SH Schleswig-Holstein
Der echte Norden

IT-Planungsrat
Digitale Zukunft gestalten

7. Fachkongress des IT-Planungsrats am 12./13. März 2019 in Lübeck


# Art. 35 DSGVO - Durchführung einer Schwellwert-Analyse (Workshop)

**Martin Rost, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

# Agenda

## 1. Komponenten einer Schwellwert-Analyse für eine Verarbeitung

Verankerung der Schwellwert-Analyse in Art. 35 DSGVO

a) „Verarbeitung“
b) Risiko, Schutzbedarf, Schutzniveau, Restrisiko
c) Kriterien für die Risiko-Schwellwert-Analyse

## 2. Übung

Durchführen einer Schwellwert-Analyse an einem Usecase

## 3. Hinweise zur Umsetzung in der Praxis

a) Privacy-Forum: Ablaufprozess für Datenschutz-Folgenabschätzung (DSFA)
b) DSK: „Simple Datenprotection Modelling“ (SDM)
c) UAGSDM: Baustein „Datenschutz-Managementsystem“ (DSMS)
d) ZIT-SH (IT-Planung Land), behördliche DSB Kr. Stormarn/Kiel (Kommune):
Formulare und Excel-Tool für Schwellwert-Analyse und Durchführung einer DSFA

## 4. Referenzen / Kontakt

# Warum muss eine Schwellwertanalyse erfolgen?

Eine Datenschutz-Folgenabschätzung (DSFA) bzw. ein Data-Protection-Impact-Assessment (DPIA) ist gemäß Artikel 35 DSGVO für **Verarbeitungstätigkeiten mit hohem Risiko** für die Freiheiten und Rechte natürlicher Personen durchzuführen.

- Eine **Schwellwert-Analyse** stellt die Höhe des Risikos fest
  → **Ausgangsfrage: Liegt ein „normales Risiko“ oder „hohes Risiko“ für eine Verarbeitungstätigkeit vor?**
- DSGVO: Bei Scoring, Profiling, automatisiertem Einzelentscheid, Einsatz neuer (Überwachungs-) Techniken, Videoüberwachung des öffentlichen Raumes sowie bei besonders schutzwürdigen Daten (Art. 9 DSGVO) besteht **grundsätzlich ein hohes Risiko** → Schwellwert-Analyse ist trivial.
- Hinweis: Der/die **Datenschutzbeauftragte** ist für Durchführung der DSFA/Schwellwertanalyse nicht verantwortlich, es ist auch keine abschließende Beurteilung abgefordert.
  → **Projektmanager*in** muss DSFA durchführen.
- Der/die **Verantwortliche** muss nach Abschluss der DSFA die Wirksamkeit der Maßnahmen nachweisen können.

# Fragen

- Was ist eine **Verarbeitung**?

- Was ist ein Datenschutz-Risiko?
- Wie führt man eine **Schwellwert-Analyse** durch?

# „Verarbeitung“ (Art. 4, Abs. 2 DSGVO)

“Im Sinne dieser Verordnung bezeichnet der Ausdruck „*Verarbeitung*“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder die Vernichtung; (….)”

# Artikel 30

## Verzeichnis der Verarbeitungstätigkeiten

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

*a) den Namen und die **Kontaktdaten des Verantwortlichen** und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;*

*b) die **Zwecke der Verarbeitung**;*

*c) eine Beschreibung der **Kategorien betroffener Personen und der Kategorien personenbezogener Daten**;*

*d) die **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;“*

*„e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein **Drittland** oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;*

*f) wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien;*

*g) **wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.**“*

Wichtig:
Art. 30 ist **nur eine Inventarisierung**, aber noch keine hinreichende Dokumentation.

Zu den zu **dokumentierenden Komponenten** einer automatisierten Verarbeitungstätigkeit zählen:

- **Daten**
- **IT-Systeme (HW/SW)**
- **Prozesse**

# Fragen

- Was ist eine **Verarbeitung**?
- Was ist ein **Datenschutz-Risiko**?
- Wie führt man eine **Schwellwert-Analyse** durch?

# Datenschutz-Risiko

- **Risikotyp 1: „Grundrechtseingriff ist nicht hinreichend milde gestaltet“**
  Die Verarbeitung einer Organisation ist nicht hinreichend zweckgesteuert, die grundrechtliche Anforderungen zugunsten von betroffenen Personen werden nicht wirksam umgesetzt.
- **Risikotyp 2: „Schutzmaßnahmen des Datenschutzes versagen“**
  Datenverarbeitung geschieht bspw. ohne Zweckbindung, die Protokollierung ist lückenhaft, das Löschen ungesichert, die Anonymisierung und das Datenschutz-Controlling bzw. Management unzureichend.
- **Risikotyp 3: „Schutzmaßnahmen der Informationssicherheit versagen“**
  Unbefugte können auf personenbezogene Daten zugreifen.

# *Risikomodellierung im Datenschutz*

Die Risiken des **Datenschutzes** sind vordringlich solche, die durch die Verarbeitungstätigkeiten einer Organisation *für die Betroffenen* bestehen.

Daraus folgt für die Risikomodellierung des (operativen) Datenschutzes:

1. **Jede Organisation gilt als Angreifer, insbesondere und auch diejenige, deren Datenverarbeitung legitim ist und eine Rechtsgrundlage hat.**

2. **Jede Verarbeitung personenbezogener Daten erzeugt deshalb immer mindestens ein „normales“ Risiko** für betroffene Personen (sowie ein „Datenschutz-Compliance-Risiko“ für die Organisation).

# Schutzbedarf, Schutzniveau, Restrisiko

„Risiko“ (DSGVO):

- Das **Gesamtrisiko** der Verarbeitungstätigkeit einer Organisation ergibt sich für Betroffene aus 3 Risikoquellen: zu intensiver Grundrechtseingriff sowie mangelhafte Schutzmaßnahmen für Datenschutz und IT-Sicherheit.

„Schutzbedarf“ (SDM):

- **Der Schutzbedarf einer Person richtet sich nach dem Risiko, das eine Verarbeitungstätigkeit ohne rechtskonform gestaltete Funktionalität und ohne implementierte Schutzmaßnahmen erzeugt.**
- *normales Risiko → normaler Schutzbedarf* des/der Betroffenen,
- *hohes Risiko → hoher Schutzbedarf*,
- ((sehr hohes Risiko) → sehr hoher Schutzbedarf (= „Gefahr für Leib und Leben“)).

„Schutzniveau“ (DSGVO):

- **Das Schutzniveau ist das Ergebnis der funktionalen Gestaltung der Verarbeitungstätigkeite sowie der Wirksamkeit der betriebenen Schutzmaßnahmen.**

„Restrisiko“ (SDM):

- **Wenn das Schutzniveau zu gering ist, ist das verbleibende Risiko („Restrisiko“) zu groß**. Ist eine Schutzmaßnahme unzureichend wirksam, können materielle und immaterielle Schäden für Betroffene entstehen, die Verarbeitungstätigkeit ist nicht rechtskonform.

**Zusammenhang: Der *Schutzbedarf* bleibt konstant, aber die *Schwere des Grundrechtseingriffs* und die *Risiken* der Verarbeitung können mittels Schutzmaßnahmen auf ein verantwortbares *Schutzniveau* bzw. *Restrisiko* reduziert werden.**

# Risikokriterien

## „Grundsätze“ Art. 5, Abs. 1 DSGVO verdichtet zu „Gewährleistungszielen“

„Personenbezogene Daten müssen...“

(a) „... in einer für die Person nachvollziehbaren Weise verarbeitet werden ... (**Transparenz**).“

(b) „... für festgelegte eindeutige und legitime Zwecke erhoben werden ... (**Zweckbindung**).“

(c) „... auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**Datenminimierung**).“

(d) „... damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ... **unverzüglich gelöscht oder berichtigt** werden.“

(f) „... Schutz vor **Verlust** ... **Integrität und Vertraulichkeit**“.

Normative Anforderungen verdichtet zu “Gewährleistungs-zielen“:

- Transparenz ✓
- Nichtverkettung ✓
- Datenminimierung ✓
- Intervenierbarkeit ✓
- Verfügbarkeit ✓
- Integrität ✓
- Vertraulichkeit ✓

# Fragen

- Was ist eine **Verarbeitung**?
- Was ist ein Datenschutz-**Risiko**?
- Wie führt man eine **Schwellwert-Analyse** durch?

# Funktion einer Schwellwert-Analyse

Eine Schwellwert-Analyse im Kontext des Artikel 35 DSGVO zur Datenschutzfolgenabschätzung soll die Entscheidung begründen, ob für eine Verarbeitungstätigkeit ein **normales oder hohes Risiko** vorliegt.
(Mit dem Analyseergebnis „geringes Risiko“ oder „normales Risiko“ muss keine Datenschutz-Folgenabschätzung durchgeführt werden.)

# „hohes Risiko“ wenn Verarbeitung in „Muss-Liste“ der DSK-Liste enthalten ist

DSK
DATENSCHUTZKONFERENZ

**Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist**

| Nr. | Maßgebliche Beschreibung der Verarbeitungstätigkeit | Typische Einsatzfelder | Beispiele |
|---|---|---|---|
| 1 | Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft:<br>• Daten zu schutzbedürftigen Betroffenen<br>• Systematische Überwachung | Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke. | Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein.<br><br>Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an. |

- 17 Eintragungen aus dem nicht-öffentlichen Bereich
- Liste ist nicht-abschließend
- referenziert in den Hinweisen am Ende die Leitlinie aus WP248 der Art. 29-Gruppe
- **Fazit:** Mäßig hilfreich als Entscheidungshilfe für die Praxis.

Quelle für „Muss-Liste“: https://www.datenschutzkonferenz-online.de/kurzpapiere.html

# „hohes Risiko“

## wenn Kriterium in WP248-Liste ausgewiesen

1. **Bewerten oder Einstufen** (Scoring)
   *(“Evaluation or scoring”)*
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
   *(“Automated-decision making with legal or similar significant effect”)*
3. **Systematische Überwachung**
   *(“Systematic monitoring”)*
4. **Vertrauliche oder höchst persönliche Daten**
   *(“Sensitive data or data of a highly personal nature”)*
5. **Datenverarbeitung in großem Umfang**
   *(“Data processed on a large scale”)*
6. **Abgleichen oder Zusammenführen von Datensätzen**
   *(“Matching or combining datasets”)*
7. **Daten zu schutzbedürftigen Betroffenen**
   *(“Data concerning vulnerable data subjects”)*
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
   *(“Innovative use or applying new technological or organisational solutions”)*
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**
   *(“When the processing in itself prevents data subjects from exercising a right or using a service or a contract”)*

Wenn aus dieser Liste mindestens *zwei Kriterien* zutreffen, besteht für die Freiheiten und Rechte betroffener Personen ein *hohes Risiko* (Risikotyp 1).

Diese **Bestimmung des Riskos** aus der Intensität des Grundrechtseingriffs bildet die Voraussetzung zur Gestaltung der gesamten Verarbeitungstätigkeit.

aus: WP 248 der Art. 29 Gruppe ab Seite 10 ff.

# „hohes Risiko“ wenn Kategorie in Artikel 9 DSGVO enthalten ist

*„(1) Die Verarbeitung personenbezogener Daten, aus denen* ***die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit*** *hervorgehen, sowie die Verarbeitung von* ***genetischen Daten, biometrischen Daten*** *zur eindeutigen Identifizierung einer natürlichen Person,* ***Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung*** *einer natürlichen Person ist untersagt.*
*(2) Absatz 1 gilt nicht in folgenden Fällen:*
*a) … j) …*
*(3)*

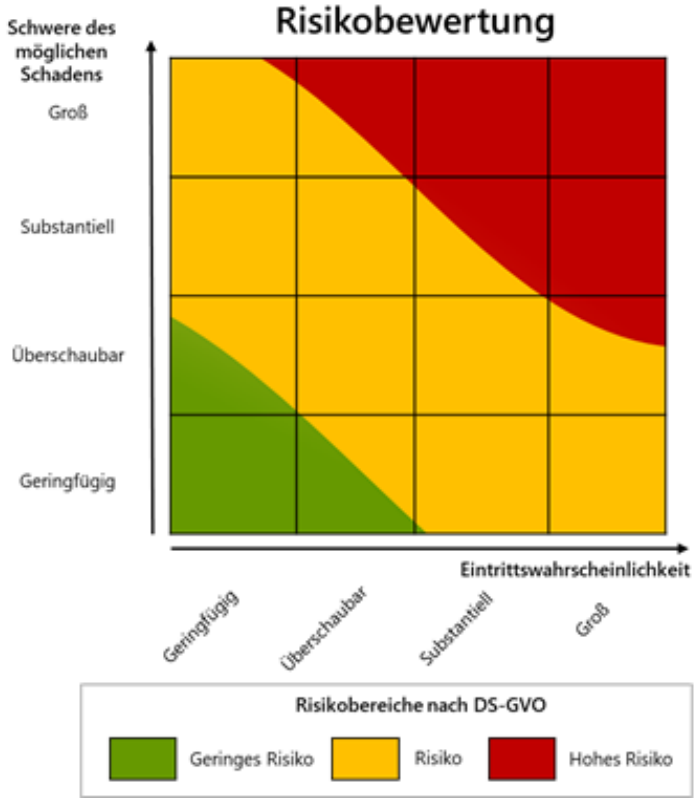
# „hohes Risiko“ wenn Verarbeitung in Artikel 35 DSGVO enthalten ist

Eine Datenschutz-Folgenabschätzung (DSFA) bzw. ein Data-Protection-Impact-Assessment (DPIA) ist durchzuführen bei:

- **Scoring, Profiling, automatisiertem Einzelentscheid, Einsatz neuer (Überwachungs-)Techniken, Videoüberwachung des öffentlichen Raumes**;
- besonders **schutzwürdigen Daten** (bspw. von Minderjährigen oder Gefangenen)

# Risikobestimmung

## bzgl. Risikotyp 2 und 3, Schutzmaßnahmen




Wenn Schutzmaßnahmen des Datenschutzes und der IT-Sicherheit *nicht implementiert sind, ausfallen oder nicht überwacht* werden (Risikotypen 2 und 3), kann die Höhe des Risikos anhand der Formel „Schwere des möglichen Schadens x Eintrittswahrscheinlichkeit“ (Art. 24 DSGVO) für Betroffene bestimmt werden.

**Erwägungsgrund 75 DSGVO führt zu Schäden:**

- Diskriminierung,
- Identitätsdiebstahl oder-betrug,
- finanzieller Verlust,
- Rufschädigung,
- wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

aus: DSK 2018: „Gemeinsame Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (2018-0525) / ebenso: DSK: „Kurzpapier Nr. 18“

# Datenschutz-Risiken durch Angreifer

Angreifer-Organisationen auf Personen:

- Datenverarbeiter und Auftragsverarbeiter (Hauptangreifer)
- Sicherheitsbehörden
- Leistungsverwaltung
- Bereitsteller von IT-(Infrastruktur)Diensten
- Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
- Versicherungen und Banken
- Forschungsinstitute, insbes. psychologischer und sozialwissenschaftlicher Art
- Krankenhäuser, Ärzte, Rechtsanwälte
- Aggressive Startups, Werbeagenturen
- Untätige Aufsichtsbehörden
- Cracker

# Vorgehensweise Schwellwert-Analyse

1. **Bestimmen des Risikos Typ 1 „Grundrechtseingriff“**
   („Risiken für Rechte und Freiheiten natürlicher Personen“)
2. **Festsetzen des Schutzbedarfs der Betroffenen** anhand der Risiken der „reinen“ Verarbeitungstätigkeit ohne Schutzmaßnahmen.
   - Geringes oder normales Risiko => normaler Schutzbedarf
   - hohes Risiko => hoher Schutzbedarf
   - *(sehr hohes Risiko => sehr hoher Schutzbedarf*
     *„sehr hohes Risiko“ nicht in DSGVO, wohl aber IT-Grundschutz des BSI)*
3. **Schutzbedarf der Betroffenen bleibt konstant, das Risiko einer Verarbeitung für den Betroffenen kann verringert werden**, durch Gestaltung der Verarbeitungstätigkeit und durch Implementation von Schutzmaßnahmen des Datenschutzes und der Informationssicherheit (Typ 2 und Typ 3) entsprechend dem festgestellten Schutzbedarf.
4. Ist das Rest-Risiko zu hoch, ist die Verarbeitung nicht aufzunehmen bzw. einzustellen, durch eine andere zu ersetzen oder Aufsichtsbehörde zu konsultieren (Art. 36 DSGVO).

# Übung
# Durchführung einer Schwellwert-Analyse für die geplante Verarbeitung „pay-as-you-drive“

1. Lesen Sie sich die Beschreibung der Verarbeitung durch! (5min)

2. Bestimmen Sie die Mittel zur Durchführung der Schwell-Analyse! (gemeinsame Diskussion, 5min)

3. Begründen Sie mit Stichworten das Risiko bzw. Schutzbedarf dieser Verarbeitung!
(5min, bitte zusammen mit dem Nachbarn oder der Nachbarin.)

# Übung
# Kriterienkataloge für „hohes Rrisiko“

WP 248 der Art. 29 Gruppe ab Seite 10 ff.:

1. **Bewerten oder Einstufen** (Scoring)
   *(“Evaluation or scoring”)*
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
   *(“Automated-decision making with legal or similar significant effect”)*
3. **Systematische Überwachung**
   *(“Systematic monitoring”)*
4. **Vertrauliche oder höchst persönliche Daten**
   *(“Sensitive data or data of a highly personal nature”)*
5. **Datenverarbeitung in großem Umfang**
   *(“Data processed on a large scale”)*
6. **Abgleichen oder Zusammenführen von Datensätzen**
   *(“Matching or combining datasets”)*
7. **Daten zu schutzbedürftigen Betroffenen**
   *(“Data concerning vulnerable data subjects”)*
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
   *(“Innovative use or applying new technological or organisational solutions”)*
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**
   *(“When the processing in itself prevents data subjects from exercising a right or using a service or a contract”)*

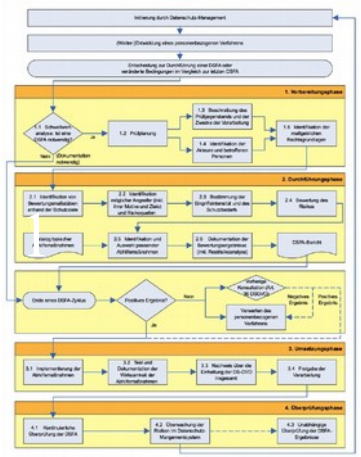
Art. 9 DSGVO:

*„(1) Die Verarbeitung personenbezogener Daten, aus denen* ***die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit*** *hervorgehen, sowie die Verarbeitung von* ***genetischen Daten, biometrischen Daten*** *zur eindeutigen Identifizierung einer natürlichen Person,* ***Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung*** *einer natürlichen Person ist untersagt.*

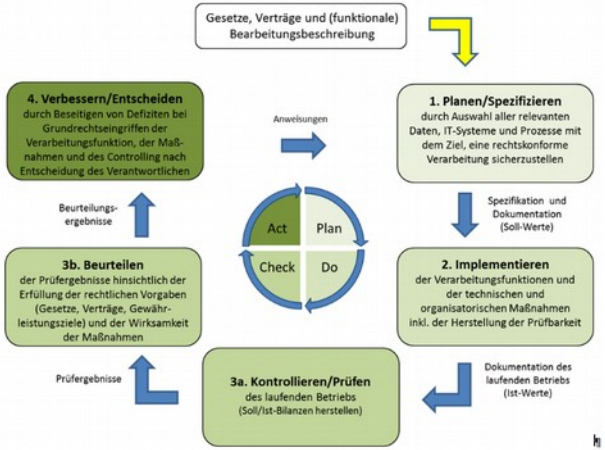
Art. 35 DSGVO:

- **Muss-Liste** der Datenschutz-Aufsichtsbehörden
- **Scoring, Profiling, automatisiertem Einzelentscheid, Einsatz neuer (Überwachungs-)Techniken, Videoüberwachung des öffentlichen Raumes**;
- besonders **schutzwürdigen Daten** (bspw. von Minderjährigen oder Gefangenen)

# Umsetzung einer DSFA in der Praxis



+ SDM Standard-Datenschutzmodell +




1. Durchführen einer DSFA mit dem **DSFA-Framework** vom Privacy-Forum
2. Bestimmen von Schutzmaßnahmen mit dem **SDM**
3. Implementieren und Kontrollieren der Schutzmaßnahmen mit **DS-Managementsystem**

# Aktueller Status SDM

SDM
Standard-Datenschutzmodell

V 1.1- 2018


Das SDM

- ist eine **Methode zur Prüfung und Beratung** des Datenschutzes von Verarbeitungstätigkeiten, zuletzt bestätigt von der DSB-Konferenz 2018/04.
- normativ **verankert in der DSGVO**, methodisch **angelehnt an IT-Grundschutz.**
- Methodik-Handbuch auf **Webseiten** der deutschen Datenschutzaufsichtsbehörden veröffentlicht, es enthält in Kap. 7 eine Auflistung generischer Schutzmaßnahmen.
- zur Version 1.1 wurde vollständig auf die DSGVO umgestellt.
- umfasst einen ersten **Katalog mit Maßnahmen**, der im September 2018 von den Datenschutzbeauftragten der Bundesländer Hessen, Mecklenburg-Vorpommern, Schleswig-Holstein, Sachsen sowie der Evangelischen Kirche Deutschlands veröffentlicht wurde.
- soll es mit **Tool-Unterstützung** geben. Gespräche mit Toolherstellern laufen.
- liegt für V1.0 in einer **Englischversion** vor.
- An der Version **SDM 2.0** wird aktuell mit Hochdruck gearbeitet: Stärkere Verankerung in der DSGVO, Schutzbedarfsfeststellung, Abgrenzung zu IT-Grundschutz, Komponenten eines Datenschutz-Managementsystems.

Quelle:
DSBK 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

# Standard-Maßnahmen zur Umsetzung der Grundsätzein Art. 5 DSGVO

Sicherstellung von ***Verfügbarkeit***
Redundante Datensätze, IT-Systeme, Prozesse, „schnelle Reparaturzeiten“

Sicherstellung von ***Integrität***
Hash-Wert-Vergleiche, Härten von IT-Systemen, Festlegen von Min./Max.-Referenzen bei Prozessen, Steuerung der Regulation von Prozessen

Sicherstellung von ***Vertraulichkeit***
Verschlüsselung, Rollen- und Berechtigungskonzepte

Sicherstellung von ***Transparenz***
Prüffähigkeit durch Spezifikation, Protokollierung, Dokumentation, Tests und Freigaben

Sicherstellung von ***Nichtverkettbarkeit*** durch Zweckbestimmung/-bindung, Pseudonymität, Anonymität; Trennung und Isolierung von Datenbeständen, IT-Systemen, Prozessabläufen, Rollen- und Berechtigungskonzepte

Sicherstellung von ***Intervenierbarkeit***
SPOC für Änderungen, Korrekturen, Löschen, Aus-Schalter, standardisierte Changemanagementprozesse in Organisationen

Quelle: SDM-Handbuch, V1.1
Kapitel 7 „generische Maßnahmen“

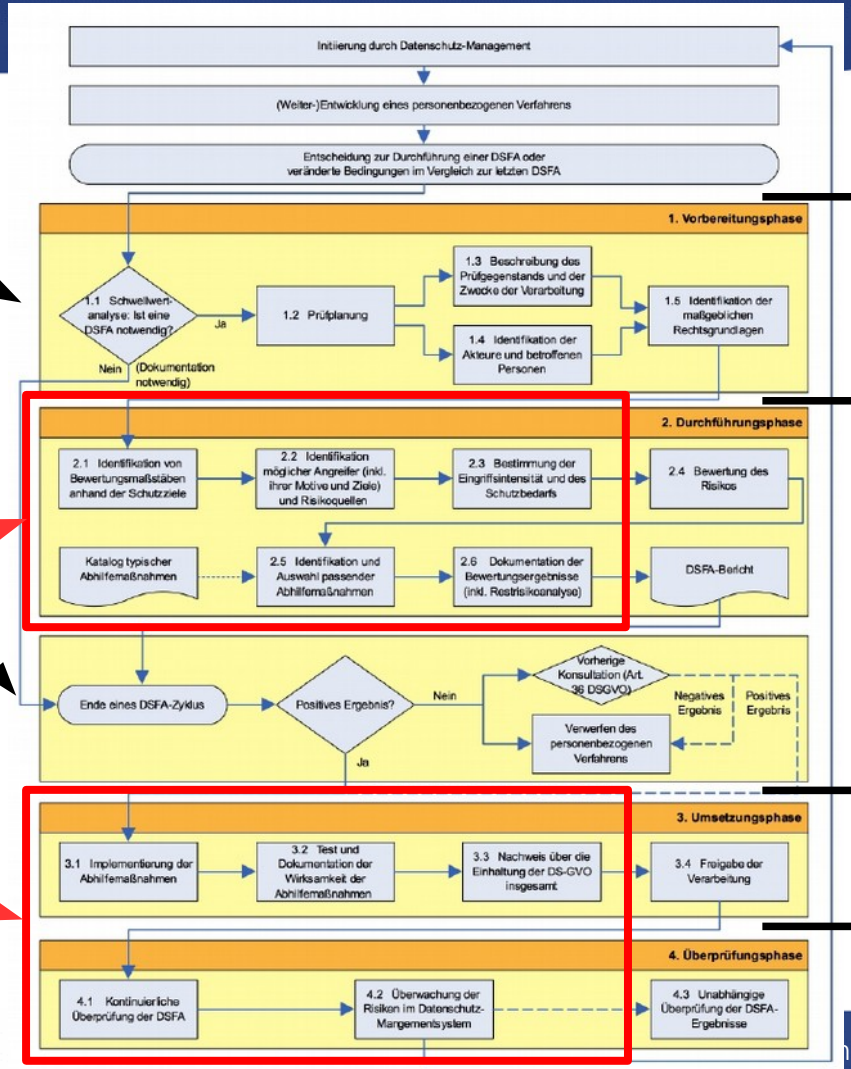
# Standard-Maßnahmen bei „hohem Risiko“ / „hohem Schutzbedarf“

- **Grundsätzlich: Betrieb der gleichen Schutzmaßnahmen wie bei „normalem Risiko“**.
- **Zusätzlich 1**: Prüfen, ob speziell angepasst auf die Verarbeitung **zusätzliche Maßnahmen** betrieben werden müssen.
- **Zusätzlich 2 (obligatorisch)**: Regel „**Anwendung der Schutzmaßnahmen auf sich selber**“ z.B.:
  - Vertraulichkeits- (Verschlüsselung) und Integritätsschutz (Signieren) für Protokoll-Daten;
  - Transparenz beim Löschvorgang durch revisionsfeste Dokumentation und Protokollierung;
  - Transparenz bei Pseudonymisierung und Anonymisierung durch Tests, Dokumentation und Protokollierung.
  - Zugang zu Rollen- und Berechtigungen mit starkem Authentifizierungsverfahren,
  - Nachweislich funktionierendes Datenschutz-Managementsystem, das Veränderungen auch durchsetzen kann
  - ...

# DSFA-Framework

typische Projektvor-bereitungen

Entscheiden und Priorisieren




SDM
Standard-Datenschutzmodell

1. Vorbereitung (*Plan*)

2. Durchführung (*Do*)

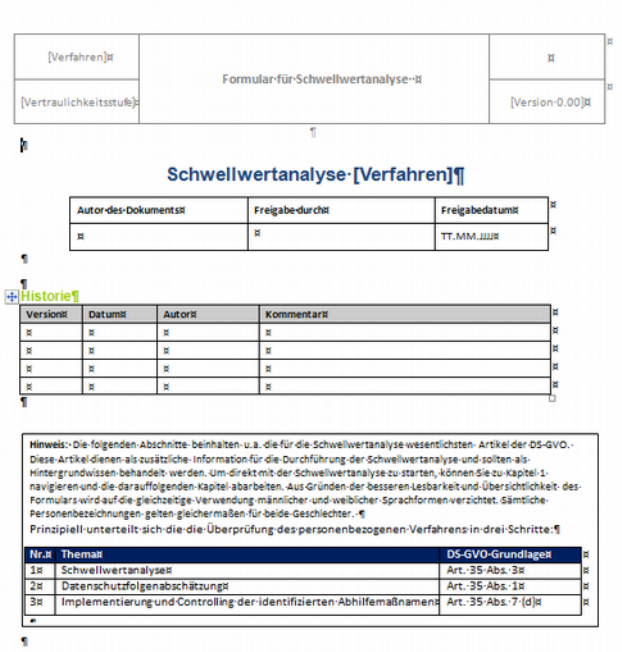
3. Umsetzung (*Act*)

4. Überprüfung (*Check*)

Quelle: https://www.forum-privatheit.de/forum-privatheit-de/ publikationen-und-downloads/veroeffentlichungen-des-forums.php

# Formular zur Schwellwert-Analyse des Zentralen IT-Managements im Land Schleswig-Holstein (ZIT-SH)

- 1. Beschreibung der Verarbeitungsweise
  - 1.1 Beschreibung des Verfahrens und deren Rollen
    - 1.1.1 Fachliche Beschreibung des Verfahrens
    - 1.1.2 Identifizieren Sie den Verantwortlichen der Datenverarbeitung
    - 1.1.3 Identifizieren Sie den behördlichen Datenschutzbeauftragten
    - 1.1.4 Identifizieren Sie die Empfänger7 (datenverarbeitende Stelle) der ...
    - 1.1.5 Liste der verarbeitenden personenbezogenen Daten
- 2. Schutzbedarfsfeststellung
- 3. Details der Verarbeitung
  - 3.1 Art der Verarbeitung
  - 3.2 Abgleich Kriterien des europäischen Datenschutzausschusses
  - 3.3 Dokumentation über datenschutzrechtliche Verhaltensregeln (wenn vor...
  - 3.4 Umstand und Kontext der Verarbeitung
  - 3.5 Umfang der Verarbeitung
  - 3.6 Zwecke der Verarbeitung
  - 3.7 Identifikation der Rechtsgrundlagen
  - 3.8 Notwendigkeit und Verhältnismäßigkeit der Verarbeitung
- 4. Ergebnis der Schwellwertanalyse



| [Verfahren] | Formular für Schwellwertanalyse | |
|---|---|---|
| [Vertraulichkeitsstufe] | | [Version 0.00] |

**Schwellwertanalyse [Verfahren]**

| Autor des Dokuments | Freigabe durch | Freigabedatum |
|---|---|---|
| | | TT.MM.JJJJ |

Historie

| Version | Datum | Autor | Kommentar |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Hinweis: Die folgenden Abschnitte beinhalten u.a. die für die Schwellwertanalyse wesentlichsten Artikel der DS-GVO. Diese Artikel dienen als zusätzliche Information für die Durchführung der Schwellwertanalyse und sollten als Hintergrundwissen behandelt werden. Um direkt mit der Schwellwertanalyse zu starten, können Sie zu Kapitel 1 navigieren und die darauffolgenden Kapitel abarbeiten. Aus Gründen der besseren Lesbarkeit und Übersichtlichkeit des Formulars wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beide Geschlechter.

Prinzipiell unterteilt sich die die Überprüfung des personenbezogenen Verfahrens in drei Schritte:

| Nr. | Thema | DS-GVO-Grundlage |
|---|---|---|
| 1 | Schwellwertanalyse | Art. 35 Abs. 3 |
| 2 | Datenschutzfolgenabschätzung | Art. 35 Abs. 1 |
| 3 | Implementierung und Controlling der identifizierten Abhilfemaßnahmen | Art. 35 Abs. 7 (d) |

# Durchführung einer toolgestützten DSFA (Fr. de Lange (Kr. Stormarn) / Hr. Amann (Kiel))

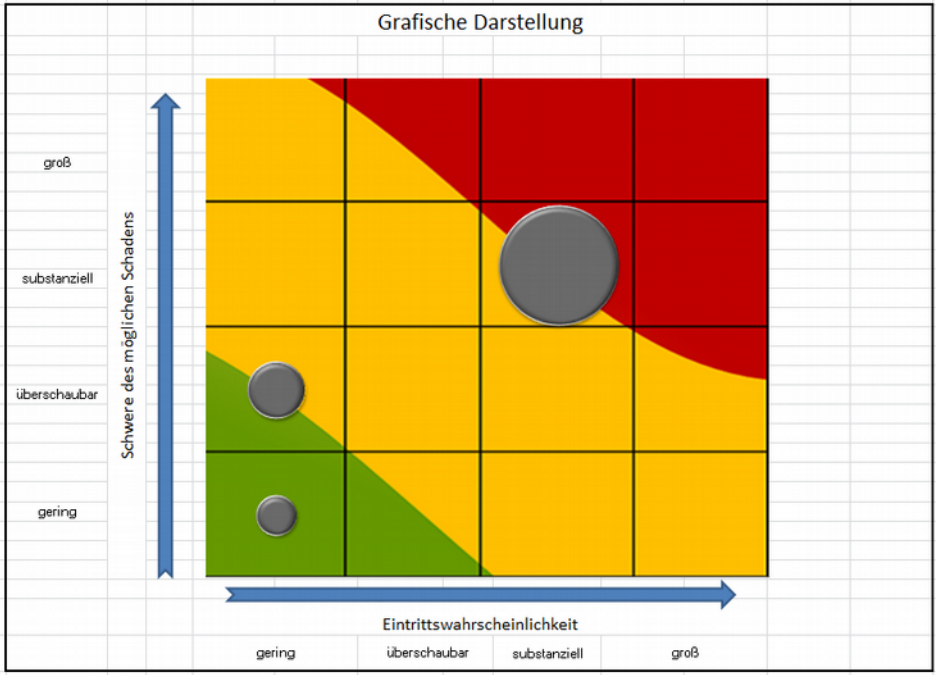
A2 | Produktphase

**Produktphase**

## Rechnerische Darstellung

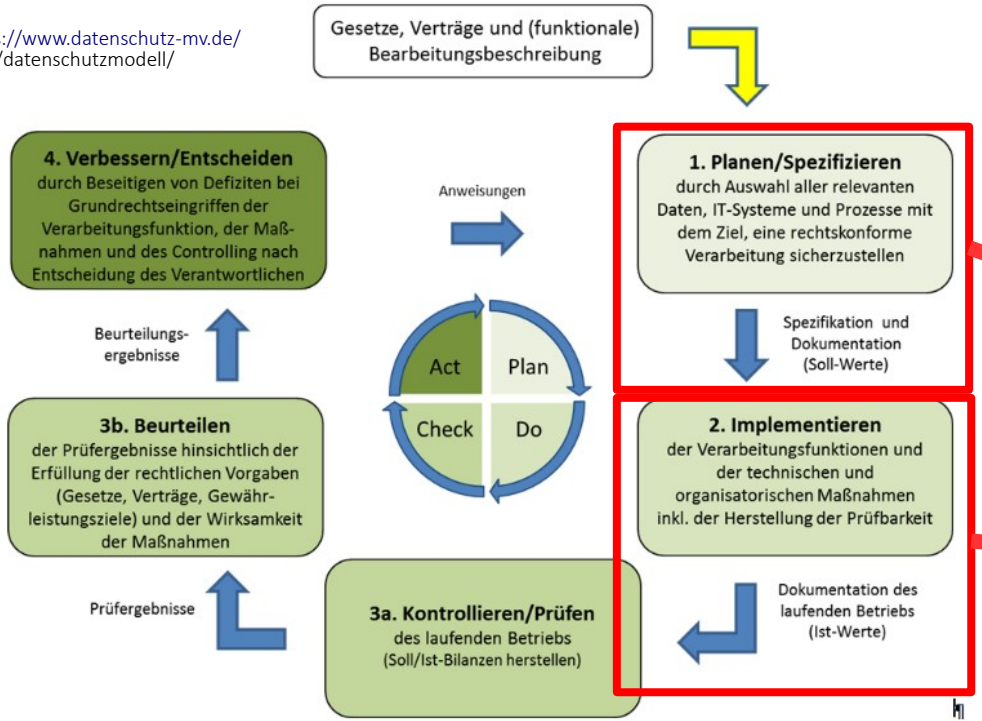
| | | Eintrittsw. | Schaden | Produkt |
|---|---|---|---|---|
| Datenminierung | | 1 | 1 | 1 |
| Verfügbarkeit | Daten | 1 | 1 | 1 |
| | Systeme | 1 | 2 | 2 |
| | Prozesse | 1 | 2 | 2 |
| Integrität | Daten | 1 | 2 | 2 |
| | Systeme | 3 | 3 | 9 |
| | Prozesse | 1 | 1 | 1 |
| Vertraulichkeit | Daten | 1 | 2 | 2 |
| | Systeme | 1 | 2 | 2 |
| | Prozesse | 1 | 2 | 2 |
| Transparenz | Daten | 1 | 1 | 1 |
| | Systeme | 1 | 1 | 1 |
| | Prozesse | 1 | 1 | 1 |
| Nichtverkettbarkeit | Daten | 1 | 1 | 1 |
| | Systeme | 1 | 1 | 1 |
| | Prozesse | 1 | 1 | 1 |
| Intervenierbarkeit | Daten | 1 | 1 | 1 |
| | Systeme | 1 | 1 | 1 |
| | Prozesse | 1 | 1 | 1 |

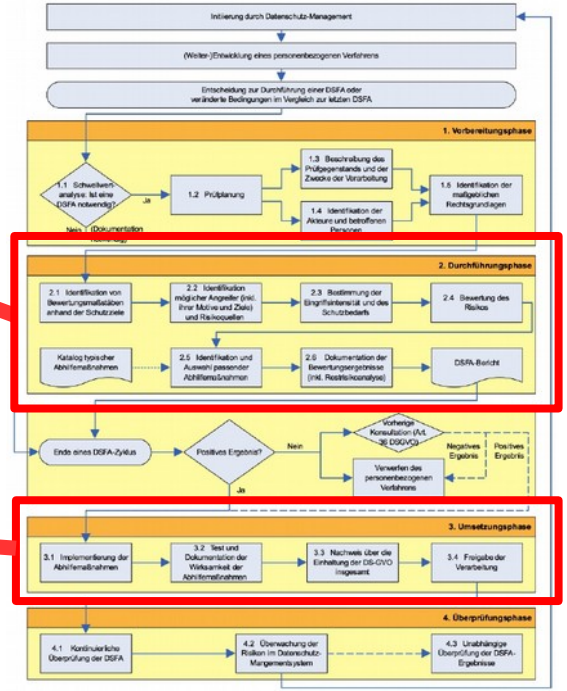
## Grafische Darstellung



# Datenschutz-Managementsystem (DSMS) für laufenden Betrieb

Quelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/



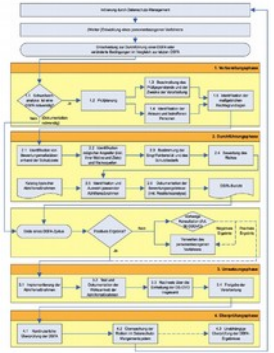

**Fokus DSMS**: *organisationsübergreifend* für alle Verarbeitungstätigkeiten (insbes. Betrieb Infrastruktur)

**Fokus DSFA**: speziell für *einzelne Verarbeitungstätigkeit*

# Referenzen

- **DSGVO: Datenschutz-Grundverordnung**
  https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
- **WP248 der Art. 29-Gruppe, Kriterienkatalog für Schwellwertanalyse**
  http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- **„Muss-Liste“ der DSK:** https://www.datenschutzkonferenz-online.de/kurzpapiere.html
- **Datenschutz-Folgenabschätzung**
  Forum Privatheit: https://www.forum-privatheit.de/forum-privatheit-de/ publikationen-und-downloads/veroeffentlichungen-des-forums.php
- **SDM-Handbuch zur Methodik**
  DSBK 2018, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
- **SDM-Bausteine** (auch Baustein: „DS-Management“)
  UAGSDM_BS: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
- **SDM-Newsletter**
  ULD: https://www.datenschutzzentrum.de/sdm/ [Link unten: „Newsletter“]
- **SDM- und DSFA-Schulungen**
  ULD: regelmäßig bei der DSA: https://www.datenschutzzentrum.de/akademie/





ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon / Durchwahl: 0431 988 – 1391
martin.rost@datenschutzzentrum.de
http://www.datenschutzzentrum.de/