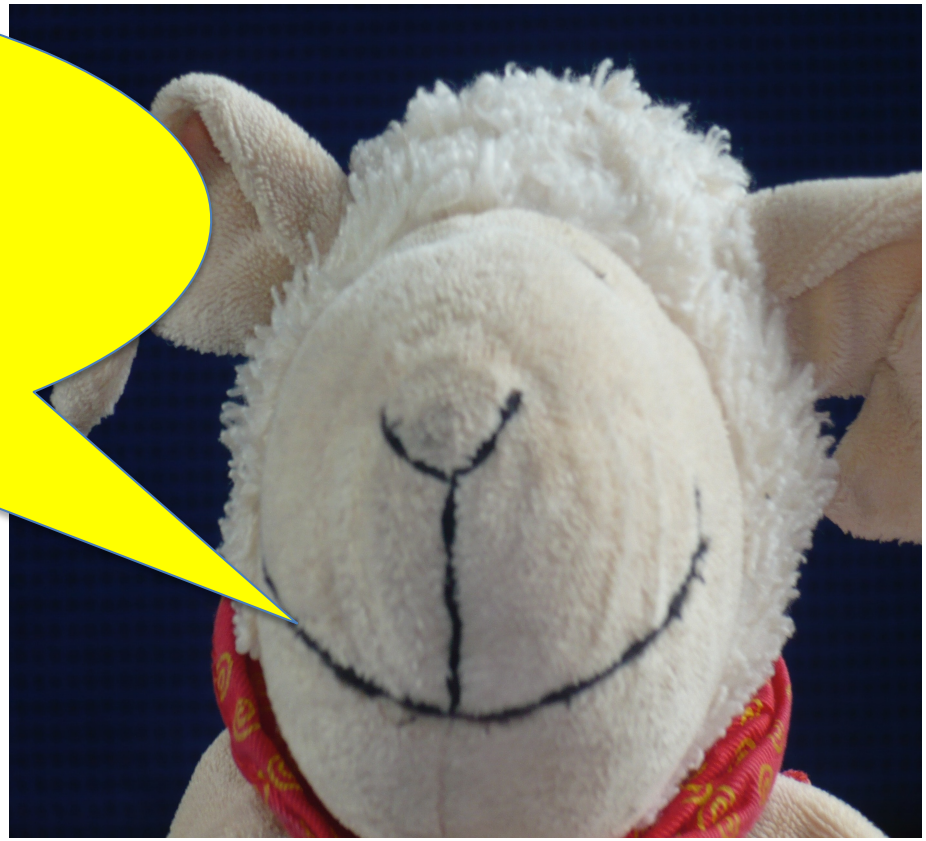
...

(4) § 8c Absatz 1 bis 3 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. § 8c Absatz 3 gilt nicht für Anbieter,

1. ***die ihren Hauptsitz in einem anderen Mitgliedsstaat der Europäischen Union haben oder***
2. ***die, soweit sie nicht in einem Mitgliedsstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedsstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.***

Für Anbieter nach Satz 2 gilt § 8c Absatz 4 nur, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.

Das war es jetzt aber wirklich!



Herzlichen Dank für Ihre Aufmerksamkeit!

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

Schlüter Graf Rechtsanwälte PartG mbB, Dortmund / Hamburg / Dubai