Datenschutz-Folgenabschätzung

– Das neue Framework –

Felix Bieker / Martin Rost

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Agenda

1. Anforderungen der DSGVO
2. Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO
3. Das neue Framework für die Durchführung der Datenschutz-Folgenabschätzung
4. Literatur

1. Anforderungen der DSGVO

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Artikel 35

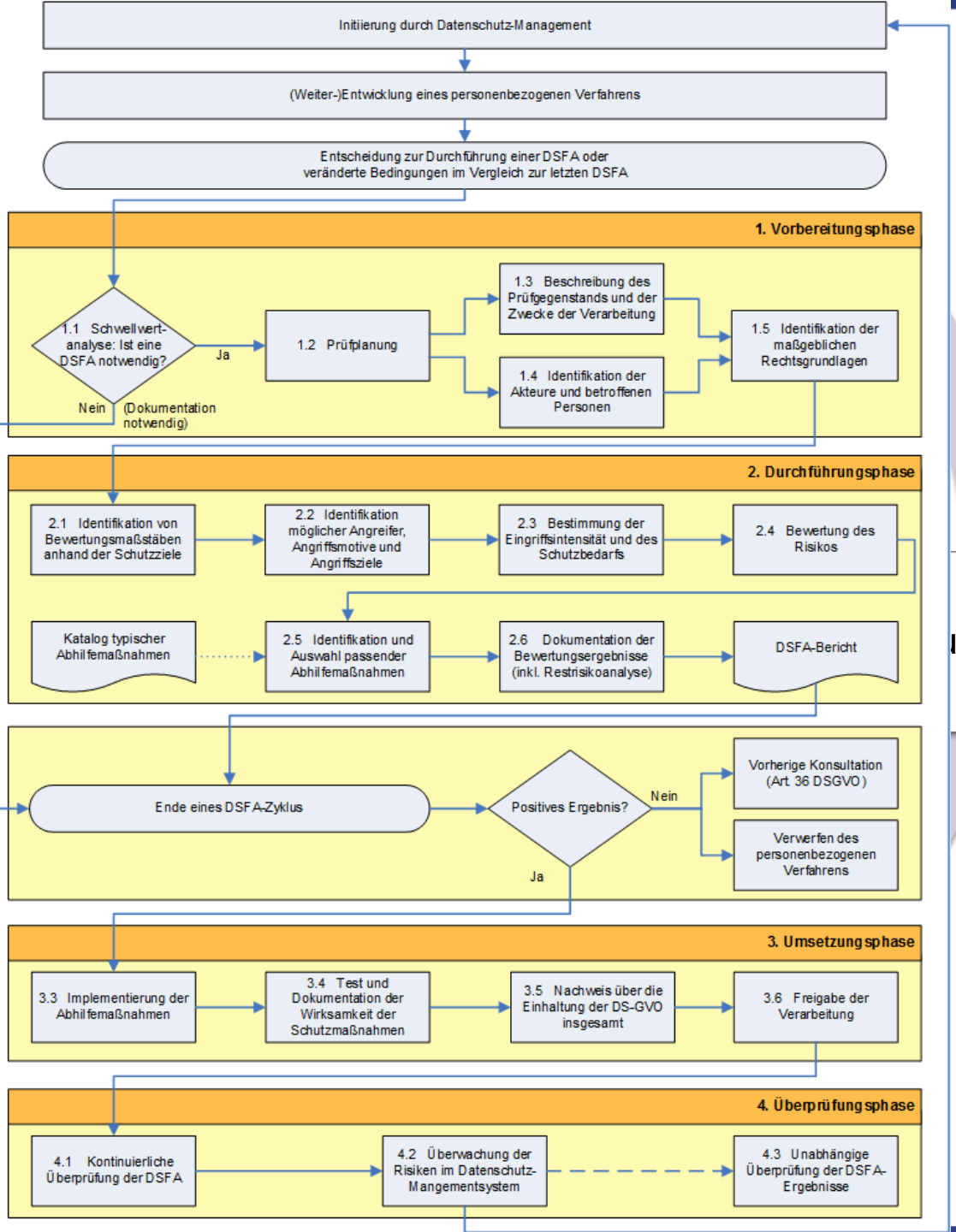
Datenschutz-Folgenabschätzung

(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.

Was ist eine Datenschutz-Folgenabschätzung?

- Instrument, um DSGVO umzusetzen
- Instrument, um in Verfahren oder Systemen die Risiken für Individuen, die von Organisationen durch Nutzung von Verfahren ausgehen, zu erkennen und zu beurteilen.
- Wortwahl: Datenschutz-Folgenabschätzung (DSFA) meint nicht: Abschätzen der Folgen, die durch Datenschutz entstehen! Sondern: Abschätzung der Folgen eines Verfahrens aus Datenschutz-Perspektive!
- Keine TFA: Im Fokus stehen auch nicht Folgen aus einer Technik, sondern die Eingriffsintensität eines Verfahren, in dem ggfs. eine neue Technik eingesetzt wird.

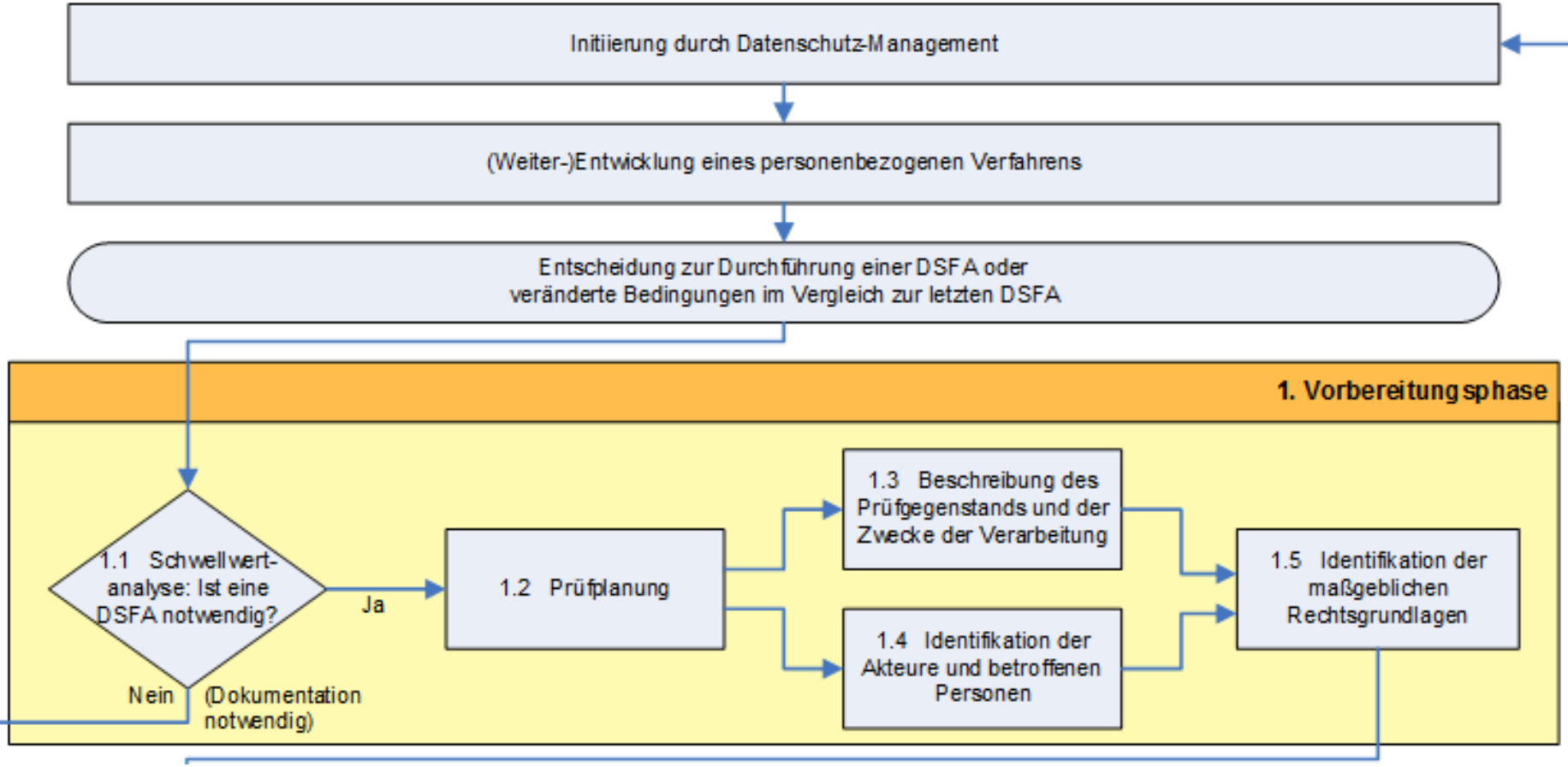
durch?



4. Überprüfu

ungsphase

1. Vorbereitungsphase



1.1 Schwellwert-Analyse

- Schwellwert-Analyse ist stets vorzunehmen!
- DSFA ist durchzuführen bei:
  - „voraussichtlich hohem Risiko“, wenn eine hohe Eingriffsintensität einer Organisation durch eine Form von Verfahrenstätigkeit vorliegt:
    1. Es werden gesetzlich festgelegte, besonders schutzwürdige **Daten** erhoben / verarbeitet / übermittelt (Auflistung aus Art. 9 u. 10 DSGVO)
    2. Es sind besonders sensible **Prozesse** systematischer, umfangreicher Überwachung vorgesehen: Scoring, Profiling, automatisierter Einzelentscheid, Video- und Telekommunikationsüberwachung (E-Mail) von Mitarbeitern, Kunden, Bürger, Patienten
    3. Es kommen besonders riskante **Techniken** zum Einsatz: Big Data, Authentisierung durch Biometrie, Infrastruktur-IT wie Active Directory, Router, Proxies, Firewalls, CPU- und Speicher-Cluster
  - Kriterien der Artikel-29-Gruppe
- Aufsichtsbehörden erstellen eine Muss-Liste (Kohärenzverfahren)

Muss-Liste

(Aktueller Stand: Sichtung von Verfahren)

Verfahrens-bezeichnung | Inhaltliche Begründung | Kriterium (Art. 29)

	A	B	C	D	E	F
1	**Blacklists**					
2		**Sachverhalt**	**Begründung**	**Bemerkung**	**Art. 29 Kriterium**	**Bewertung**
3	**Finanz und Versicherungsbranche**					
4	1	Scoring Verfahren durch Auskunfteien, Banken, Versicherungen	- hohes Risiko finanzieller Nachteile für Betroffene durch erhöhte Kreditzinsen, Versicherungsbeiträge aufgrund eines schlechten score-Wertes - hohes Risiko, dass ein schlechter Score-Wert aufgrund veralteter oder falscher Angaben errechnet wurde - besonders umfangreiche Datenverarbeitung, weil es eine Vielzahl von Kunden betrifft - Scoring-Verfahren sind Stand der Technik, bei denen neue Technologien zur Score-Wert-Berechnung eingesetzt werden		1. Scoring 2. Automatisierte Einzelentscheidung (mit Rechtswirkung) (+)/(-) 5. Umfangreiche Datenverarbeitung (+)/(-) 6. Verkettung von Daten (+)/(-)	
5	2	Bewertung des Fahrverhaltens für Kraftfahrzeug-Haftpflichtversicherungstarife vom Typ Pay as You drive, sowie andere Verhaltensbasierte Tarife	Mithilfe einer sogenannten On-Board-Unit (OBU) werden Angaben zum Beschleunigungs- und Bremsverhalten, zur Geschwindigkeit und teilweise auch zur Fahrtzeit sowie GPS-Daten des Fahrzeugs erhoben und für die Erzeugung von Scorewerten genutzt. Es besteht daher das Risiko, das Bewegungsprofile erstellt werden. Die Scorewerte bewerten zudem das Fahrverhalten des Fahrers und können diesen bei Kenntnisnahme Dritter auch in versicherungsfremdem Kontext in Misskredit bringen.		1. Scoring 2. Automatisierte Einzelentscheidung (mit Rechtswirkung) 3. Systematisches Beobachten 4. Sensitive Daten 5. Umfangreiche Datenverarbeitung 8. Neue Technologien/Verarbeitungen 9. Verarbeitung außerhalb EWR 10. Hürde für den Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen zu können	
6	3	Datenverarbeitung durch Kreditinstitute / Die Verarbeitung von pbDaten zu Bank- und Finanzdienstleistungsgeschäften durch Kredit- und Finanzdienstleistungsinstitute	- Die Daten liefern umfangreiche Informationen, die von betroffenen Personen üblicherweise als vertraulich betrachtet werden. Sie ermöglichen eine umfassende Analyse der Lebens- und Konsumgewohnheiten der betroffenen Personen. Sie sind in erheblichem Umfang dazu geeignet, betroffene Personen zu bewerten, die Beurteilung und das Ansehen der betroffenen Personen zu prägen und die Teilnahme am Wirtschaftsleben zu beeinflussen. Daten über die finanziellen Verhältnisse Betroffener werden in sehr großem Umfang verarbeitet. Gemeint ist nicht nur der Umfang des Vorliegens von Einzeldaten über Betroffene über einen in aller Regele sehr langen Zeitraum hinweg, sondern auch die Anzahl der Betroffenen. - Über die finanziellen Verhältnisse hinaus können auch sensible personenbezogene Daten betroffen sein, wenn sich etwa aus Girokontoauszügen Hinweise auf Gesundheitsdaten, Gewerkschafts- oder Parteizugehörigkeit, sexuelle Vorlieben etc. sowie auf Aufenthaltsorte ergeben. - Verbunden mit dem Abschluss von Kontoverträgen, in vielen Fällen auch während der Vertragslaufzeit, werden Auswertungen und Scorings der Betroffenen vorgenommen, um ihre Kreditwürdigkeit zu überprüfen.	Die Begründung orientiert sich an III. B. b) des Entwurfs WP 248 (1. und 5.)	3. Systematisches Beobachten möglich wird jedoch nicht gemacht 4. Sensitive Daten nur teilweise 5. Umfangreiche Datenverarbeitung	
7	4	Betrieb einer Wirtschaftsauskunftei einschl. Scoringberechnung	Riesige Datenmengen, die geschäftsmäßig an Dritte übermittelt werden. Bonitäts- bzw. Scoringberechnung entscheidet über Teilnahmemöglichkeiten am Wirtschaftsleben. Dadurch ein starker Grundrechtseingriff. Gefahr der Fehlberechnung im Rahmen automatisierter Einzelentscheidungen, der Personenverwechslung.		1. Scoring 2. Automatisierte Einzelentscheidung (mit Rechtswirkung) (+)/(-) 5. Umfangreiche Datenverarbeitung (+)/(-) 6. Verkettung von Daten (+)/(-)	

1.2 Prüfplanung

- Konventionelles Projektmanagement
  - Empfehlung: DSFA als ein Projekt anlegen
  - Ressourcen für das Projekt klären (Zeitraum und Zeitbedarf, Budget, Personal)
  - Expert_innen-Projektteam zusammenstellen, Rollen klären
  - Projektmanagement-Methode bestimmen
  - Empfehlung: Projekt in Phasen einteilen (typisch: Inventarisierung, Plan für Mängelbehebung, Mängelbehebung, Test & Freigabe mit Management der Phasenübergänge durch Lenkungskreis)

1.3 Prüfgegenstand, 1.4 Akteure, 1.5 Rechtsgrundlagen

1.3 Beschreibung des Prüfgegenstands und der Zwecke der Verarbeitung

- Klären, dass der Verfahrenzweck legitim ist und das Verfahren rechtskonform betrieben werden kann (Verbot mit Erlaubnisvorbehalt)
- Prüfgegenstand ist eine Datenverarbeitung (Verfahren):
  - Daten, Formate, Protokolle, IT-Systeme, Prozesse, Funktionsrollen
- Zwecke der Datenverarbeitung
  - Datenminimierung, Zweckbindung

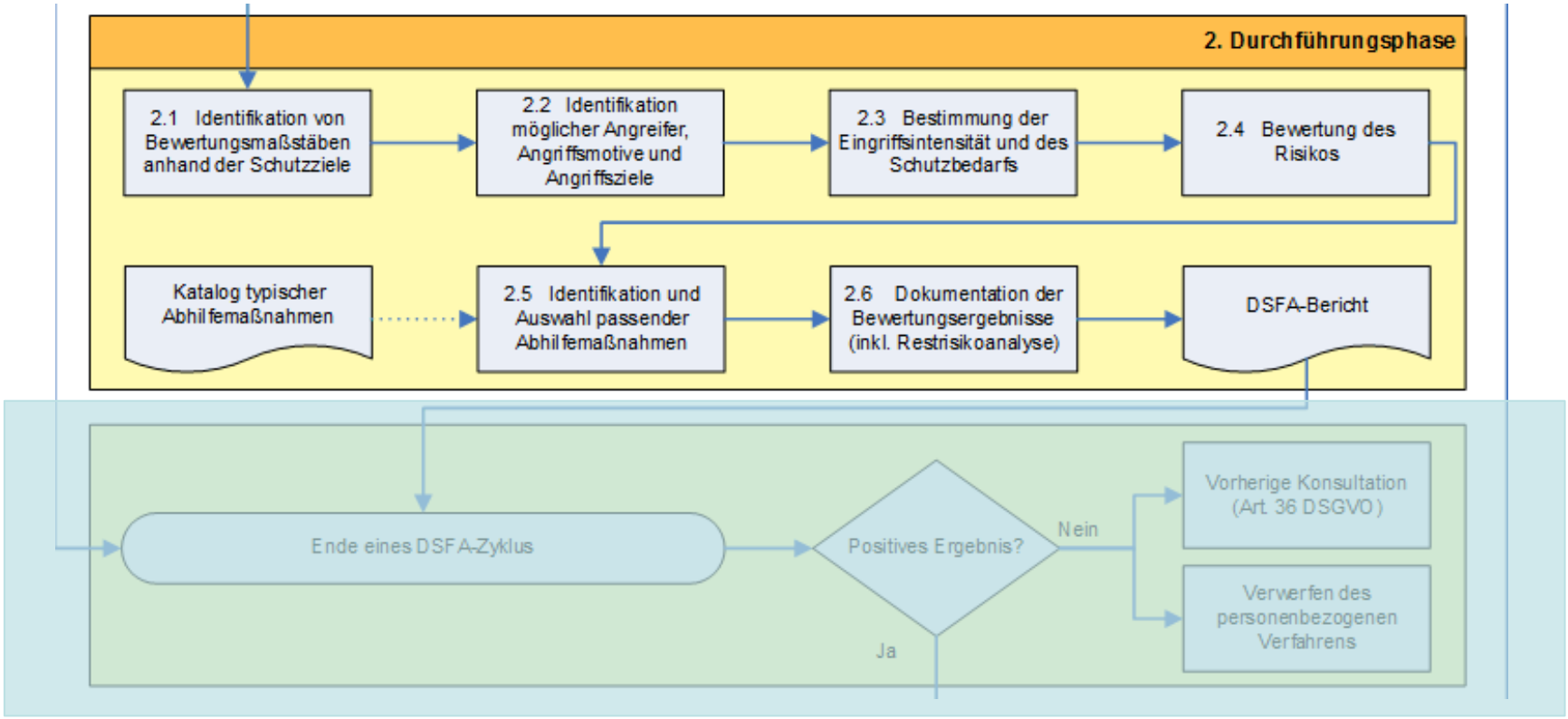
1.4 Identifikation der Akteure und betroffenen Personen

- Innerhalb und außerhalb der Organisation
- Hersteller, Betreiber, Dienstleister, Mitarbeiter, Dritte

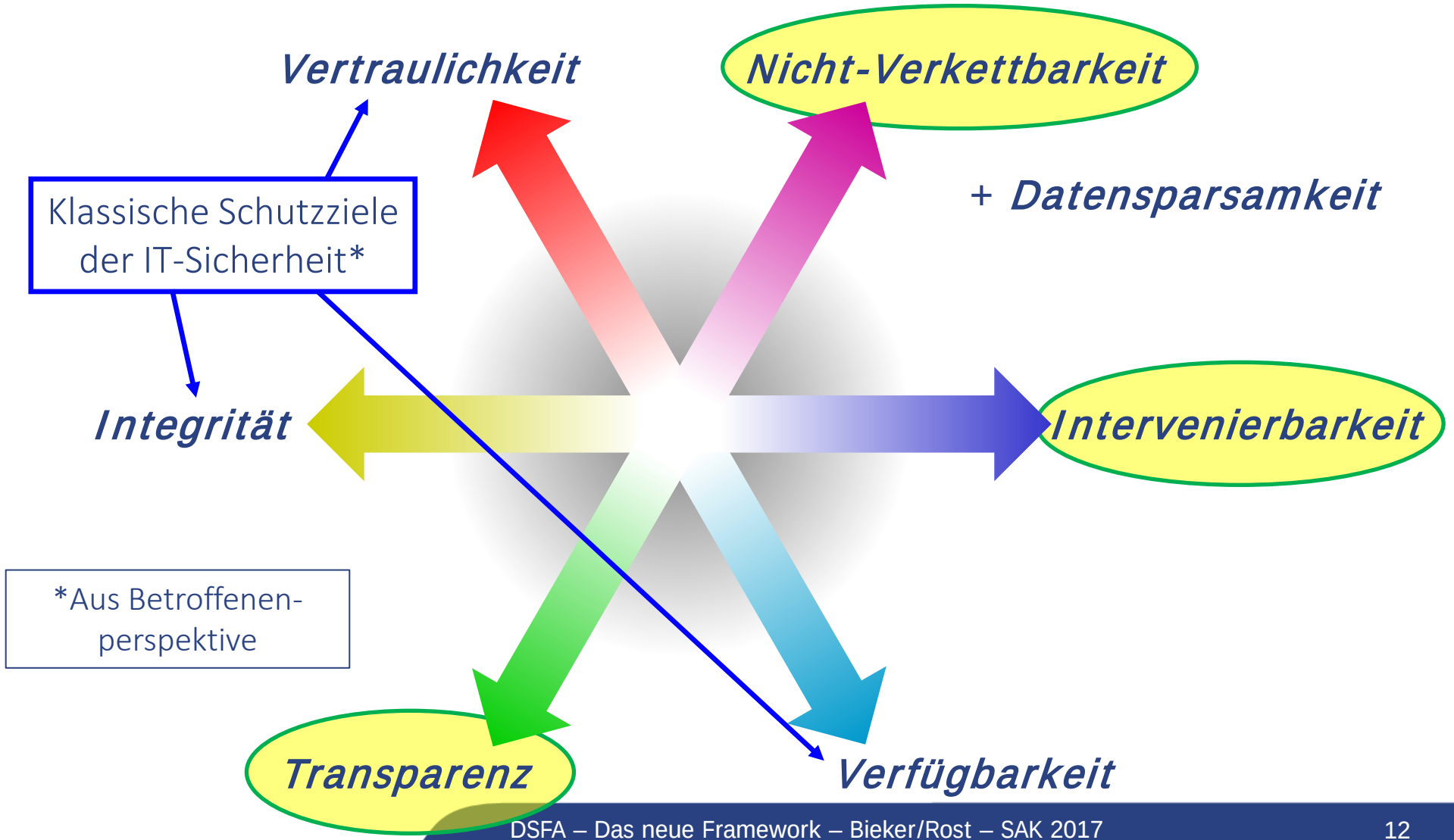
1.5 Identifikation der maßgeblichen Rechtsgrundlagen

- **Verbot mit Erlaubnisvorbehalt: Verarbeitung nur mit Rechtsgrundlage**
- Gesamte Datenverarbeitung muss rechtmäßig sein!

2. Durchführungsphase & Entscheidung



2.1 Identifikation der Bewertungsmaßstäbe



2.2 Identifikation möglicher Angreifer

- **Verantwortliche Stelle** ist immer der Hauptangreifer (Risikogeber). (erzeugt Grundrechtsbeeinträchtigung, bricht die informationelle Selbstbestimmung des Bürgers, des Kunden, des Patienten usw. und erzeugt durch die Datenverarbeitung die Risiken in Bezug auf die Informationssicherheit.)
- **Staatliche Stellen** (z.B. Sicherheitsbehörden: Innenministerien, Polizei, Geheimdienste, Militär etc. / staatliche Leistungsverwaltung: Leistungsträger für Arbeitslosengeld II („Hartz IV"), Rentenversicherungsträger etc. / Statistikämter / versagende Aufsichtsbehörden)
- **Unternehmen** (z.B. Technologiehersteller, Systemintegratoren, IT-Diensteanbieter (Zu-gang, Inhalte etc.) / Banken, Versicherungen / Wirtschaftsauskunfteien, Adress- und Daten-handel, Marktforschung / Werbung / Interessenvereinigungen, Verbände / Arbeitgeber)
- **Gesundheitswesen** (z.B. Krankenhäuser, Ärzte / gesetzliche und private Krankenversicherungen)
- **Forschung** (z.B. Medizinforschung, Sozialforschung, Universitäten)
- **Hacking** / Aspekte der IT-Sicherheit

2.3 Bestimmung der Eingriffsintensität und des Schutzbedarfs

Eingriff: Fremdbestimmung einer Person durch eine Organisation

Mangelnde Ordnungsmäßigkeit / Compliance der Organisation: Risiko, dass die Organisation (auch) nicht-legitime Zwecke verfolgt und/oder personenbezogene Daten zweckunbestimmt oder zwecküberdehnend verarbeitet.

Mangelnde IT-Sicherheit der Organisation: Risiko, dass unbefugte Dritte sich Zugriff auf ein Verfahren – auf Datenbestände, IT-Systeme oder Prozessen – verschaffen.

2.3 Bestimmung der Eingriffsintensität und des Schutzbedarfs

Bei der Definition des Schutzbedarfs ist grundsätzlich davon auszugehen, **dass jedes personenbezogene Verfahren mindestens normal aufweist**.

Ein **hoher Schutzbedarf** besteht, wenn

- die Eingriffsintensität hoch ist;
- der Betroffene von den Entscheidungen bzw. Leistungen einer Organisation abhängig ist;
- Daten verarbeitet werden, welche gesetzlich als besonders schutzwürdig ausgewiesen sind;
- keine real nachweislich funktionierenden Möglichkeiten der Intervention und des effektiven Selbstschutzes für Betroffene bereitstehen;
- die Organisation über nur unzureichende Schutzmaßnahmen der IT-Sicherheit verfügt bzw. keine Nachweise darüber erbringen kann;
- der Betroffene mit (ungeregelten) organisationsexternen zweckändernden Zugriffen rechnen muss.
- …

2.4 Bewertung des Risikos für Rechte und Freiheiten natürlicher Personen

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

2.5 Identifikation der Abhilfemaßnahmen

Referenzschutzmaßnahmen:

- Datensparsamkeit – Reduzierung von Daten/Personenbezug
- Verfügbarkeit – Redundanz, Backup
- Integrität – Authentisierung/Autorisierung, Signaturen, Hash-Wert-Vergleiche
- Vertraulichkeit - Verschlüsselung, Zugriffsschutz, Rollen- & Rechtekonzept
- Nichtverkettung – Pseudonymisierung/Anonymisierung von Datenbeständen und Kommunikationsbeziehungen, Trennung von Verfahren, Datenbeständen, IT-Systemen, Prozessen, Rollen & Rechtskonzept, Identitätsmanagement
- Transparenz – *Zweck*: Herstellen von Kontrollierbarkeit, Prüffähigkeit Beurteilbarkeit des Verfahrens und der Wirksamkeit der Maßnahmen! *Mittel*: Spezifikation, Dokumentation, Protokollierung des Verfahrens, Informationen bei Erhebung, Benachrichtigung bei Bearbeitung der Betroffenen (Beauskunften), Audits
- Intervenierbarkeit – Löschen, Sperren, Change Management, Aus-Schalter zum Deaktivieren/Stoppen von Gerätschaften

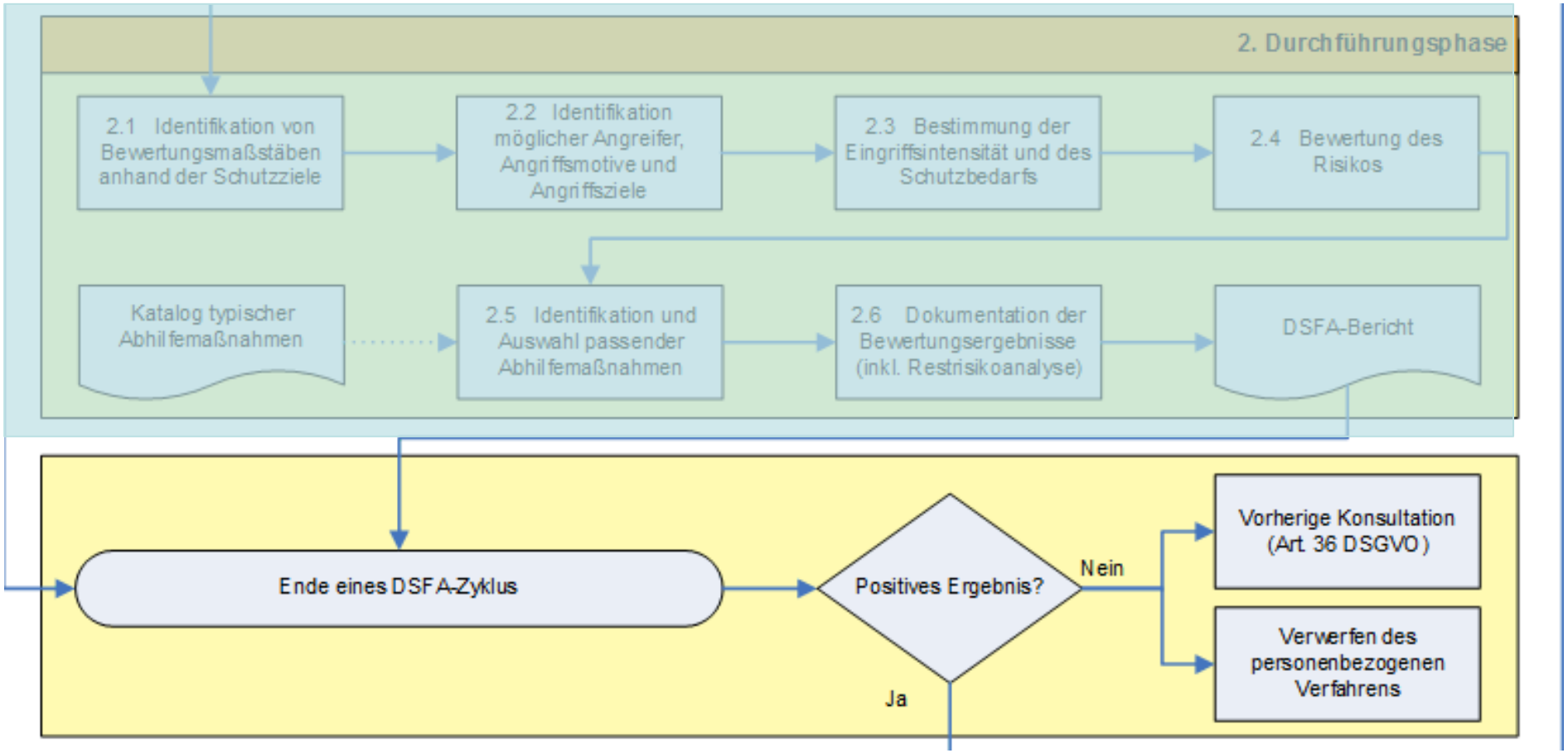
Standard-Datenschutzmodell

- Die DSB-Konferenz hat 11/2016 die SDM-Methodik im SDM-Handbuch (52 Seiten), Version 1.0 angenommen, Modell ist auf den Webseiten der deutschen Datenschutzaufsichtsbehörden publiziert.
- Kap. 7 des Handbuchs listet generische Maßnahmen auf, der konkretisierende Maßnahmenkatalog wird 2017 in Einzelbausteinen durch AK-Technik veröffentlicht.
- Normativ verankert in der DSGVO, methodische Anlehnung an IT-Grundschutz (SDM ersetzt DS-Baustein im IT-GS).
- Eine Englischübersetzung liegt der Artikel-29-Gruppe vor.
- Autorenteam umfasst ca. 8 Personen verschiedener Aufsichtsbehörden
- Betriebskonzept:
  - Erarbeiten neuer Bausteine bislang ausschließlich Datenschutzaufsichtsbehörden vorbehalten;
  - Kontrollierte Fortschreibung von Bausteinen

2.6 Dokumentation der Bewertungsergebnisse und DSFA-Bericht

- Wichtiger Teil der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)
- Dokumentiert vorherige Schritte (Mindestinhalt nach DSGVO) und ist Grundlage der Entscheidung über Datenverarbeitung
- Inklusive Restrisikoanalyse

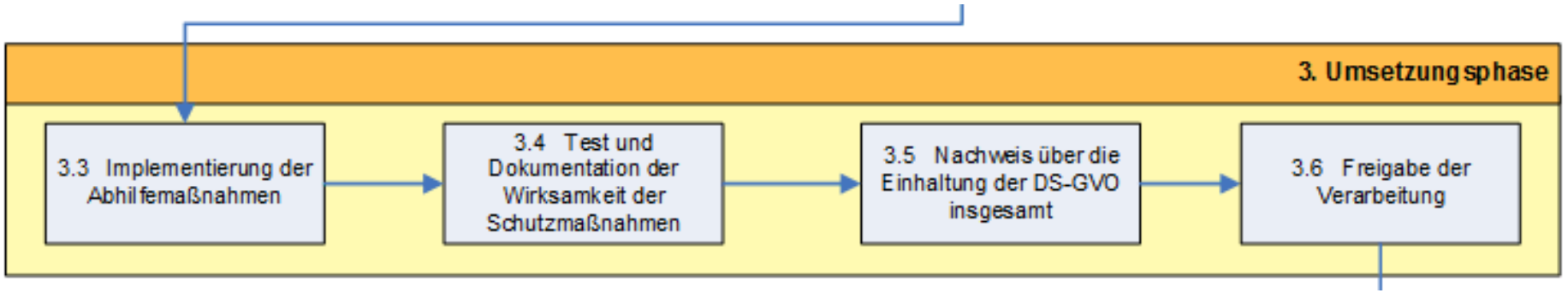
Entscheidung über Verfahren



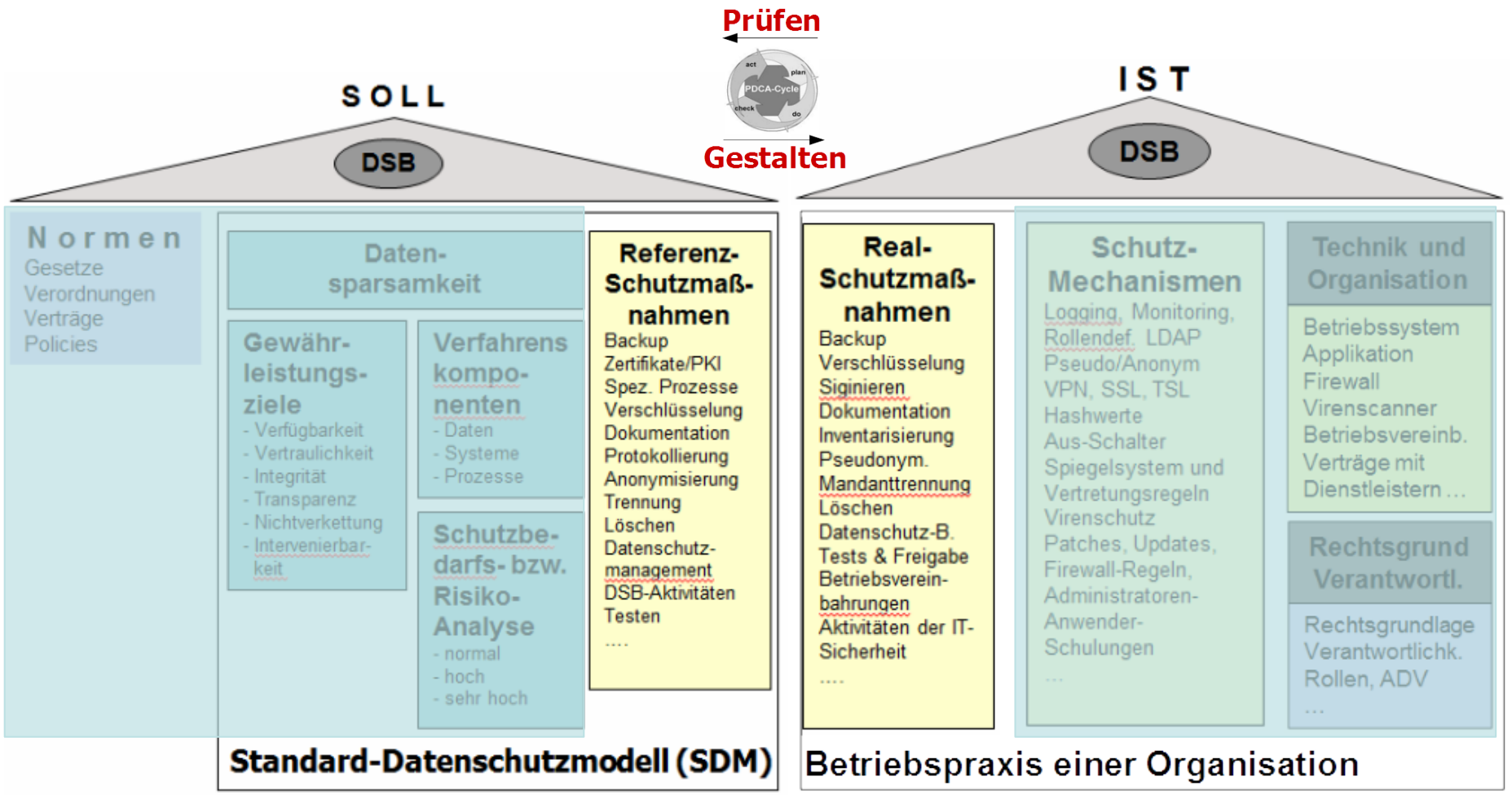
Entscheidung über Verfahren

- Hat DSFA ein positives Ergebnis erzielt?
  - Wenn nein:
    - Verwerfen des Verfahrens (keine Datenverarbeitung)
    - Weitere Abhilfemaßnahmen denkbar um Risiken zu verringern
    - Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO
  - Wenn ja: Umsetzung der Abhilfemaßnahmen

3. Umsetzungsphase



3.2 Implementierung



3.3 Test und Dokumentation

- **Testkonzept** für Funktionen und Schutzmaßnahmen entwickeln
- **Protokollierung** der Tests und die Freigabe der Tests
- Tests mit **Echtdaten** nur ganz zum Schluss und unter engen Bedingungen
- Eine **Pilotphase zählt bereits zum Echtbetrieb**, Pilotphasen müssen zeitlich begrenzt sein
- Dokumentation sollte auf den **Nachweis der Wirksamkeit** der Abhilfemaßnahmen abzielen (Nachweis muss der Verantwortliche nach Art. 35 Abs. 3 DSGVO beibringen)

3.4 Nachweis über die Einhaltung der DSGVO insgesamt, 3.5 Freigabe der Verarbeitung

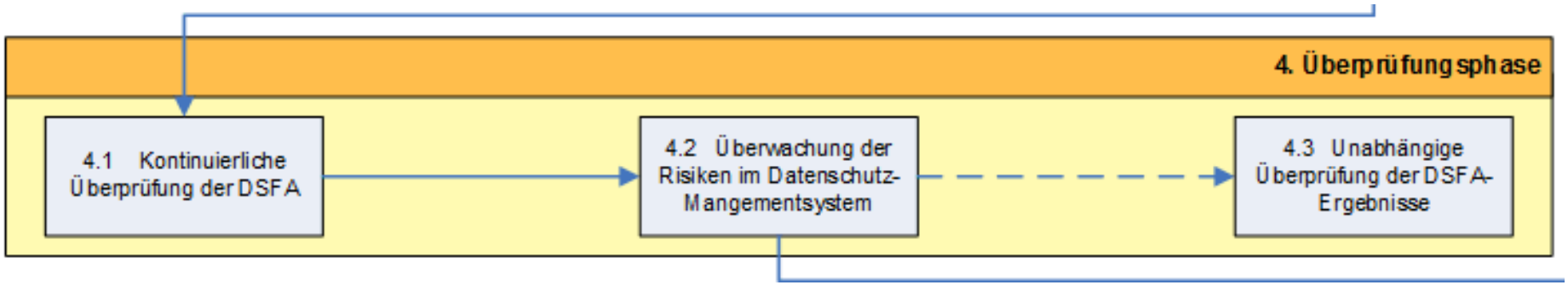
3.4 Nachweis

- Weitere Dokumentation als Teil der Rechenschaftspflicht (Art. 5 Abs. 3 DSGVO)
- Dokumentiert Umsetzung und bestätigt Wirksamkeit der Abhilfemaßnahmen
- Einhaltung der sonstigen Vorschriften der DSGVO

3.5 Freigabe

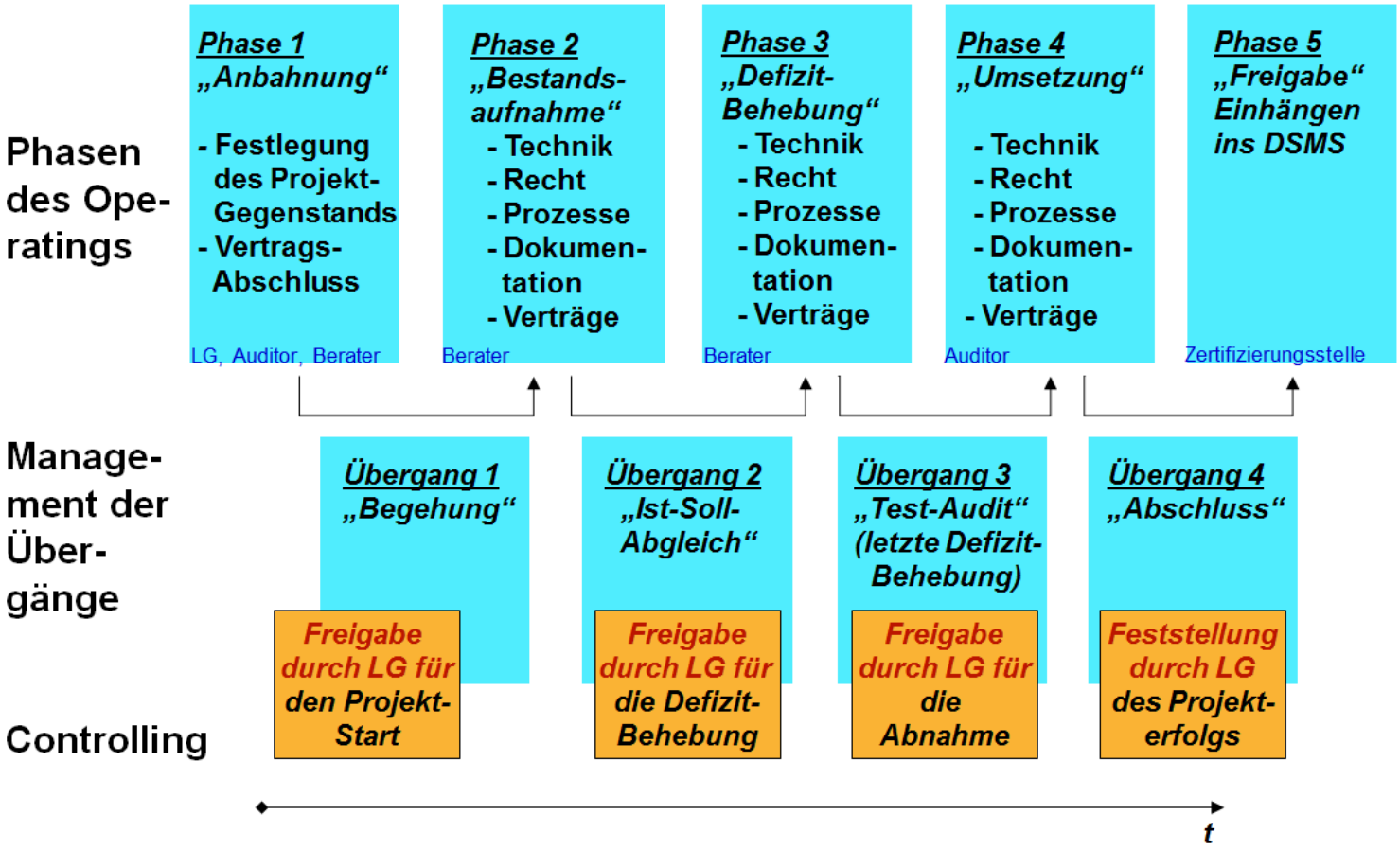
- Nach vollständiger Umsetzung der Abhilfemaßnahmen und Vorliegen der vollständigen Dokumentation kann Verantwortlicher das Verfahren offiziell freigeben

4. Überprüfungsphase



4.1 Kontinuierliche Überprüfung der DSFA

Entspricht weitgehend der Forderung nach einem Projektmanagement für eine DSFA

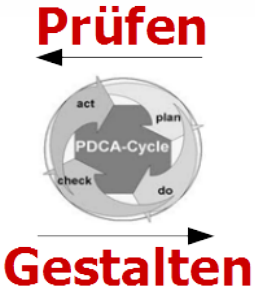


4.2 Überwachung der Risiken im DSMS

Welche spezifischen Datenschutzrisiken erzeugt ein Verfahren?

1. *Spezifisches Risiko für den Betroffenen*
   Die Intensität des **Grundrechtseingriffs** durch ein Verfahren wurde nicht ausreichend gemildert, bspw. durch ein schlechtes Verfahrensdesign und durch fehlende oder falsch implementierte und betriebene Technik und Abhilfemaßnahmen.
2. *Spezifisches Risiko für die Organisation*
   Das Verfahren ist nicht legitim oder die Rechtsgrundlage zur Überwindung des Verbots mit Erlaubnisvorbehalt reicht nicht aus (**Compliance-Risiko**).
3. Risiko *sowohl für den Betroffenen als auch die Organisation*
   Die Schutzmaßnahmen der **IT-Sicherheit** reichen nicht aus.

4.2 Überwachung der Risiken im DSMS



SOLL

DSB

Normen
Gesetze
Verordnungen
Verträge
Policies

Daten-sparsamkeit

Gewähr-leistungs-ziele
- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Transparenz
- Nichtverkettung
- Intervenierbar-keit

Verfahrens kompo-nenten
- Daten
- Systeme
- Prozesse

Schutzbe-darfs- bzw. Risiko-Analyse
- normal
- hoch
- sehr hoch

Referenz-Schutzmaß-nahmen
Backup
Zertifikate/PKI
Spez. Prozesse
Verschlüsselung
Dokumentation
Protokollierung
Anonymisierung
Trennung
Löschen
Datenschutz-management
DSB-Aktivitäten
Testen
....

Standard-Datenschutzmodell (SDM)

IST

DSB

Real-Schutzmaß-nahmen
Backup
Verschlüsselung
Signieren
Dokumentation
Inventarisierung
Pseudonym.
Mandanttrennung
Löschen
Datenschutz-B.
Tests & Freigabe
Betriebsverein-bahrungen
Aktivitäten der IT-Sicherheit
....

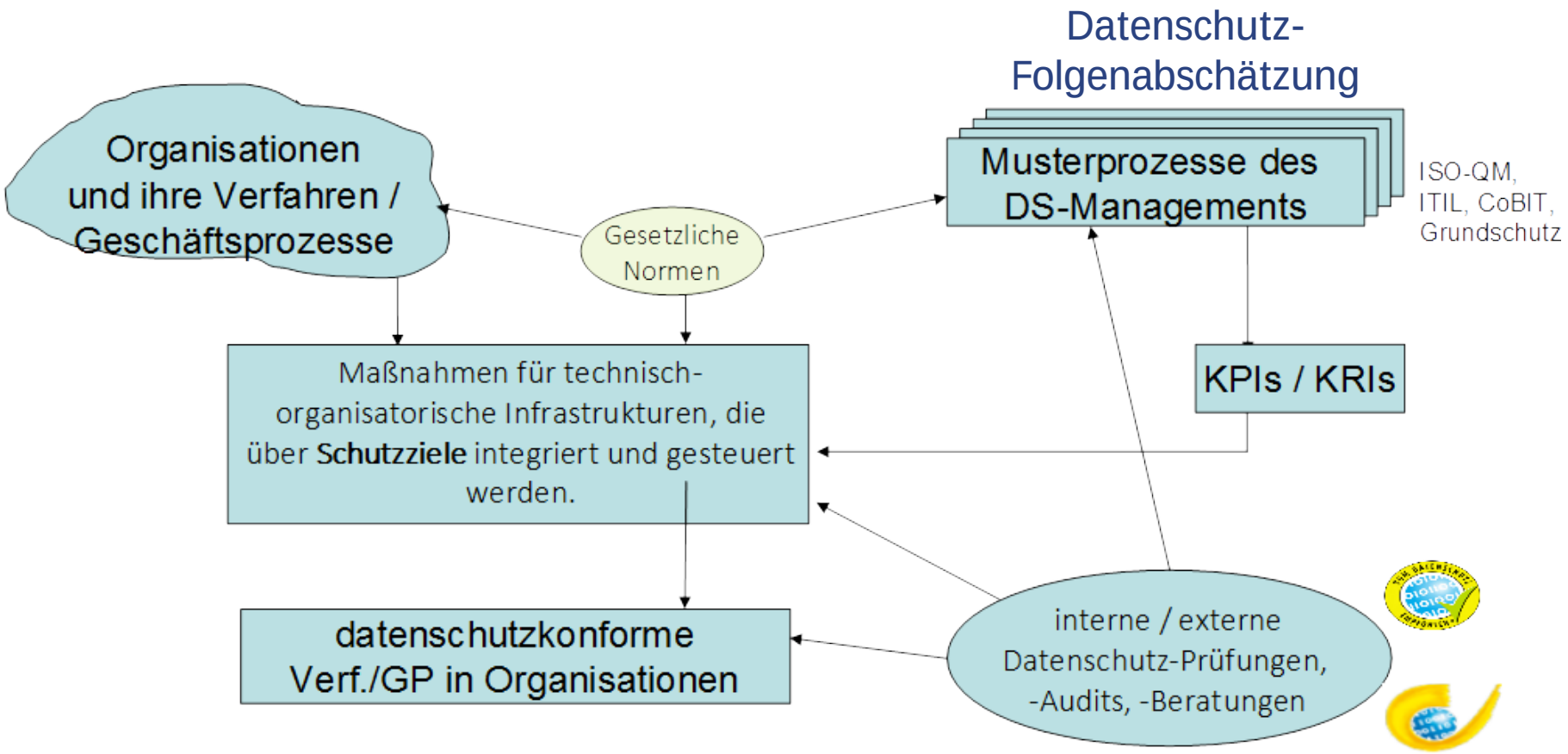
Schutz-Mechanismen
Logging, Monitoring, Rollendef. LDAP
Pseudo/Anonym
VPN, SSL, TSL
Hashwerte
Aus-Schalter
Spiegelsystem und Vertretungsregeln
Virenschutz
Patches, Updates, Firewall-Regeln, Administratoren-Anwender-Schulungen
...

Technik und Organisation
Betriebssystem
Applikation
Firewall
Virenscanner
Betriebsvereinb.
Verträge mit Dienstleistern ...

Rechtsgrund Verantwortl.
Rechtsgrundlage
Verantwortlichk.
Rollen, ADV
...

Betriebspraxis einer Organisation

4.2 Überwachung der Risiken im DSMS



4.3 Unabhängige Überprüfung der DSFA-Ergebnisse

- Überprüfung durch unabhängigen Dritten
- Am besten in Form eines Audits

Literatur

- Forum Privatheit: White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz
  https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php
- AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung
  https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_0.pdf
- Bieker/Hansen/Friedewald: Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, Recht der Datenverarbeitung (RDV) 2016, S. 188

Vielen Dank für die Aufmerksamkeit!

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Felix Bieker – uld63@datenschutzzentrum.de
Martin Rost – uld32@datenschutzzentrum.de
Telefon: 0431 988 – 1200
http://www.datenschutzzentrum.de/