BELASTBARE GUTACHTEN

GASTBEITRAG DR. STEFAN HIRSCHMEIER

Stefan Hirschmeier

Dipl.-Informatiker Dipl.-Kaufmann

IT-Berater und IT-Gutachter

Von der IHK öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung

WARUM BELASTBARE GUTACHTEN?

- Weil **nicht-belastbare Gutachten** kein Sinn machen
  - Können den Sachverständigen in Haftungs-Schwierigkeiten bringen
  - Unnötige Unsicherheiten und Verzögerungen in der Klärung erzeugen
  - Parteien, Richtern und Schlichtern das Leben schwer machen
  - Gutachten sind ein Beweismittel, vor Gericht als auch außer Gericht
- Im Bereich IT-Sicherheit und IT-Forensik geht es oft um Strafrecht
  - Bedeutet: Es geht nicht nur um Geld, sondern ggf. auch um Knast

WIE SIEHT EIN GUTES GUTACHTEN AUS?

Warum muss ich das überhaupt wissen?

- Gutachter: Damit ich ein gutes Gutachten schreiben kann, zu Ruhm und Ehre gelange, und mir selbst keine Haftungs-Eier lege
- Richter /Schlichter: Damit ich einschätzen kann, ob das vorliegende Gutachten mir ein neutrales Bild vom Sachverhalt vermittelt
- Beteiligter: Damit ich einschätzen kann, ob das Gutachten anfechtbar ist

EIN GUTACHTEN IST VIEL TEXT – WORAN BELASTBARKEIT ERKENNEN?


1


2


3


4


5


6


7


8


9

10

11


12


13


14


15


16


17


18

ZUTRÄGLICHE FAKTOREN

- Mit Objektivität erhöht sich auch die Belastbarkeit
- Saubere Arbeit erhöht die Belastbarkeit (nix quick‘n‘dirty)
- Qualitätssicherung erhöht die Belastbarkeit (dreimal prüfen!)
- Dokumentation erhöht die Belastbarkeit (nix agiles manifesto)
- Nachvollziehbarkeit erhöht Belastbarkeit (keine Black box)
- Nicht aus dem Fenster lehnen (Gültigkeit der Aussagen prüfen!)
- Verständlichkeit, guter Aufbau und Lesefluss (Probelesen)
- Fast behördlich arbeiten!

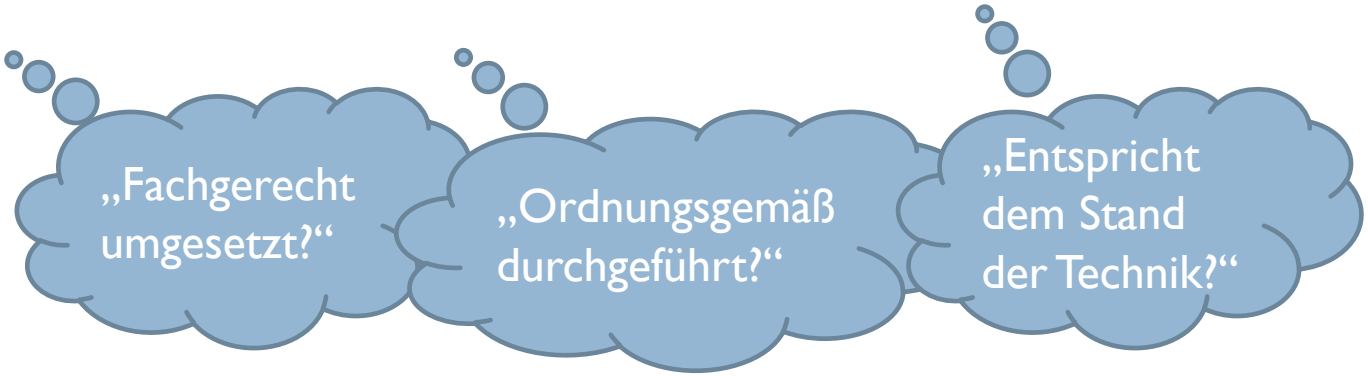
Gutachten
=
Expert
OPINION
?

WAS MACHT EIN BELASTBARES GUTACHTEN AUS?

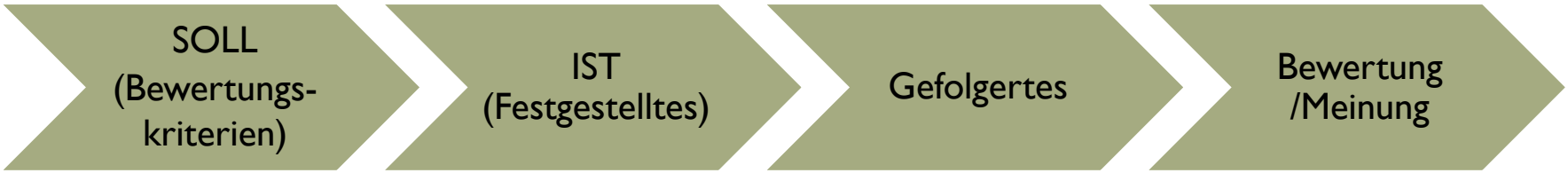
„Einhalten einer Reihenfolge vom Formalen über das Festgestellte zum Gefolgerten, dann zur Bewertung, zuletzt zur Meinung und Empfehlung“ (Volger & Wißner, 2000, S. 9)

Mal bildlich:

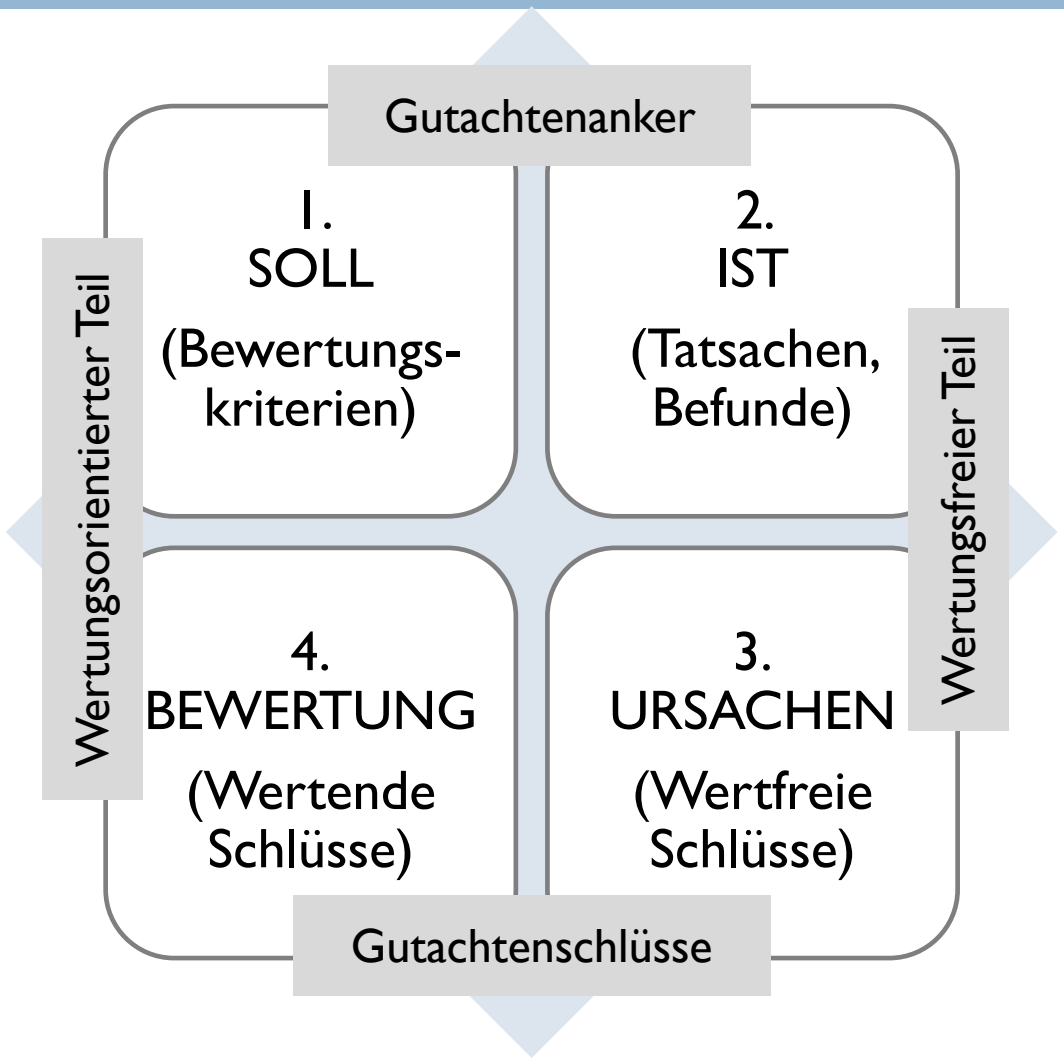
OFT: FRAGEN NACH DER BESCHAFFENHEIT



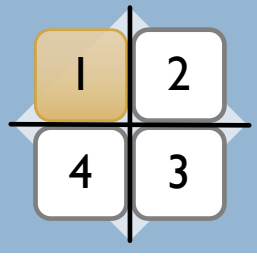
Aufbau des Gutachtens



KOMPONENTEN DES SACHVERSTÄNDIGENBEWEISES



1. SOLL (BEWERTUNGSKRITERIEN)



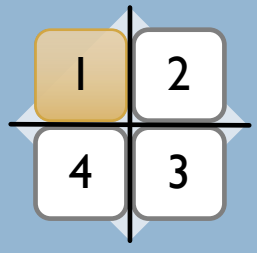
„Wurde die Sicherheit fachgerecht umgesetzt?“

Wonach richten?

- Vertragliche Anforderungen
- Normen (DIN, ISO)
- Erfahrung des Sachverständigen
- Meinung einer Gruppe von Experten
- Lehrmeinung und Best Practices

Problem: Oft nicht festgehalten!

1. SOLL (BEWERTUNGSKRITERIEN)



„Entspricht die Sicherheit dem
Stand der Technik?“

Was zum Teufel ist der Stand der Technik?

~~Vertragliche Anforderungen~~

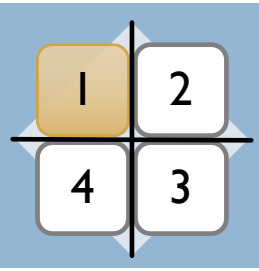
Normen (DIN, ISO)

Erfahrung des Sachverständigen

Meinung einer Gruppe von Experten

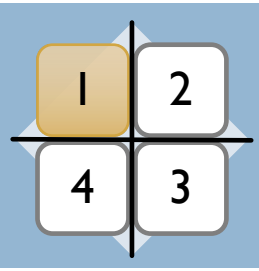
Lehrmeinung und Best Practices

1. SOLL (BEWERTUNGSKRITERIEN)



- **Standards und Normen**
  - IT-Sicherheit: ISO 2700x, IT-Grundschutz-Kataloge, ...
  - Vorteile: Sehr breite Akzeptanz
  - Nachteile: nicht immer aktuell (Prozess der Bildung von Normen dauert mehrere Jahre)
- **Herrschende Lehrmeinung und Best Practices**
  - Vor- und Nachteile ähnlich wie Standards und Normen
- **Standpunkt einer Gruppe von Experten**
  - Kann aktueller sein als das konsolidierte Wissen von Normen und Best Practices
  - Muss fundiert und sehr gut begründet werden, sonst angreifbar
  - Kann ggf. den Stand der Forschung darstellen
- **Erfahrung des Sachverständigen**
  - subjektiv und angreifbar (allerletzte Option!)

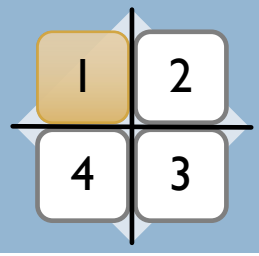
1. SOLL (BEWERTUNGSKRITERIEN)



Es gibt nicht nur den Stand der Technik....

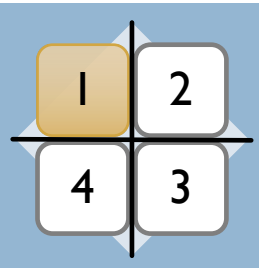
- Alle drei Stände ändern sich laufend
- Der Stand der Technik hinkt immer dem Stand der Wissenschaft hinterher
- Der Stand der Technik wird meist als Referenz genommen
- Es ist oft schwierig genug, den Stand der Technik überhaupt eindeutig zu bestimmen, und daraus prüfbare Bewertungskriterien abzuleiten

ALLGEMEIN ANERKANNTE REGELN DER TECHNIK



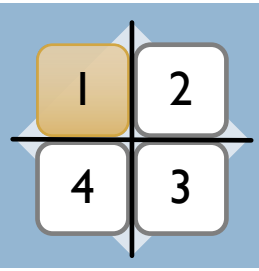
- „Der Begriff der **allgemein anerkannten Regeln der Technik** ist nicht in einer Rechtsvorschrift definiert, sondern durch die Rechtsprechung näher festgelegt worden. Nach nahezu allgemeiner Meinung ist der Begriff erfüllt, wenn eine technische Regel nach wissenschaftlicher Erkenntnis für *theoretisch richtig* gehalten wird und ***in der Praxis als bewährt*** angesehen wird, wobei Mindermeinungen außer Acht bleiben. Wissenschaftlich-theoretisch richtig ist eine Regel, wenn sie ausnahmslos wissenschaftlicher Erkenntnis entspricht und keinem wissenschaftlichen Meinungsstreit mehr unterliegt. In der Praxis bewährt hat sich eine technische Regel, wenn sie von den einschlägigen Fachkreisen durchweg anerkannt und angewandt wird.“ (Roeßner, 2008, S. 205)

STAND DER TECHNIK



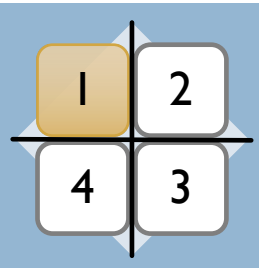
- „beinhaltet alle zu einem Zeitpunkt auf einem bestimmten Gebiet bekannten technischen Erkenntnisse. Er wird auch als ***das technisch Machbare*** bezeichnet. Er ***unterscheidet sich von den allgemein anerkannten Regeln der Technik, dass die Praxisbewährung nicht vorliegen muss***. Zur Erfüllung dieses Begriffs genügen auch mit der Praxis vergleichbare Versuche, wenn sie mit hinreichender Gewissheit Rückschlüsse auf die Verwendbarkeit und Eignung in der Praxis zulassen. Der rechtliche Maßstab für das Erlaubte oder Gebotene wird mit dieser technischen Anforderung **an die Front der technischen Entwicklung verlagert** (BVerfG NJW 1979, 359-Kalkar)“ (Roeßner, 2008, S. 206).
- Die „Verlagerung an die Front“ wird am klarsten, wenn man die Bedeutung des Begriffs im Patentrecht betrachtet: „Eine Erfindung gilt als neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst alle Kenntnisse, die vor dem für den Zeitrang der Anmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind“ (§ 3 Abs. 1 PatG).

STAND VON WISSENSCHAFT UND TECHNIK



- Eine allgemein gültige Definition des Begriffs liegt bisher nicht vor.
- „Literatur und Rechtsprechung stellen im Wesentlichen darauf ab, dass „Stand der Wissenschaft“ neue wissenschaftlich-theoretische Erkenntnisse meine, die **über die bereits realisierten technischen Möglichkeiten (=Stand der Technik) hinausreichen**, um eine Einhaltung eines höchstmöglichen Sicherheitsniveaus zu erreichen.“ (Roeßner, 2008, S. 207)

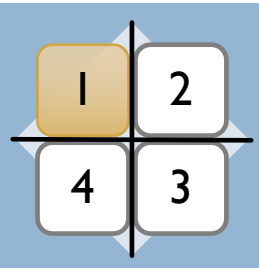
CASE UNSICHERE WEBSEITE



- B sollte für K eine Webseite bauen auf Grundlage eines Joomla-CMS.
- 3 Wochen nach Fertigstellung wurde die Webseite von einem Unbekannten gehackt und darüber tausende Spam-Emails versandt.
- Kläger K ist der Meinung, die Webseite sei nicht ausreichend gesichert gewesen.
- Beweisfragen: „Ist der Sicherheitsvorfall auf eine mangelhafte Leistung des Beklagten zurückzuführen? Wurde die Webseite nach dem Stand der Technik erstellt?“

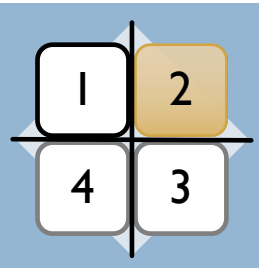
- Was ist passiert – Vermutungen vorab?
  - Zu einfaches (Standard-) Admin-Passwort gewählt
  - Sicherheitslücke in der Joomla-Version bei Standardpfad http://www.example.de/administrator

CASE – 1. SOLL



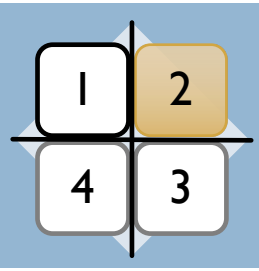
- Bewertungskriterien für die übliche Sicherheit einer Webseite?
- Welche Bewertungskriterien kann man heranziehen?
  - Normen? Best Practices? Sonstiges?
- Hierzu gibt es wohl kaum Normen oder Lehrmeinungen
  - Und nun?
- Best Practices unter Webdesignern suchen
- Angenommen, es besteht weitgehend Einigkeit bei drei Punkten
  - http://www.example.de/administrator muss umbenannt werden
  - http://www.example.de/administrator nur von fester IP anfragbar
  - http://www.example.de/administrator mit doppelter Passwortabfrage

2. IST (FESTSTELLUNGEN, TATSACHEN)



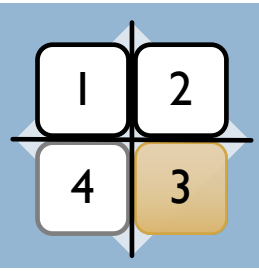
- Tatsachen setzen Wahrnehmbarkeit voraus
  - Per Untersuchung feststellbar
  - Nur in Stichproben (ökonomisch) nachprüfbar
  - Nicht (mehr) nachprüfbar
- Genaue Dokumentation ist oberwichtig
  - Fotos oder Videos machen, für jeden relevanten Schritt
  - Bei Referenzen genaue, nachprüfbare Quelle angeben
  - Lückenlos arbeiten

CASE – 2. IST



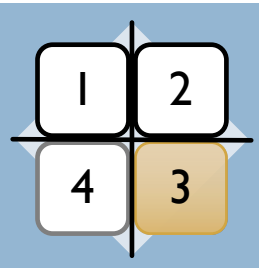
- Allgemeine Feststellungen
  - Welche Joomla-Version wurde genutzt? 5.43.21
  - Wurden zu dieser Joomla-Version Sicherheitslücken bekannt? Ja, eine Woche nach Fertigstellung der Webseite.
  - Wie lautete das Admin-Passwort? FZ0ghp$$
- Feststellung zu den Prüfpunkten
  - Wurde der Pfad für die Admin-Oberfläche geändert? Nein.
  - Gab es eine doppelte Passwortsicherung? Nein.
  - Wurden nur feste IPs zugelassen? Nein, weil keine feste IP vorhanden.

3. URSACHEN



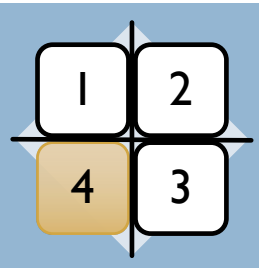
- „Der Begriff der Ursache ist nicht eindeutig, vielmehr werden ihm in verschiedenen Lebens-, Wissenschafts- und Rechtsbereichen unterschiedliche Begriffsinhalte beigemessen“ (Bayerlein, 2008, S. 470).
- Ursache = Schlussfolgerung aus mehreren Tatsachen
- Ursache kann nicht selbst sinnlich wahrgenommen werden, sondern nur durch Triangulation von Feststellungen erschlossen werden.
- Für die Ursachenanalyse sind mindestens zwei Feststellungen notwendig, z.B. eine erste Feststellung über die Lauffähigkeit eines Systems *mit* der zu untersuchenden Komponente und eine zweite Feststellung *ohne* sie.
- Genaues Austarieren der Aussage: „mit an Sicherheit grenzender Wahrscheinlichkeit“, „sehr wahrscheinlich“, „wahrscheinlich“, „unwahrscheinlich“ etc.

CASE – 3. URSACHEN



- Was war die Ursache für den Sicherheitsvorfall?
- „Mit hoher Wahrscheinlichkeit eine Sicherheitslücke in der Joomla-Version, die nur ausnutzbar ist, wenn der Standard-Admin-Pfad nicht geändert oder andersweitig geschützt wird.“

4. BEWERTUNG



- „Das Werturteil ist nach deutschem Verständnis eine subjektive Stellungnahme, eine positive oder negative Bewertung mit Bezug auf Tatsachen“ (Stegmann, 2004, S. 287)
- Bewertende Aussagen sind manchmal der **einzig gelesene Teil**
- haben im Vergleich zu den anderen Teilen die größten Konsequenzen
- Überaus **vorsichtige Formulierungen** wichtig!
- Wertungen erfolgen rein technisch, keinesfalls juristisch
- Auf Basis quantitativer und qualitativer Bewertungskriterien
- Die Bewertungskriterien müssen abschließend auf eine wertende Skala aufgetragen werden (quasi zwischen gut und schlecht).

CASE – 4. BEWERTUNGEN

- Beweisfrage 1: „Ist der Sicherheitsvorfall auf eine mangelhafte Leistung des Beklagten zurückzuführen?“
  - Ja, denn der Beklagte hätte als Fachkundiger eine zusätzliche Sicherung der Admin-Seite durchführen müssen.
- Beweisfrage 2: „Wurde die Webseite nach dem Stand der Technik erstellt?“
  - Nein, eine zusätzliche Sicherung der Admin-Seite hätte eingebaut werden müssen.

- Belastbares Gutachten? Angriffspunkte?

ANGRIFFSPUNKTE

- Von Beklagtenseite
  - „Die zusätzliche Sicherung ist nur in den Augen einiger Webdesigner vonnöten, aber längst nicht Bestandteil des Standes der Technik.“
  - „Zum Zeitpunkt der Fertigstellung und der Abnahme war die Sicherheitslücke nicht bekannt.“
- Entgegnung von Klägerseite
  - „Der Beklagte hätte auch kurz nach Fertigstellung eine Hinweispflicht auf etwaige Sicherheitslücken der verwendeten Version gehabt.“
  - etc.

FAZIT ZU BELASTBAREN GUTACHTEN

- SOLL: Die Bestimmung eines SOLL ist oft eine Herausforderung (Stand der Technik...)
- IST: Feststellungen sind eigentlich Handwerk. Leider kann oft aber nicht mehr alles festgestellt werden.
- URSACHEN: Ursachenforschung kann schwierig sein, wenn Feststellungen fehlen. Sie sind immer mit Wahrscheinlichkeiten behaftet.
- BEWERTUNG: Bewertungen können nicht stärker sein als das Fundament aus Soll, Ist und Ursachen.
- Für einen Beteiligten geht das Gutachten meist schlecht aus. Diese Partei wird nach Angriffspunkten suchen. Mit einem angreifbaren Gutachten lenkt der Sachverständige das Feuer auf... sich! Deswegen ist Belastbarkeit oberstes Gebot.

FAZIT ZUM STAND DER TECHNIK

- Der Stand der Technik ändert sich laufend, und somit auch der Stand der Technik bezüglich Sicherheit.
  - Bsp.: Mit neuer Art, Webseiten zu erstellen, entstehen auch neue Sicherheitsprobleme.
  - Zunächst schwammiger Begriff, nicht auslegungsfrei
  - Der Stand der Technik muss laufend neu konkretisiert werden (von wem?)

- Was heute noch sicher genug erscheint, ist morgen nicht mehr sicher.
  - Man kann sich nicht auf einem Sicherheitsstand ausruhen.
  - Oder nutzt noch jemand WEP-Verschlüsselung?
  - Oder ignoriert noch jemand Sicherheitsupdates für Betriebssystem und Apps?

DISKUSSION / FOOD FOR THOUGHT „STAND DER TECHNIK“ IN GESETZEN

Art. 32 DSGVO

Sicherheit der Verarbeitung

Das was Google kann?

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein: