Die neue EU-DSGVO – was kommt auf uns zu?

Gotha, 09.05.2018

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Dipl.-Ing.(Univ.) Dipl.-Ing.(FH) Matthias Dick
Dozent der Fakultät Wirtschaftsrecht HS Schmalkalden
nebenamtl. Dozent der TVS Weimar
Datenschutzbeauftragter

Dies ist keine öffentliche Veranstaltung!

Inhaltlich wurde sich auf subjektiv ausgewählte Schwerpunkte orientiert, welche nicht den Anspruch auf Vollständigkeit erheben.

Rechtsstand: 01.03.2018

Text in einem blauen Feld ist immer original EU-DSGVO

Inhalt:

- Allgemeine Grundlagen – Vorbetrachtungen
- Die neue EU-DSGVO
- Datenerhebung
- Auftragsdatenverarbeitung
- Technisch-organisatorische Maßnahmen und Dokumentationspflichten
- Der Datenschutzbeauftragte
- Folgen bei Nichtbeachtung/Verstößen
- Besondere Baustellen
- Fazit

allgemeine Grundlagen - Vorbetrachtungen

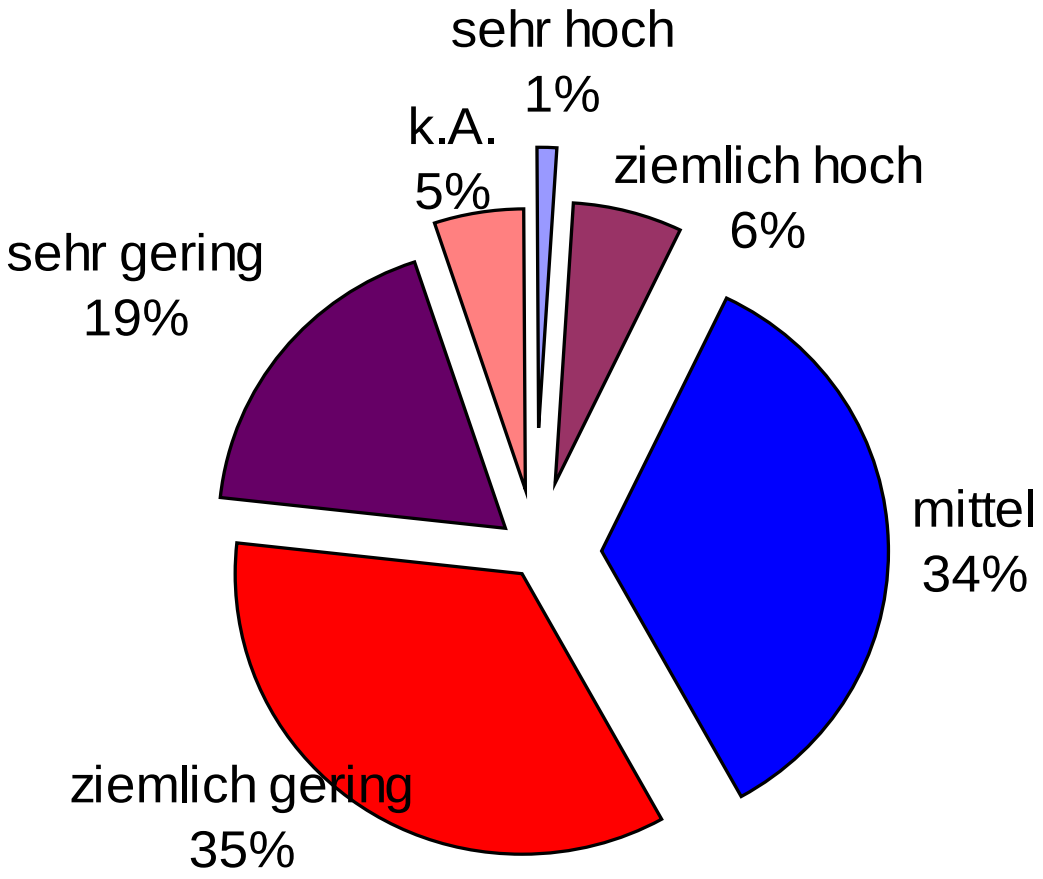
Eigene Fragestellung:

Habe ich Informationen, die für Dritte interessant sind?

Wann bemerke ich spätestens, dass Daten manipuliert sind?

Wie lange kann ich ohne IT meine Abläufe aufrecht erhalten?

Einschätzung zum derzeitigen Sicherheitsrisiko



Quelle: InformationWeek 15/16

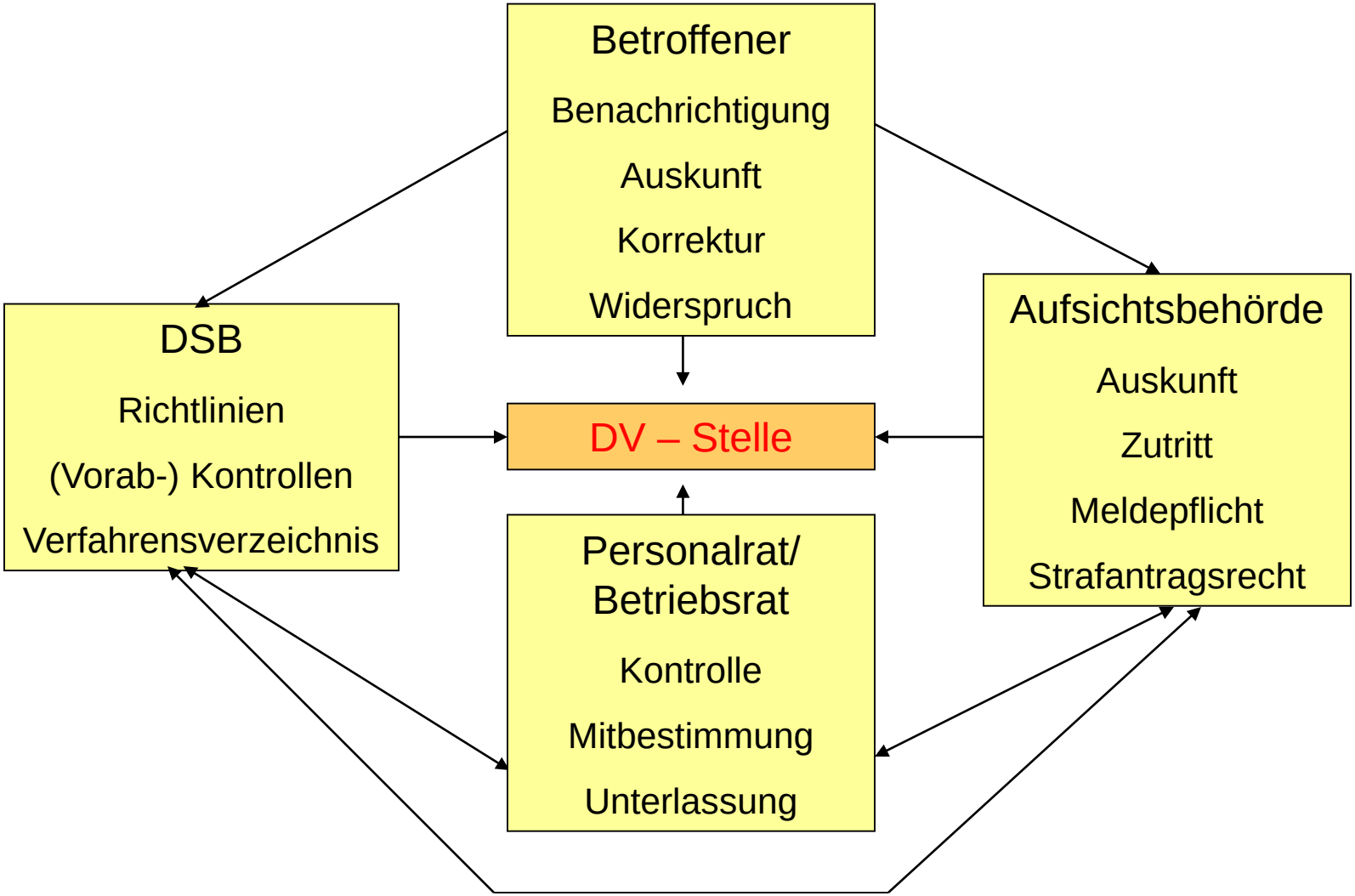
Kombination von Datenschutz und Datensicherheit in der heutigen Informationsgesellschaft

Datenschutz: Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts durch unberechtigtem Umgang mit personenbezogenen Daten.

Datensicherheit: Technisch organisatorische Maßnahmen zum Schutz von personenbezogenen und behörden-/ firmen-relevanten Daten vor Zugriff unberechtigter Dritter.

! Qualitätsmerkmal !

Das Datenschutz - Kontrollsystem



Die neue EU-DSGVO

Inkrafttreten/Gültigkeit

- Die neue DSGVO ersetzt die Datenschutzrichtlinie 95/46/EG von 1995.
- Die DSGVO ist am 25.05.2016 in Kraft getreten. Sie enthält aber auch Öffnungsklauseln, welche den Mitgliedsstaaten Spielraum geben, eigene Regelungen zu treffen.
- Sie ist ab dem 25.05.2018 gültig und ab diesem Zeitpunkt unmittelbar anwendbares Recht.

Art. 99 Inkrafttreten und Anwendung

1. Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

2. Sie gilt ab dem 25. Mai 2018.

Systematik

- Die DSGVO besteht aus 99 Artikeln (Art.) und 173 Erwägungsgründen (ErwG).

- Sie wurde fast komplett technikneutral formuliert, um so auch zukünftig für Neuerungen anwendbar zu sein.

- Die ErwG sind als Erläuterungen für die einzelnen Artikel zu sehen.

Es wird nicht mehr zwischen öffentlichen und nicht-öffentlichen Stellen unterschieden!

- Sachlicher Anwendungsbereich:

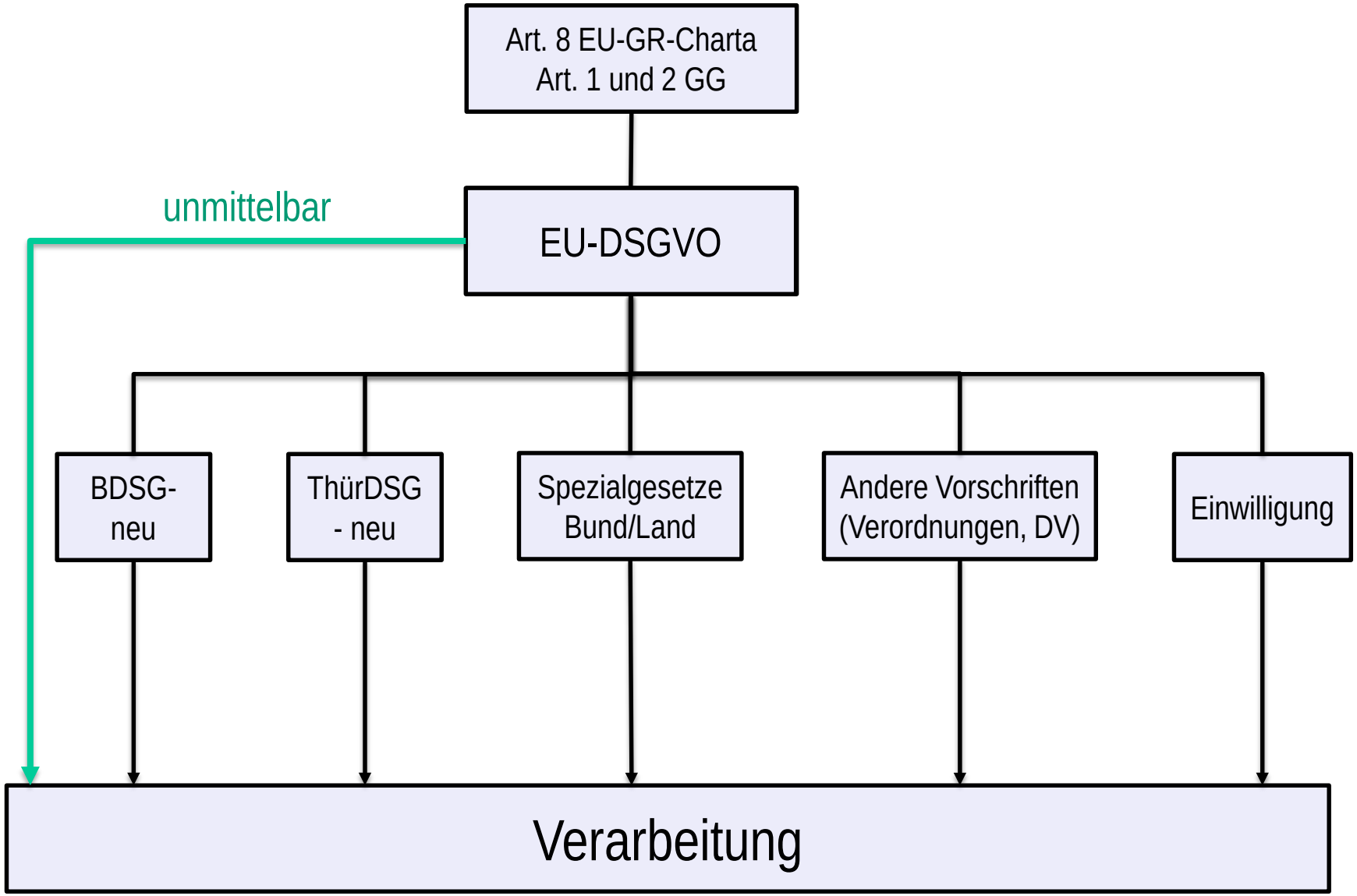
  Nach Art. 2 (1) findet die Verordnung Anwendung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

  Erfasst wird davon also auch die mündliche Befragung, vorausgesetzt das Ergebnis wird zumindest dateimäßig notiert Art. 4 Nr. 6.

- Räumlicher Anwendungsbereich:

  Nacht Art. 3 (1) und Art. 3 (2) das gesamte Gebiet der Europäischen Union.

Das neue System des Datenschutzes



Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

§ 3 (1) BDSG
§ 3 (1) ThürDSG

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

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

Bisher galt in Deutschland der Grundsatz: *„Verbot mit Erlaubnisvorbehalt“*

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

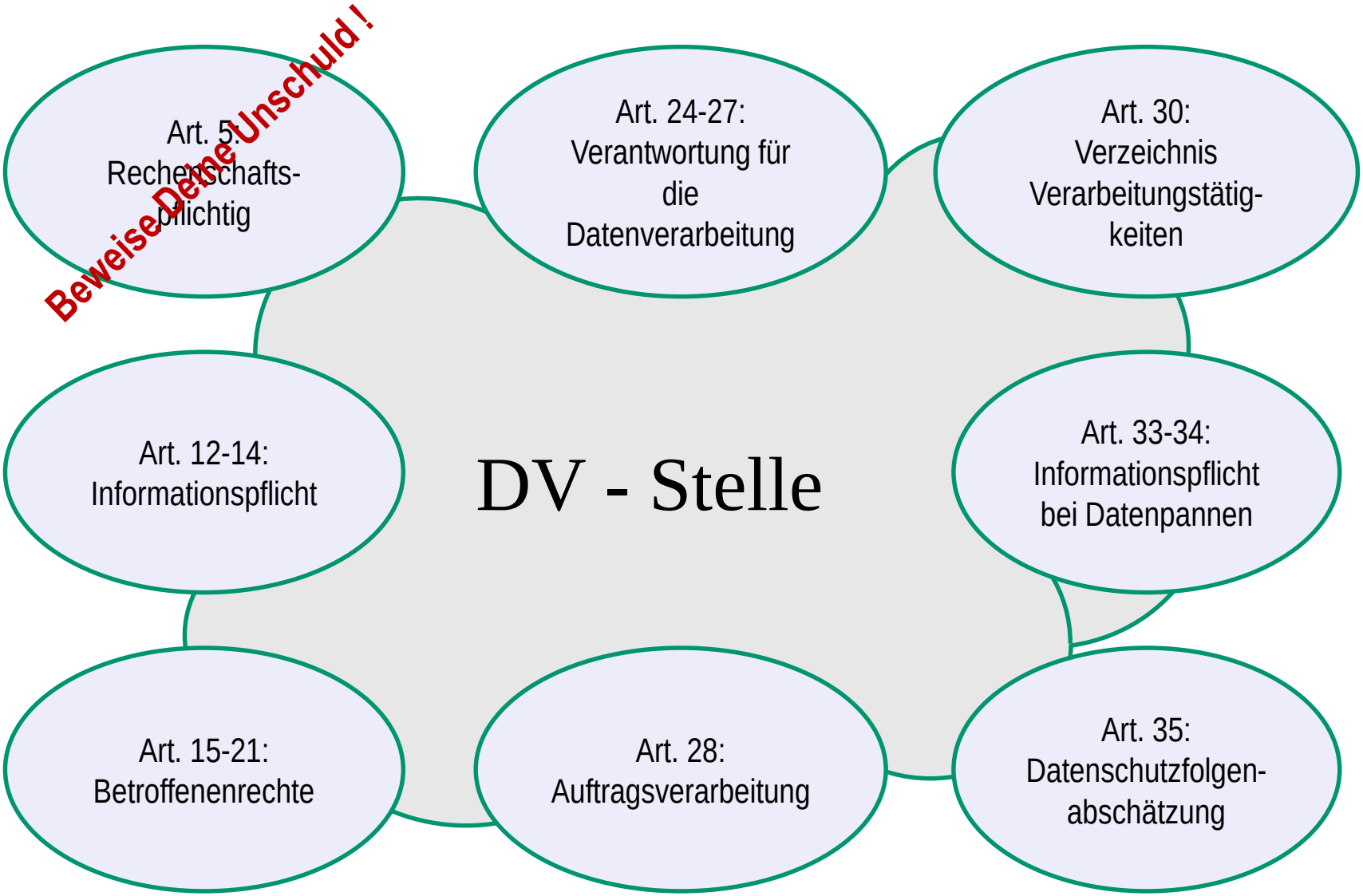
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Abs. 1 verarbeitet werden ("Speicherbegrenzung");

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Wer ist eigentlich Verantwortlich?

Art. 4 Nr. 7: "Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;


Beweise Deine Unschuld !
Art. 5:
Rechenschafts-
pflichtig
Art. 24-27:
Verantwortung für
die
Datenverarbeitung
Art. 30:
Verzeichnis
Verarbeitungstätig-
keiten
Art. 12-14:
Informationspflicht
DV - Stelle
Art. 33-34:
Informationspflicht
bei Datenpannen
Art. 15-21:
Betroffenenrechte
Art. 28:
Auftragsverarbeitung
Art. 35:
Datenschutzfolgen-
abschätzung

Datenerhebung

Vorrang der Direkterhebung?

§ 19 ThürDSG bzw. § 4 BDSG: Datenerhebung
(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.
(2) Personenbezogene Daten sind beim Betroffenen zu erheben.

Art. 6: Rechtmäßigkeit der Verarbeitung
(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

Einwilligung ? (vgl auch ErwG: 32; 40; 42; 43)

Art. 6 Rechtmäßigkeit der Verarbeitung
(1)
Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
a)
Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

Art. 4 Nr. 11:
"Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Art. 7: Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1)
Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a)
den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b)
die Kontaktdaten des Datenschutzbeauftragten;
c)
die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

(2) Zusätzlich zu den Informationen gemäß Abs. 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a)

die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b)

das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

[…]

d)

das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

→ Eventuell könnte ErwG 58 helfen, welcher die Bereitstellung von Informationen auch über die Website ermöglicht.

Auftragsdatenverarbeitung

§ 8 ThürDSG: Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

§ 11 BDSG: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Art. 4 Nr. 8:
"Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Art. 28 Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

technisch-organisatorische Maßnahmen und Dokumentationspflichten

§ 9 ThürDSG/ § 9 BDSG Technische und organisatorische Maßnahmen

(1) Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (ErwG 78)

(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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

2)
Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Dokumentationspflichten nach der DSGVO

- Basis ist Art. 5 (2) DSGVO – Rechenschaftspflicht – Beweise Deine Unschuld!

  - ♦ Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
  - ♦ Datenschutzfolgeabschätzung (Art. 35 DSGVO)

- Verantwortliche und Auftragsverarbeiter müssen jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Verarbeitungen nachzuweisen.

- Verstöße sind bußgeldbewährt – auch für Kommunen!

Verzeichnis der Verarbeitungstätigkeiten

Es sind also nicht IT-Verfahren, sondern die Verarbeitungstätigkeiten aufzunehmen.

Bisher war es das Verfahrensverzeichnis nach § 10 ThürDSG bzw. § 4 d BDSG.

Art. 30 Verzeichnis von Verarbeitungstätigkeiten

(1)
Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben: […]

(2)
Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält: […]

Verpflichtet sind (eigentlich) die Verantwortliche und der Auftragsverarbeiter, nicht der DSB → aber wo funktioniert das ☹!

(3)
Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
(4)
Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Das Verzeichnis muss insbesondere enthalten:

- ♦ Verantwortliche Stelle
- ♦ Kontaktdaten des DSB
- ♦ den Zweck der Verarbeitung
- ♦ die Kategorien der personenbezogenen Daten
- ♦ die betroffenen Personen und Empfänger
- ♦ Löschungsfristen der jeweiligen Datenkategorien
- ♦ Beschreibung der technisch-organisatorischen Maßnahmen

Datenschutzfolgeabschätzung (ErwG 84, 89 bis 93)

Sie ist vergleichbar mit der Vorabkontrolle, aber weitreichender!

Art. 35 Datenschutz-Folgenabschätzung
(1)
Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2)
Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3)
Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
a)
systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b)
umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c)
systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Der Datenschutzbeauftragte ☺

§ 38

Datenschutzbeauftragte nicht-öffentlicher Stellen

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Neh-

Folgen bei Nichtbeachtung/Verstößen

Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen (ErwG 148; 150; 151)

(1)

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(4)

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: […]

(5)

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist: […]

besondere Baustellen ????

entfallene bzw. nicht mehr klar geregelte Vorschriften

- Beschäftigtendatenschutz (§ 33 ThürDSG; § 32 BDSG)

- Videoüberwachung (§ 25 a ThürDSG; § 6 b BDSG)

Neu

→ § 26 BDSG-neu	Beschäftigtendatenschutz
→ § 4 BDSG-neu	Videoüberwachung