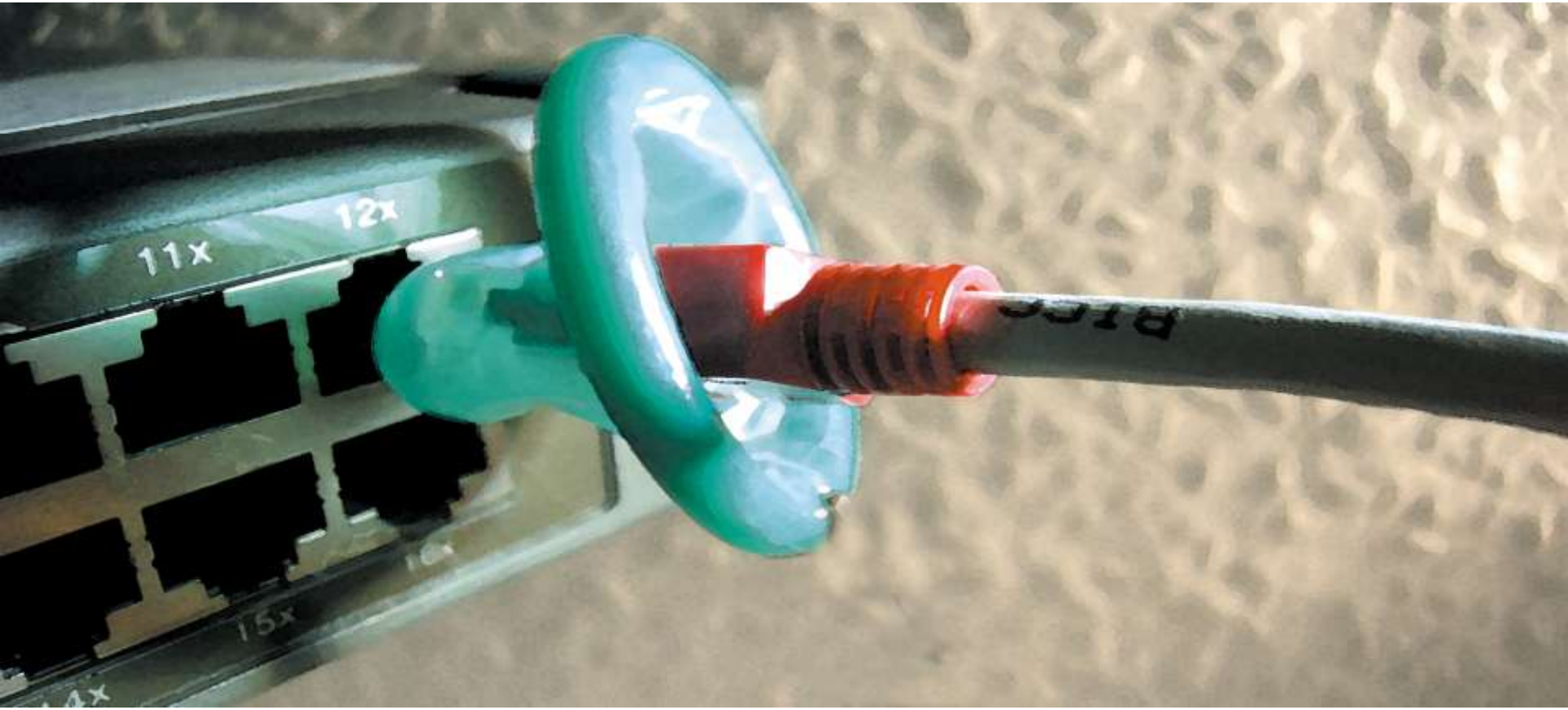
IT Systembetreuung Neitzel

Risiko-Management für IT-Unternehmen

Risiken erkennen, bewerten, vermeiden, vernichten und versichern

Frankfurt den 28.02.2013

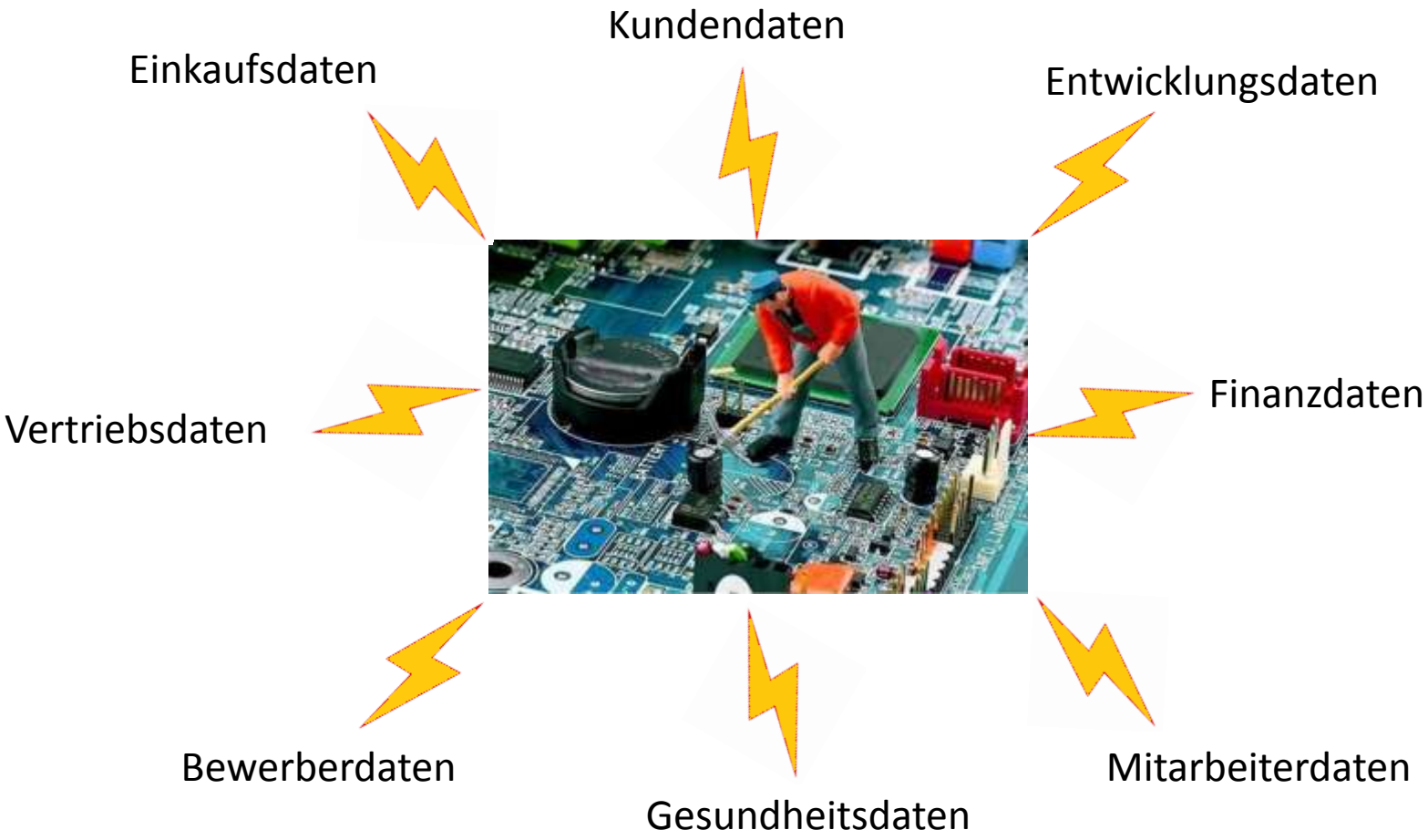
IT Systembetreuung Neitzel



Datenschutz schützt…

das Vertrauen in ihr Unternehmen

Schützenswerte Daten



*„Wenn wir nicht sicher wissen, was passieren wird, aber die **Eintrittswahrscheinlichkeit** kennen, ist das **RISIKO**.*
*Wenn wir aber noch nicht einmal die Wahrscheinlichkeit kennen, ist es **UNGEWISSHEIT**.“*

Definition Datenschutz

IT Systembetreuung Neitzel

Datenschutz schützt den **Einzelnen** davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem **Persönlichkeitsrecht** beeinträchtigt wird.

Datenschutz ist Schutz des Rechts auf informationelle Selbstbestimmung

Definition Datenschutz

IT Systembetreuung Neitzel

Schutz von natürlichen Personen

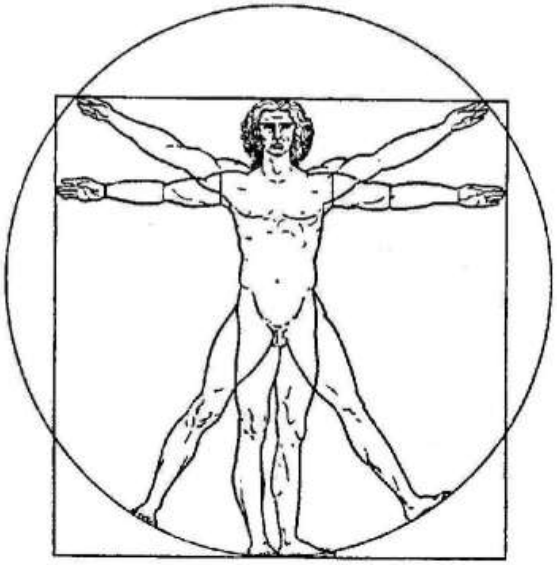
§4 Abs. 1 BDSG: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig,
soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet
oder der Betroffene eingewilligt hat.

Verbot mit Erlaubnisvorbehalt

Was sind Personenbezogene Daten?

Allgemeine Unterscheidung in 5 Schutzstufen

Schutzstufe A:
Frei zugängliche Daten, die keinen Schutz erfordern:



Mitgliederverzeichnisse

Adressbücher

Schutzstufe B:
Missbrauch dieser Daten lässt keine besondere Beeinträchtigung schutzwürdiger Belange erwarten.

Akademischer Grad

Berufsbezeichnung

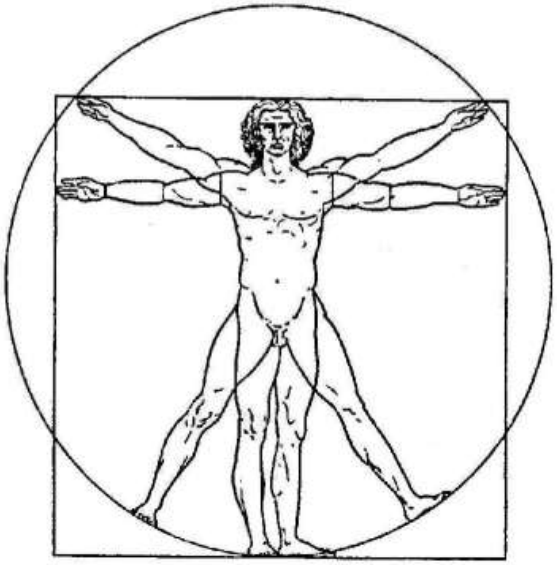
Telefonnummer

Was sind Personenbezogene Daten?

Allgemeine Unterscheidung in 5 Schutzstufen

Schutzstufe C:

Missbrauch kann Betroffenen in seiner gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen (ANSEHEN) beeinträchtigen



Familienstand

Schulzeugnisse

Staatsangehörigkeit

Ergebnisse von Beurteilungen

Einkommen

Ordnungswidrigkeiten (leicht)

Was sind Personenbezogene Daten?

Allgemeine Unterscheidung in 5 Schutzstufen

Schutzstufe D:

Missbrauch kann Betroffenen in seiner gesellschaftlichen Stellung oder wirtschaftlichen Verhältnissen erheblich (EXISTENZ) beeinträchtigen

Gesundheitliche Daten

Unterbringung in Anstalten

Straffälligkeiten

MPU

Schulden, Pfändungen

Konkurse, Eidesstattliche Vers.

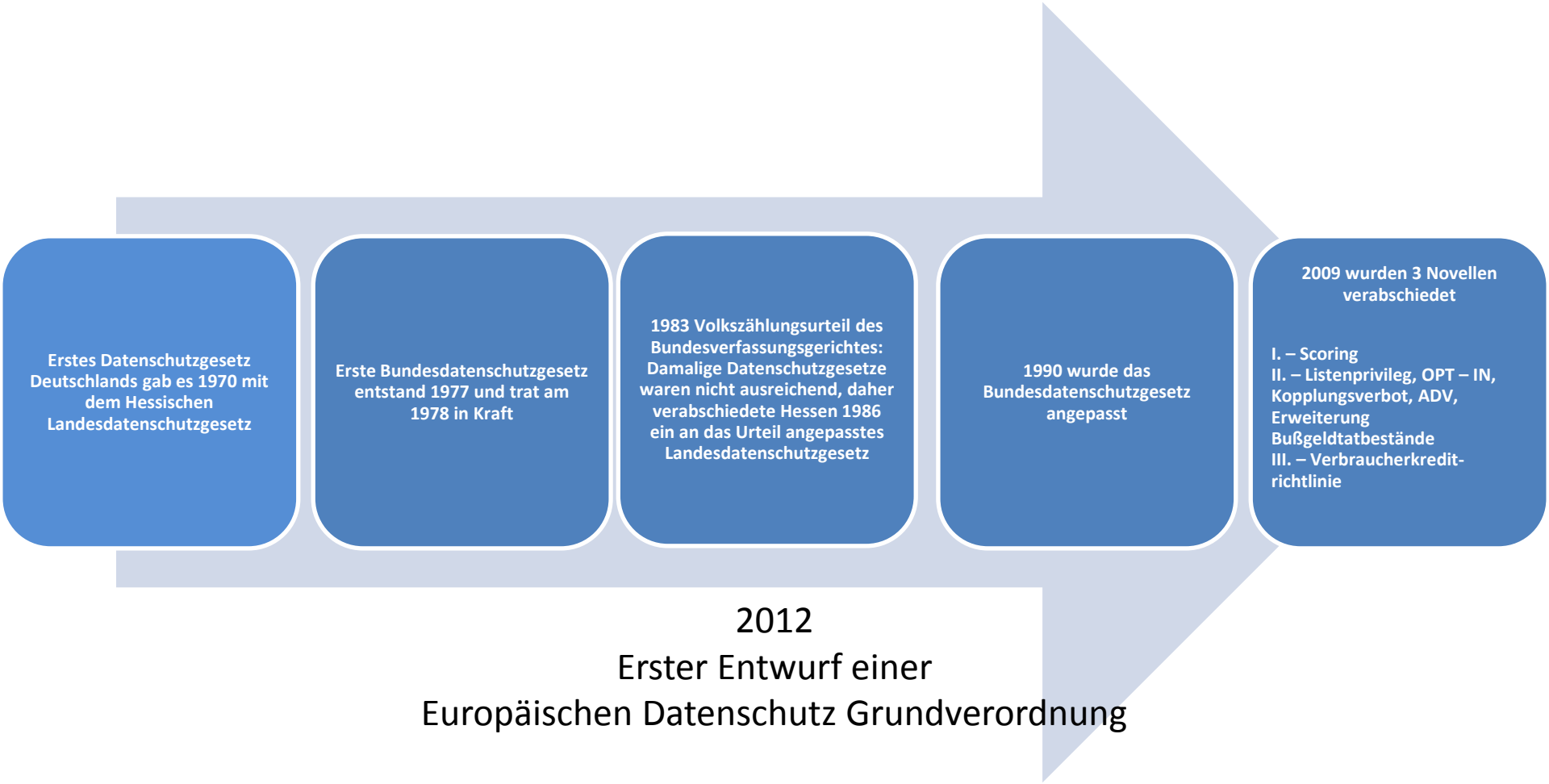
Was sind Personenbezogene Daten?

Allgemeine Unterscheidung in 5 Schutzstufen

Schutzstufe E:
Missbrauch kann für Betroffenen lebensbedrohlich sein, seine Gesundheit gefährden oder seine Freiheit beeinträchtigen

Zugehörigkeit zu Geheimdiensten
V-Leute
Mitglieder von Sonderkommandos
Zeugenschutzprogramm

Die Entwicklung des Datenschutzes



Gesetze, Vorschriften und Compliance im Datenschutz

BDSG Bundesdatenschutzgesetz

StGB Strafgesetzbuch

EG Datenschutzrichtlinie

LDSG Landesdatenschutzgesetze

BetrVG Betriebsverfassungsgesetz

TMG Telemediengesetz

§

BGB Bürgerliches Gesetzbuch

TKG Telekommunikationsgesetz

KDO - Anordnung über kirchlichen Datenschutz

UWG: Gesetz gegen unlauteren Wettbewerb

ISO 2700x, ISO 900x

PCI Vorschriften

BSI Empfehlungen

Folgen bei Verstößen gegen Datenschutzvorschriften

Geldbußen von bis EUR 50.000 z.B. für:

Fehlende, nicht rechtzeitige oder nicht ordnungsgemäße Bestellung eines DSB

Verstoß gegen eine Anordnung der Aufsichtsbehörde

Nicht erfolgte, unvollständige, verspätete oder falsche Auskunft gegenüber einem Betroffenen

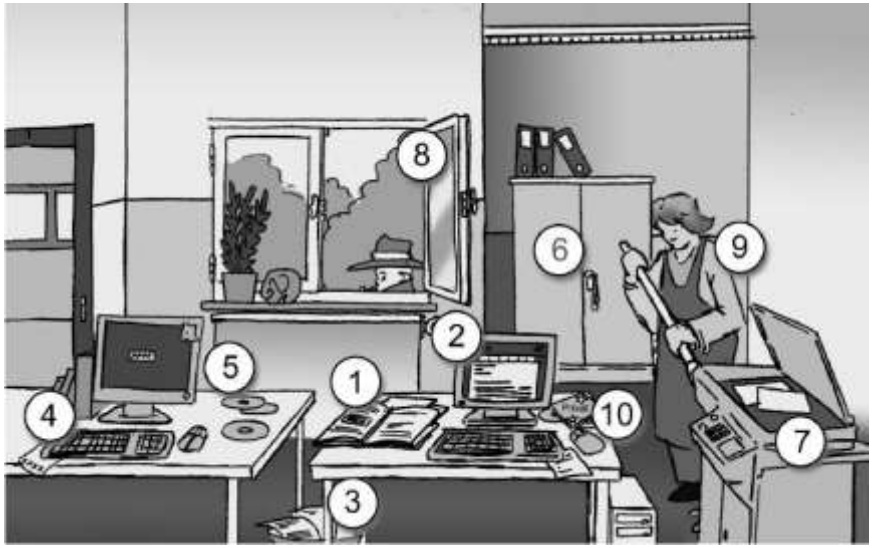
Pflichtverletzung bei der Auftragsdatenverarbeitung

Fehlende Widerrufs-belehrung bei einer werblichen Ansprache

Folgen bei Verstößen gegen Datenschutzvorschriften

Freiheitsentzug bis zu 2 Jahren oder Geldstrafe:
wenn **vorsätzlich** gegen **Bezahlung** oder mit **Gewinnabsicht** gegen das BDSG verstoßen wurde.

Top 10 Fehler im Datenschutz



1: Akten offen liegen lassen und sich vom Schreibtisch entfernen?

2: Den Zugriff auf den Computer bei Abwesenheit nicht sperren?

3: Ausdrucke mit sensiblen Daten in den Papiermüll?

4: Passwörter liegen unter oder neben der Tastatur ?

5: Sicherheitskopien auf CD/DVD liegen ohne Schutz auf dem Tisch?

6: Der Schlüssel zum Aktenschrank steckt und niemand ist im Büro?

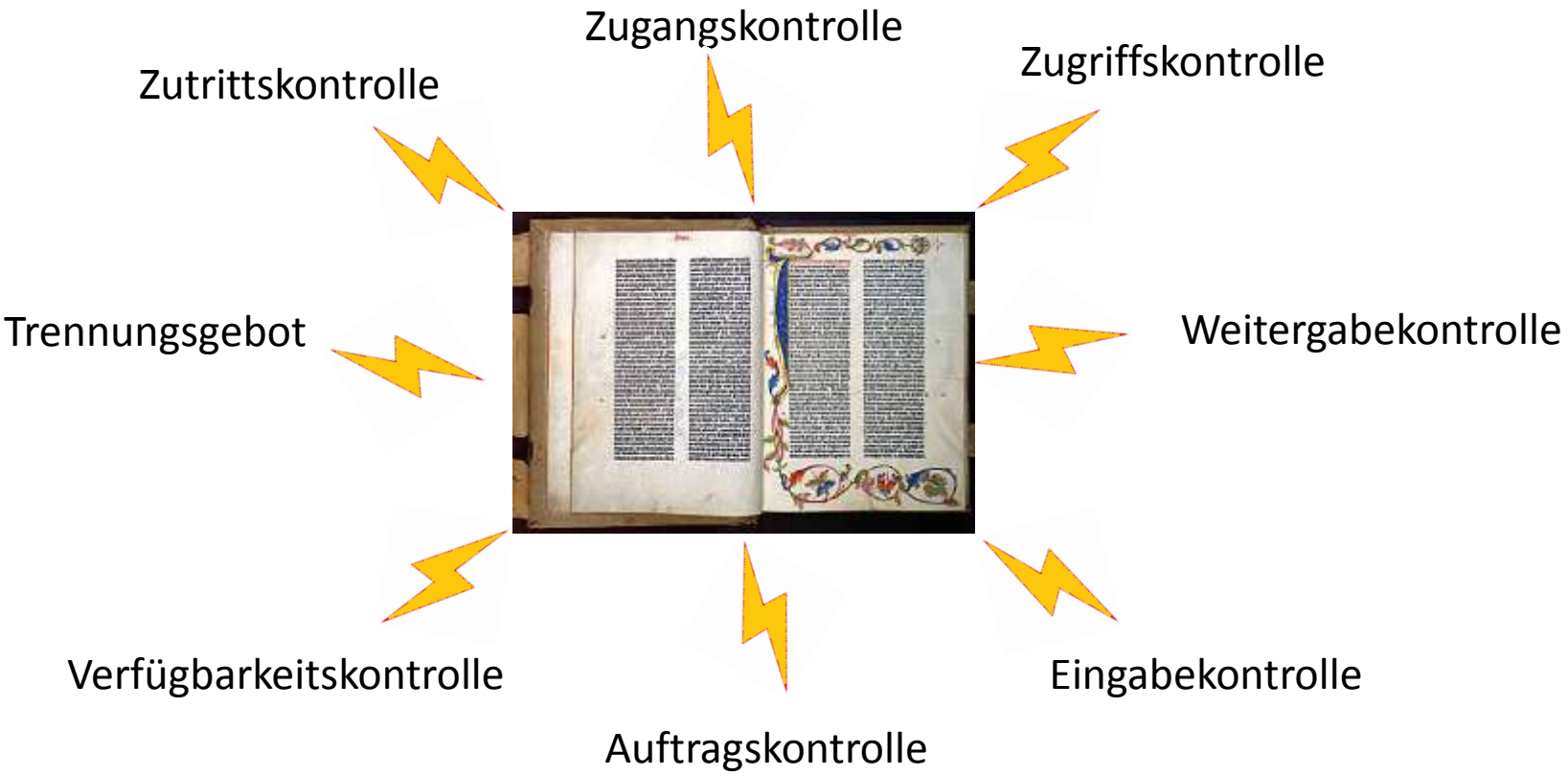
7: Kopien (Originale) bleiben auf dem Kopierer oder Scanner?

8: Ein Fenster im EG steht trotz Abwesenheit offen?

9: Die Reinigungskraft hat ohne Aufsicht Zutritt in sensible Bereiche?

10: Private Datenträger werden im Unternehmen verwendet, sie könnten Schadsoftware enthalten

Die 8 Gebote
oder Werkzeuge des Datenschutzes



Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Zutrittskontrolle	Es muss sichergestellt sein, dass nur berechtigte Personen Zutritt zu dem Gebäude haben. Besucher dürfen nicht unbeaufsichtigt bleiben	Nicht gewollter Zugang zu den Räumlichkeiten, Gefahr von Manipulation, Diebstahl, Spionage	• Verschlossene Außentüren • Schlüsselregelung • Alarmanlage • Separate Zutrittssicherung bei sensiblen Bereichen (Serverräume, Datenschränke)

Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Zugangskontrolle	Nur tatsächlich berechtigte Personen dürfen Zugang zu der Infrastruktur bekommen.	Unberechtigtes Anmelden an PCs kann zu Datenverlust, Spionage, Manipulation uvm führen.	• Anmeldung an PCs mit Benutzer-kennung und Passwort • Regelmäßiger Wechsel des Passwortes • Groß- und Klein-buchstaben, Zahlen und Sonderzeichen • Mind. 8 Zeichen • Kennworthistorie • Ausschluss von Trivialpasswörtern • Sperren des PCs bei Abwesenheit

Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Zugriffkontrolle	Es sollten immer nur so wenige Zugriffsrechte wie möglich, aber so viele wie nötig existieren	Unberechtigter Zugriff auf Daten; unnötige Rechte;	Implementierung verschiedener Nutzerrechte-Ebenen.

Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Weitergabekontrolle	Daten dürfen während der Übertragung oder des Transportes nicht von Unbefugten gelesen, kopiert, verändert oder gelöscht werden	Daten können in falsche Hände gelangen oder abhanden kommen	• Verschlüsselung, VPN • Fax – Protokoll • Verschlossene Behälter • Überbringung durch Boten • Regelungen zur Nutzung von Internet und E-Mail • Verfahren zur Aktenvernichtung und Datenträger-entsorgung • Festlegung sicherer Versandverfahren für vertrauliche Post

Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Eingabekontrolle	Jederzeit muss nachvollziehbar sein, wer welche Daten eingegeben, verändert oder gelöscht hat	Datenmanipulation Datenverlust Datendiebstahl	Protokollierung Benutzeridentifikation

Die 8 Gebote

Herausforderung	Beschreibung	Risiko	Lösung
Auftragskontrolle	Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur gemäß den Weisungen des Auftraggebers verarbeitet werden	Vermeidung von unbefugtem Zugriff auf Ihre Daten bei Auftragnehmern.	• Vertrag zur Auftragsdaten-verarbeitung gemäß §11 BDSG • Vor-Ort-Kontrollen des Auftrag-nehmers • Stichproben-prüfung • Zertifikate oder Ergebnisse eines Datenschutzaudits vorlegen lassen • Weisungsbefug-nisse festlegen

Die 8 Gebote

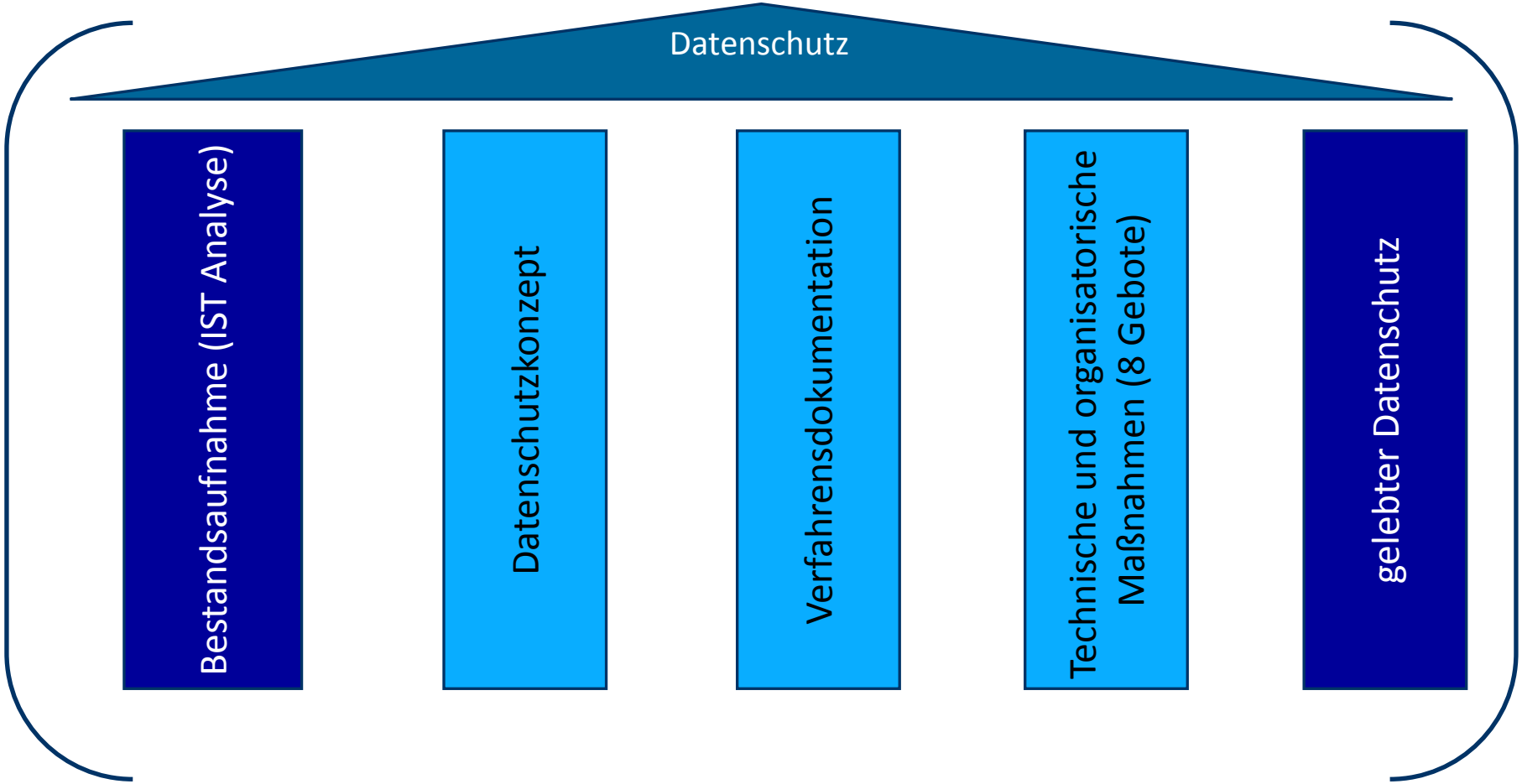
Herausforderung	Beschreibung	Risko	Lösung
Verfügbarkeits-kontrolle	Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden	(personenbezogene) Daten können permanent verloren gehen oder in falsche Hände gelangen Dadurch hoher Imageverlust möglich	• Brandschutzmaß-nahmen • Einbruch- und Diebstahlschutz • Schutz vor äußeren Risiken • Backupkonzept inkl. regelmäßiger Prüfung • Geübtes Restore der Daten-sicherung • Virenschutzkon-zept, Firewall • Notfallkonzept

Die 8 Gebote

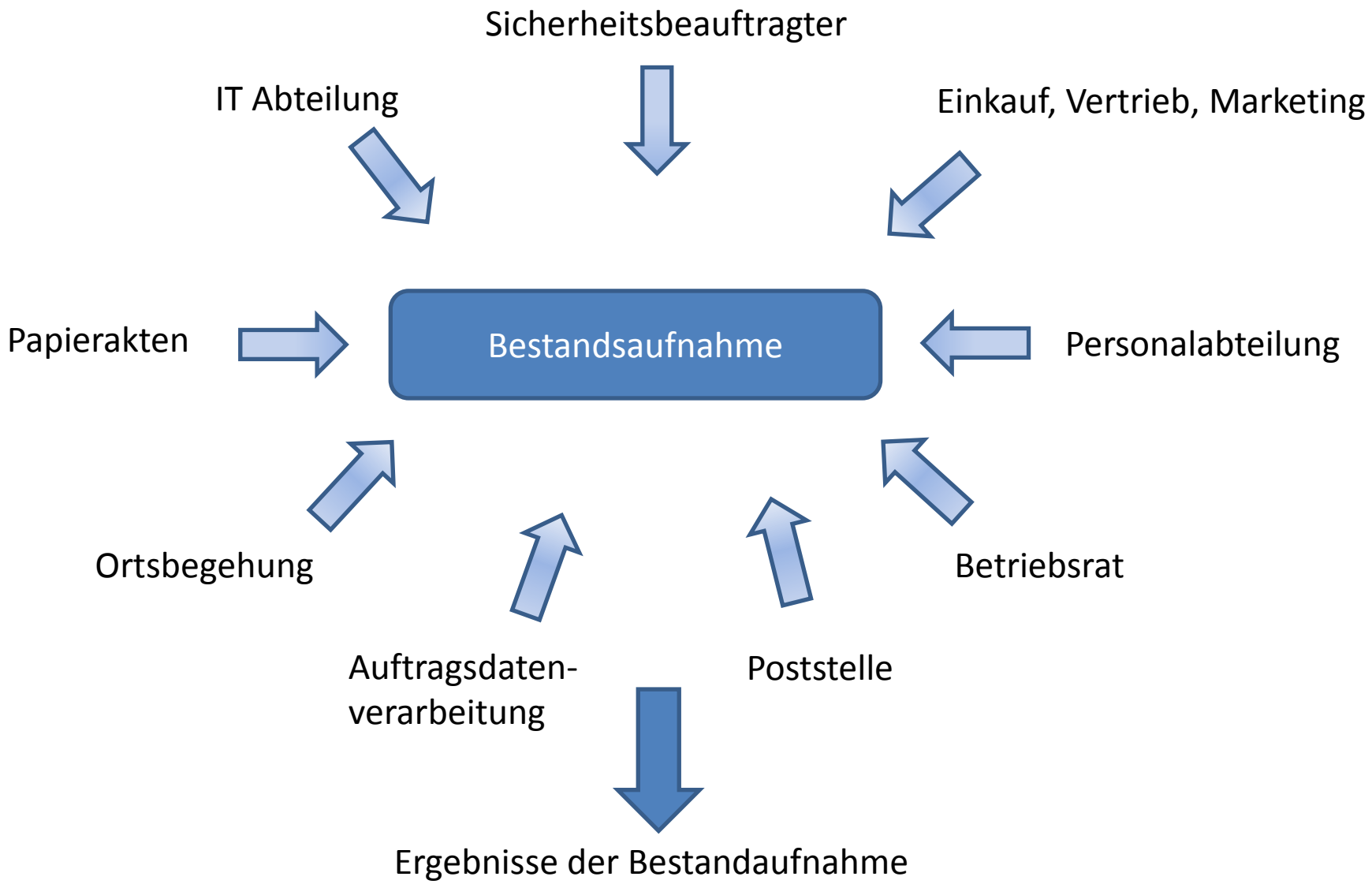
Herausforderung	Beschreibung	Risko	Lösung
Trennungsgebot	Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können z.B. Produktiv –Daten von Testdaten trennen Daten für Gebührenberechnung nicht als Adressdaten verkaufen	Verarbeitung von personenbezogenen Daten ohne Erlaubnis	• Trennung Produktiv- und Testdaten • Logische / physikalische Trennung der Datenbestände / Datenbanken • Getrennte Anwendungen

Betriebliche Datenschutz - Einführung

IT Systembetreuung Neitzel



Bestandsaufnahme (IST – Analyse)



Datenschutzkonzept

IT Systembetreuung Neitzel

Ermittlung des Schutzbedarfs

Pflichtenheft / Maßnahmenkatalog

Einholung von Angeboten

Priorisierung

Verfahrensdokumentation

Verfahrensverzeichnis

Öffentliches Verfahrensverzeichnis

Datenschutzerklärung

Dokumentation muss auf dem aktuellen Stand sein. Ein Bereich bei Prüfungen durch Aufsichts-behörde

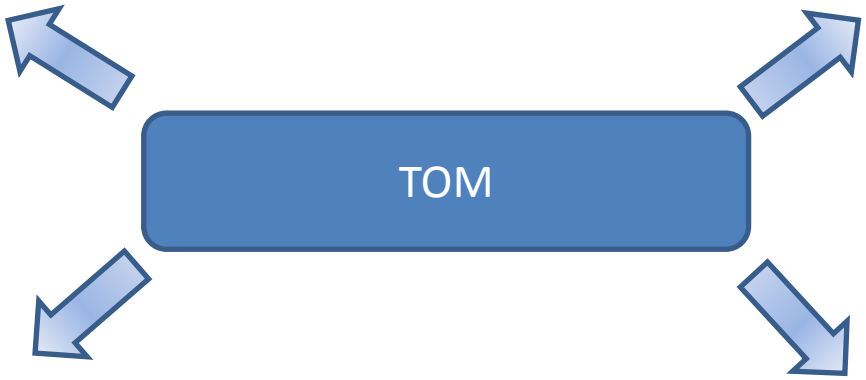
Auflistung aller Verfahren, mit denen personenbezogene Daten verarbeitet werden. (internes Verfahrensverzeichnis)

Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOM)

8 Gebote

Grundlage für Auftragsdatenverarbeitung



Kernbereich bei Prüfungen durch Aufsichtsbehörden

Müssen auch bei Auftragnehmer überprüft werden

Gelebter Datenschutz

Gelebter Datenschutz

Prozess für ausscheidende MA

Schulungen der Mitarbeiter (Neueinstellungen)

DSB diskret kontaktieren

Aktualisierung der Dokumentation

Gelebter Datenschutz

Information des DSB über geplante neue Verfahren (

Bearbeitung von Auskunftsersuchen

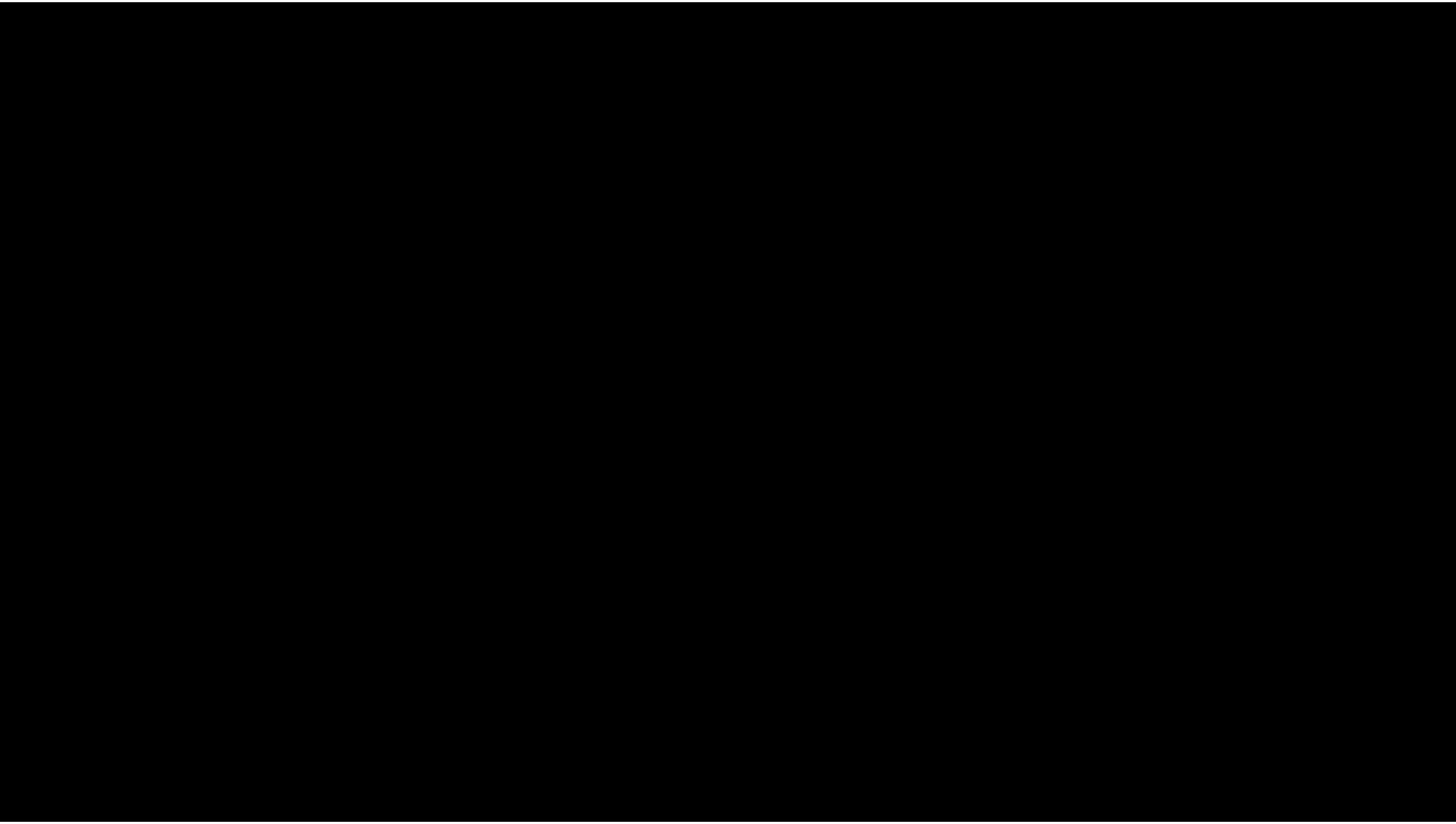
Aktualisierung des Sicherheitskonzeptes

Umsetzung von Gesetzesänderungen

Leben ohne Datenschutz

IT Systembetreuung Neitzel

Leben ohne Datenschutz



IT Systembetreuung Neitzel

"Datenschutz ist unerlässliche Voraussetzung für eine demokratisch verantwortbare Informationsgesellschaft."

Hartmut Lubomierski, Landesdatenschutzbeauftragter Hamburg auf einer Presseerklärung zum 1. Europäischen Datenschutztag am 28. Januar 2007

Ich bedanke mich für Ihre Aufmerksamkeit

Robert Neitzel

info@edvsachverstaendiger.info
http://www.edvsachverstaendiger.info