Foto: Ian Burt

Datenschutz-Folgenabschätzung
- ein neues Instrument der EU-DS-GVO

Martin Rost

19.09.2016, Kiel

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

Grundgesetz

Artikel 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

EU-Grundrechte-Charta

Artikel 1 - Würde des Menschen

Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.

Artikel 8 - Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf *Schutz der sie betreffenden personenbezogenen Daten.*

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit *Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage* verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer *unabhängigen Stelle überwacht.*

Schicksal des nationalen Datenschutzrechts

- **Regelfall: Rechtgrundlagen des BDSG und Landesdatenschutz sind obsolet** (soeben veröffentlicht: Entwurf eines BDSG-Übergangsgesetzes)
- Ausnahmen
  - Gesetzliche Regeln für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, Art. 2 Abs. 2 DSGVO
    - Selbstorganisation des Staates
    - Sozialdatenschutz (?)
    - Justiz und Rechtpflege
  - Außen- und Sicherheitspolitik
  - staatliche Gefahrenabwehr und Strafverfolgung (Art. 2 Abs. 2 DSGVO)
  - Öffnungsklauseln
  - Ergänzungen/Konkretisierungen durch delegierte Rechtsakte der Kommission

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

Art. 5 DS-GVO

„Grundsätze für die Verarbeitung personenbezogener Daten“ (I)

„(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; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („**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**“);“*

„Grundsätze für die Verarbeitung personenbezogener Daten“ (II)

*„(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 Absatz 1 verarbeitet werden („Speicherbegrenzung“);*

*f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);*

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

DS-GVO und Schutzziele in Art. 5: Essentials

Art. 5 Abs. 1 „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) „... **Integrität und Vertraulichkeit**“.

Es fehlt: **Verfügbarkeit** ?

Schutzziele:

- **Transparenz** ✓
- **Nicht-Verkettbarkeit** ✓
- **Datensparsamkeit** ✓
- **Intervenierbarkeit** ✓
- **Integrität** ✓
- **Vertraulichkeit** ✓

Art. 25 DS-GVO

„Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“

„(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. (...)“*

Proaktiver Datenschutz, heisst:

- Spezifikation eines Verfahrens im Hinblick auf Umsetzung der *Datenschutzgrundsätze* => *Art 5 DS-GVO*
- Privacy-By-Design

Art. 32 DS-GVO

„Sicherheit der Verarbeitung“ - Schutzziele

(...), diese Maßnahmen schließen unter anderem Folgendes ein:

*a) die **Pseudonymisierung und Verschlüsselung** personenbezogener Daten;*

*b) die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzustellen**;*

*c) die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

- „Sicherheit der Verarbeitung“ MUSS in einem Datenschutzgesetz primär dem Betroffenen gelten... allerdings ist vielfach unklar, ob der Konflikt „Schutz von Geschäftsprozessen“ vs. „Schutz von Betroffenen“ den Gesetzesautoren hinreichend klar vor Augen stand.
- Weitere Bestätigung der Schutzziele. Meint „Belastbarkeit“ mehr als „gesicherte Verfügbarkeit“?
- Warum solche Redundanzen wie
  a) Verschlüsselung der Daten (konkret)
  b) Sicherstellung der Vertraulichkeit von Systemen (abstrakt)?

Art. 32 DS-GVO „Verfahren zur Prüfung“

*d) **ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.*

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

- Regelmäßige *Überprüfung der Wirksamkeit von TOMen* → Datenschutz-Managementsystem
- Welche „Verfahren“ zur „Überprüfung, Bewertung, Evaluierung“ der Datenschutz-Wirksamkeit stehen zur Verfügung? Das leisten bspw. weder ISO27001(ISMS), 29100(PrivFrame) oder DIN-Verfahren oder IT-Grundschutz des BSI.

Abs. 3: „Die Rolle von Verbandsregelungen oder Zertifizierungen“

*(3) Die Einhaltung **genehmigter Verhaltensregeln** gemäß Artikel 40 oder eines **genehmigten Zertifizierungsverfahrens** gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*

Artikel 40 DS-GVO „Verhaltensregeln“ (I)

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die ***Ausarbeitung von Verhaltensregeln****, die nach Maßgabe der* ***Besonderheiten der einzelnen Verarbeitungs-bereiche*** *und der* ***besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung*** *beitragen sollen.*

(2) ***Verbände*** *und andere Vereinigungen, die Kategorien von Verant-wortlichen oder Auftragsverarbeitern vertreten****, können Verhaltens-regeln ausarbeiten*** *oder ändern oder erweitern,* ***mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird****:*

a) ***faire und transparente Verarbeitung****;*

b) ***die berechtigten Interessen des Verantwortlichen*** *in bestimmten Zusammenhängen;*

c) ***Erhebung personenbezogener Daten****;*

Interessensverbände sollen Regelungen treffen können bzgl. bspw. Fairness und Transparenz..

„…berechtigte Interessen des Verantwortlichen in bestimmten Zusammen-hängen“… man fragt sich: Wie kommen solche Anfor-derungen“ in ein Gesetz?

Artikel 40 DS-GVO „Verhaltensregeln“ (II)

*d) **Pseudonymisierung personenbezogener Daten**;*
*e) **Unterrichtung der Öffentlichkeit und der betroffenen Personen**;*
*f) **Ausübung der Rechte betroffener Personen**;*
g) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
*h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die **Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32**;*
i) die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;
*j) **die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen** oder*
*k) **außergerichtliche Verfahren und sonstige Streitbeilegungsverfahren** zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln 77 und 79.*

…. Pseudonymisierung, Ausübung Betroffenen-rechte, Sicherheitsmaß-nahmen, Übermittlung in Drittländer oder internatio-nale Organisationen...

Artikel 40 DS-GVO „Verhaltensregeln“ (III)

*(5) **Verbände** und andere Vereinigungen gemäß Absatz 2 des vorliegenden Artikels, die beabsichtigen, Verhaltensregeln auszuarbeiten oder bestehende Verhaltensregeln zu ändern oder zu erweitern, **legen den Entwurf** der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung **der Aufsichtsbehörde vor**, die nach Artikel 55 zuständig ist. **Die Aufsichtsbehörde gibt eine Stellungnahme darüber ab**, ob der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist und genehmigt diesen Entwurf der Verhaltensregeln bzw. den Entwurf zu deren Änderung oder Erweiterung, wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien bietet.*

…. Aufsichtsbehörde gibt Stellungnahme ab … und genehmigt den Entwurf, falls er hinreicht.

Artikel 40 DS-GVO „Verhaltensregeln“ (IV)

*(6) **Wird durch die Stellungnahme nach Absatz 5 der Entwurf der Verhaltensregeln bzw. der Entwurf zu deren Änderung oder Erweiterung genehmigt** und beziehen sich die betreffenden Verhaltensregeln nicht auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so nimmt **die Aufsichtsbehörde die Verhaltensregeln in ein Verzeichnis auf und veröffentlicht sie**.*

*(9) **Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass die ihr gemäß Absatz 8 übermittelten genehmigten Verhaltensregeln bzw. deren genehmigte Änderung oder Erweiterung allgemeine Gültigkeit in der Union besitzen.** Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.“*

Die zuständige Aufsichtsbehörde führt ein öffentliches Verzeichnis über genehmigte Verfahren, die Kommission kann derart taxierte Verfahren dann für Europa übernehmen.

Art. 32 DS-GVO
Abs. 4: ADV-Aktivitäten nur auf Anweisung

*(4) **Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten**, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.“*

Verantwortlicher und Auftragsverarbeiter „unternehmen Schritte, um sicherzustellen“ - sie sind offenbar nicht darauf verpflichtet sicherzustellen, sondern nur Schritte zu unternehmen? Das ist eine Abschwächung!

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

Was meint Datenschutz-Folgenabschätzung?

1. Wortwahl: Datenschutz-Folgenabschätzung (DSFA) meint
Nicht: Abschätzen der Folgen, die durch Datenschutz entstehen!
Sondern: Abschätzung der Folgen eines Verfahrens aus Datenschutz-Perspektive!
1. Keine TFA: Im Fokus stehen auch nicht Folgen aus einer Technik, sondern die Eingriffsintensität eines Verfahren, in dem eine neue Technik eingesetzt wird.
2. DSFA ist ein Instrument, um in Verfahren oder Systemen die Risiken für Betroffene, die von Organisationen durch Nutzung von Verfahren ausgehen, zu erkennen und zu beurteilen.
3. Eine DSFA bildet dabei die Basis zum Bestimmen (noch nicht unbedingt: zur Durchsetzung) von Gegenmaßnahmen.

DSFA Art. 35 Abs. 1 Relevanzschwelle

*„(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.“*

- Trigger für eine DSFA ist „Form der Verarbeitung“, nicht: „neue Technologie“ (keine TFA!)
- „hohes Risiko“ = **starker Grundrechtseingriff** bei Bürgern, Kunden oder Patienten, nicht jedoch Risikokalküle oder Schäden, die dem Einzelnen entstehen könnten.
- Leitung ist für die Durchführung einer Vorab-Abschätzung einer DSFA verantwortlich, ob sie überhaupt durchzuführen ist.

DSFA Art. 35 Abs. 2
Rolle des Datenschutzbeauftragten

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

Eine übliche Formulierung wäre:
Der DSB ist zu beteiligen.
(was könnte dem DSB außer abzuwarten bleiben: Übernahme des Projektmanagements für DSFA? Oder das genau nicht, sondern nur Ratschläge im Lenkungskreis des Projekts erteilen?)

DSFA Art. 35 Abs. 3 „besondere Verfahren“

„(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 ein-schließlich Profiling*** *gründet und die ihrerseits* ***als Grundlage für Entschei-dungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten*** *oder diese in ähnlich erheblicher Weise beeinträchtigen;“*

Umfasst

- Scoring,
- Profiling,
- automatisierte Einzelentscheidungen.

DSFA Art. 35 Abs. 3 „besondere Daten“

„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.“*

Artikel 9 DS-GVO – Verarbeitung besonderer Kategorien personenbezogener Daten
(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.*

Geläufig aus § 3 Abs. 9 BDSG:
„Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.“

Ergänzt um „genetische Daten“

DSFA Art. 35 Abs. 3c „besonderes Verfahren“

„c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.“

Videoüberwachung (auch Drohnen)

DSFA Art. 35 Abs. 4
Liste der DSFA-Verfahren

„(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.“

Datenschutzaufsichtsbehörden müssen eine Liste für Verfahren erstellen, für die eine DSFA obligatorisch ist.

DSFA Art. 35 Abs. 5
Liste für Nicht-DSFA-Verfahren

„(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.“

Datenschutzaufsichtsbehörden listen Verfahren, für die **keine DSFA** notwendig ist.

DSFA Art. 35 Abs. 6 Kohärenzverfahren für Listen

„(6) ***Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63*** *an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder* ***die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen*** *könnten.“*

- Für beide Listen gilt Kohärenzverfahren → hohe Abstimmungsvoraussetzungen
- DSFA nur einmal durchzuführen, dann genehmigt für die gesamte internationale Prozesskette.
- „Freier Verkehr pers. bez. Daten“ ist mit Datenschutzrecht nicht vereinbar, es immer nur „konditionierter Verkehr pers. bez. Daten“ denkbar.

DSFA Art. 35 Abs. 7a Dokuanforderungen

„(7) Die Folgenabschätzung enthält zumindest Folgendes:

*a) eine **systematische Beschreibung** der **geplanten Verarbeitungsvorgänge** und **der Zwecke der Verarbeitung**, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten **berechtigten Interessen**;“*

Transparenz eines Verfahrens durch

- systematische Dokumentation der Spezifikation
- die Zwecke (Plural!) der spezifizierten Verarbeitung
- Ausweis der Interessen der verantwortlichen Stelle (Wer stellt die Berechtigung fest?)

DSFA Art. 35 Abs. 7b

Bewertung der Notwendigkeit und Verhältnismäßigkeit

*„b) eine **Bewertung** der **Notwendigkeit** und **Verhältnismäßigkeit** der Verarbeitungsvorgänge in **Bezug auf den Zweck**;“*

Juristische Begründung für das Verfahren

DSFA Art. 35 Abs. 7c
Bewertung von Risiken

*„c) eine **Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen** gemäß Absatz 1 und“*

- „Bewertung von Risiken“ ist eigens benannt und könnte durchaus ökonomisch gemeint sein. Aus Datenschutzsicht müssen Risiken dagegen **beurteilt** werden.
- Anstatt die Risiken für Personen wären für eine DSFA die Motive, Möglichkeiten und Aktivitäten der Organisationen als Angreifer in den Blick zu nehmen, die ein Verfahren und neue Techniken nutzen können wollen, um davon abgeleitet die Risiken der Eingriffe in die Grundrechte von Personen zu beurteilen.

DSFA Art. 35 Abs. 7d Maßnahmen

*„d) die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und **der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird**, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“*

Zu den **geplanten Abhilfemaßnahmen** und Nachweis der Ordnungsmäßigkeit sollen zählen:

- Garantien (Prüfsiegel)
- technische Sicherheitsfunktionen
- organisatorische Regelungen
- Transparenzanforderung: Diese geplanten Maßnahmen müssen von vornherein so spezifiziert werden, dass die beabsichtigte Wirksamkeit dokumentiert werden kann -> hohe Anforderungen an Protokollierung!

DSFA Art. 35 Abs. 8
Bedeutung verbandseigener Regelungen

„(8) Die Einhaltung ***genehmigter Verhaltensregeln gemäß Artikel 40*** *durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung,* ***gebührend zu berücksichtigen****.“*

Die Macht der Interessensverbände wird durch §40 gegenüber den Aufsichtsbehörden massiv gestärkt. Verbandseigene Ausarbeitungen sollen eine **Bindungswirkung** auf die Aufsichtspraxis durch Aufsichtsbehörden entfalten. Das kann absehbar wiederum eine weitere Stärkung bspw. der Bedeutung von DIN/ISO-Aktivitäten im Bereich der Grundrechtswahrung bedeuten, obwohl diese keinerlei Orientierung an Grundrechten und deren Operationalisierung durch Datenschutz aufweisen.

DSFA Art. 35 Abs. 9 Folgenabschätzung

*„(9) Der Verantwortliche holt gegebenenfalls den **Standpunkt der betroffenen Personen oder ihrer Vertreter** zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.“*

DSFA Art. 35 Abs. 10

„(10) ***Falls die Verarbeitung*** *gemäß Artikel 6 Absatz 1 Buchstabe c oder e* ***auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats****, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln* ***und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte****, gelten die* ***Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist,*** *vor den betreffenden Verarbeitungstätigkeiten* ***eine solche Folgenabschätzung durchzuführen.****“*

Folge?

Wenn irgendwo in EU-Land bereits eine DSFA zu einem Verfahren durchgeführt wurde, muss keine weitere DFSA durchgeführt werden.

Datenschutz-Folgenabschätzung, Art. 35 Abs. 11

„(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ***ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durch-geführt wird****; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.“*

- Ein Verfahren ist nach der Implementation zu überprüfen, und zwar am Maßstab der bereits durchgeführten DSFA!
- Wenn das Verfahren geändert wurde, muss eine Überprüfung durchgeführt werden.

DSFA
Art. 35 DS-GVO, Resümee

1. **Eine Datenschutz-Folgenabschätzung ist grundsätzlich durchzuführen**:
   - wenn auf DSFA-Liste der Aufsichtsbehörden notiert
   - bei „hohem Risiko“
   - bei besonderen Verfahren: Scoring, Profiling, automatisiertem Einzelentscheid, Videoüberwachung;
   - bei besonderen Daten: Rasse/ Ethnie, pol./rel./phil. Meinung oder Zugehörigkeit, Gewerkschafts-zugehörigkeit, Gen-, Biometrie- Gesundheitsdaten, Sexualleben
2. **Trotz hohen Risikos muss keine DSFA erfolgen wenn**
   - wenn auf der Nicht-DSFA-Liste der Aufsichtsbehörden notiert
   - irgendwo in EU-Land eine DSFA bereits erfolgte
3. **Bestandteile** einer DSFA:
   - Beschreibung des Verfahrens, der Zwecke, der berechtigten Interessen sowie eine Bewertung der Notwendigkeit der DV, der Verhältnismäßigkeit und der Risiken für Betroffene;
   - Beschreibung der geplanten Schutzmaßnahmen inkl. Nachweis über deren Wirksamkeit;
   - Extern auditierte Verfahren und Audits sind zu berücksichtigen
   - Standpunkte der Betroffenen ist einzuholen;
4. Der **Datenschutzbeauftragte** ist nicht verantwortlich, auch keine abschließende Beurteilung
5. Der **Verantwortliche** muss Wirksamkeit der Schutzmaßnahmen des Verfahrens prüfen.

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

Überblick Standard-Datenschutzmodell

heise online > News > 2015 > KW 40 > Datenschützer verabschieden neues Prüfmodell

« Vorige | Nächste »

Datenschützer verabschieden neues Prüfmodell

heise online 01.10.2015 14:13 Uhr – Christiane Schulzki-Haddouti vorlesen

(Bild: BSI)

Die Datenschutz-Aufsichtsbehörden von Bund und Ländern empfehlen, das Standard-Datenschutzmodell anzuwenden. Dieses unterstützt ein strukturiertes Prüfen von IT-Prozessen, was bisher mangels eines eigenen Prüfmodells nicht möglich war.

- Regelungskern: 7 Schutzziele
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- 3 Schutzbedarfsabstufungen, formuliert aus Betroffenenperspektive
- Referenzkatalog mit Schutzmaßnahmen
- Die DSB-Konfererenz SDM-Handbuch (V0.9 / Oktober 2015) angenommen, auf den Webseiten der deutschen Datenschutzaufsichtsbehörden publiziert.
- Auf der DSB-Konferenz im November soll V1.0 (mit Referenz-Maßnahmenkatalog) erscheinen.

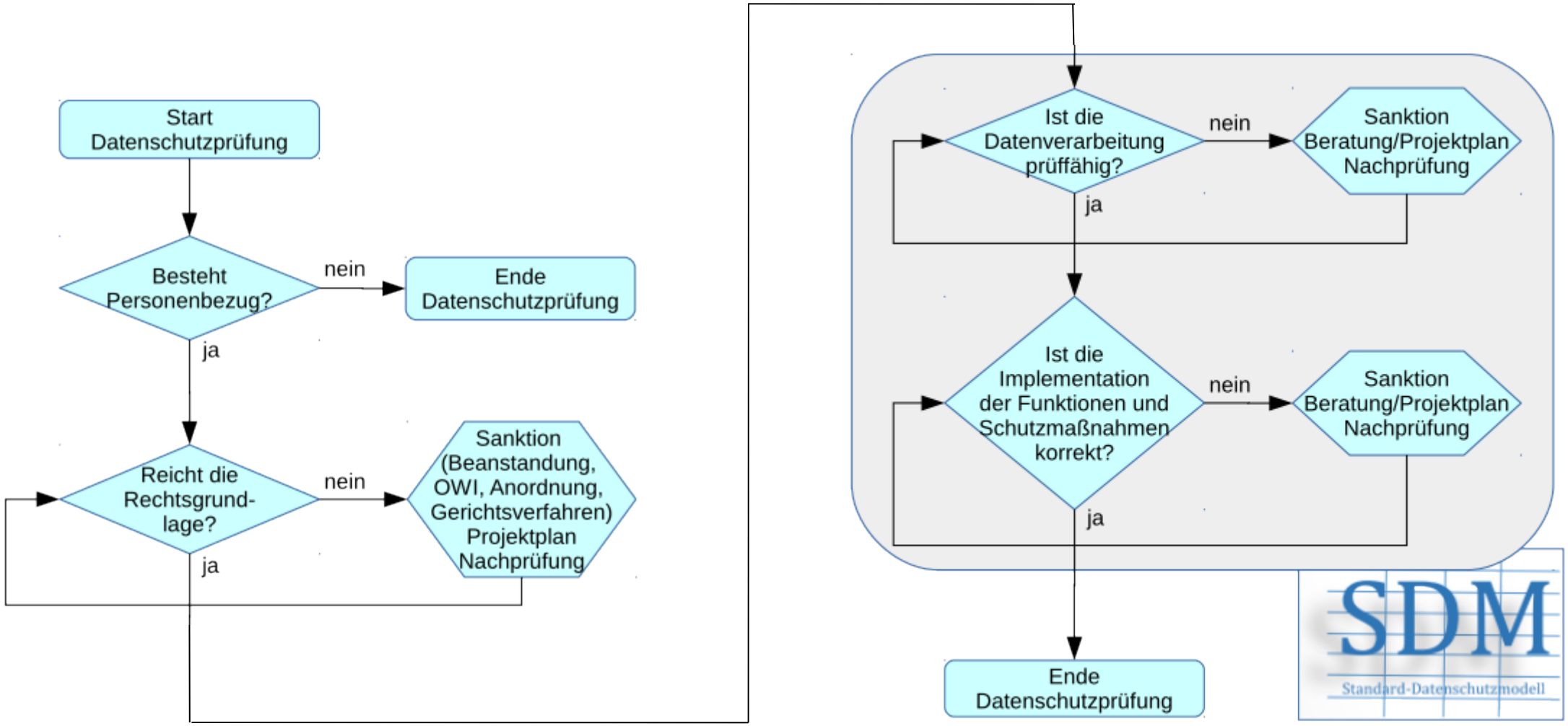
Mapping
SDM-Schutzziele und DS-GVO

Schutz-ziele:	Datenspar-samkeit	Verfügbar-keit	Integrität	Vertraulich-keit	Nichtver-kettbarkeit	Transparenz	Intervenier-barkeit
Artikel der DS-GVO:	5c/e, 25	13, 15, 20, 25, 32	5d,f, 25, 32	5f, 25, 28/3b, 32	5b, 25, 32	5a, 12, 13, 14, 15, 25, 32, 33, 34	12/2, 15e, 16, 17, 18, 19, 20, 21, 22/3, 25, 28/3g

Referenzkatalog mit Schutzmaßnahmen (aktuell in Entwicklung)

* **Datensparsamkeit** / Reduzierung erfasstet Attribute betroffener Personen und der Verarbeitungsoptionen / Reduzierung der Möglichkeiten der Kenntnisnahme vorhandener Daten
* **Verfügbarkeit** / Redundanz, *Backup* und Restore / *Vertretungsregeln*
* **Integrität** / technischer Integritätsschutz (elektronische Signaturen und deren Prüfungen) / Soll-Definitionen für Prozesse, mit Ereignisdefinitionen zur Prüfbarkeit von Soll-Abweichungen
* **Vertraulichkeit** / *Verschlüsselung* von Datenbeständen und Kommunikationen / Beerechtigungen- & Rollenkonzept
* **Nichtverkettbarkeit** / Trennung / *Isolierung* unter der inhaltlichen Maßgabe der Umsetzung informationeller Gewaltenteilung / *Anonymisierung* / Pseudonymisierung
* **Transparenz** / *Spezifikation* von geplanten Systemen / *Dokumentation*, die eine Prüffähigkeit von Ist-Zuständen und Soll-Vorgaben erlaubt / *Protokollierung* von Prozess-Ereignissen / Auskunft
* **Intervenierbarkeit** / Berichtigung, Sperrung, Löschung, Widerspruch („Außenschnittstelle“ einer Organisation) / Prozesse einer Organisation zur Erkennung und Bearbeitungen von Störungen, Problembearbeitungen und Änderungen („*Changemanagement*“)

Prüfablauf Datenschutz

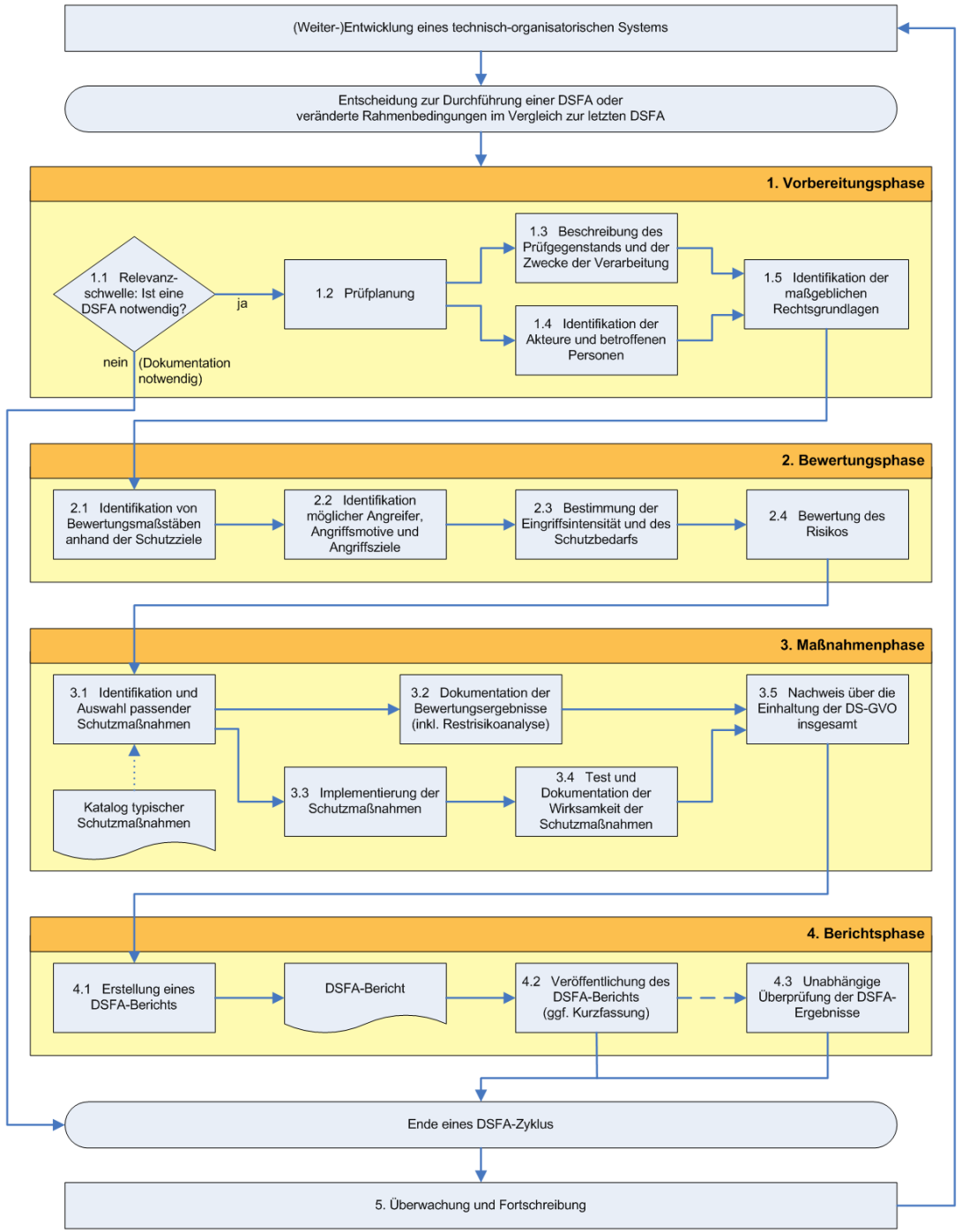


Agenda

1. Die Verankerung der DS-GVO in der EU-Grundrechte-Charta
2. Die zentralen TO-Maßnahmen der DS-GVO: Art. 5, 25, 32
3. Datenschutzfolgen-Abschätzung (DSFA) gemäß Art. 35
4. DS-GVO und Standard-Datenschutzmodell (SDM)
5. Standardisierter DSFA-Prozess
6. Hochzeit DSFA mit SDM

DSFA-Standardprozess

(Bieker / Hansen / Friedewald 2016)



Vier Phasen der DSFA:

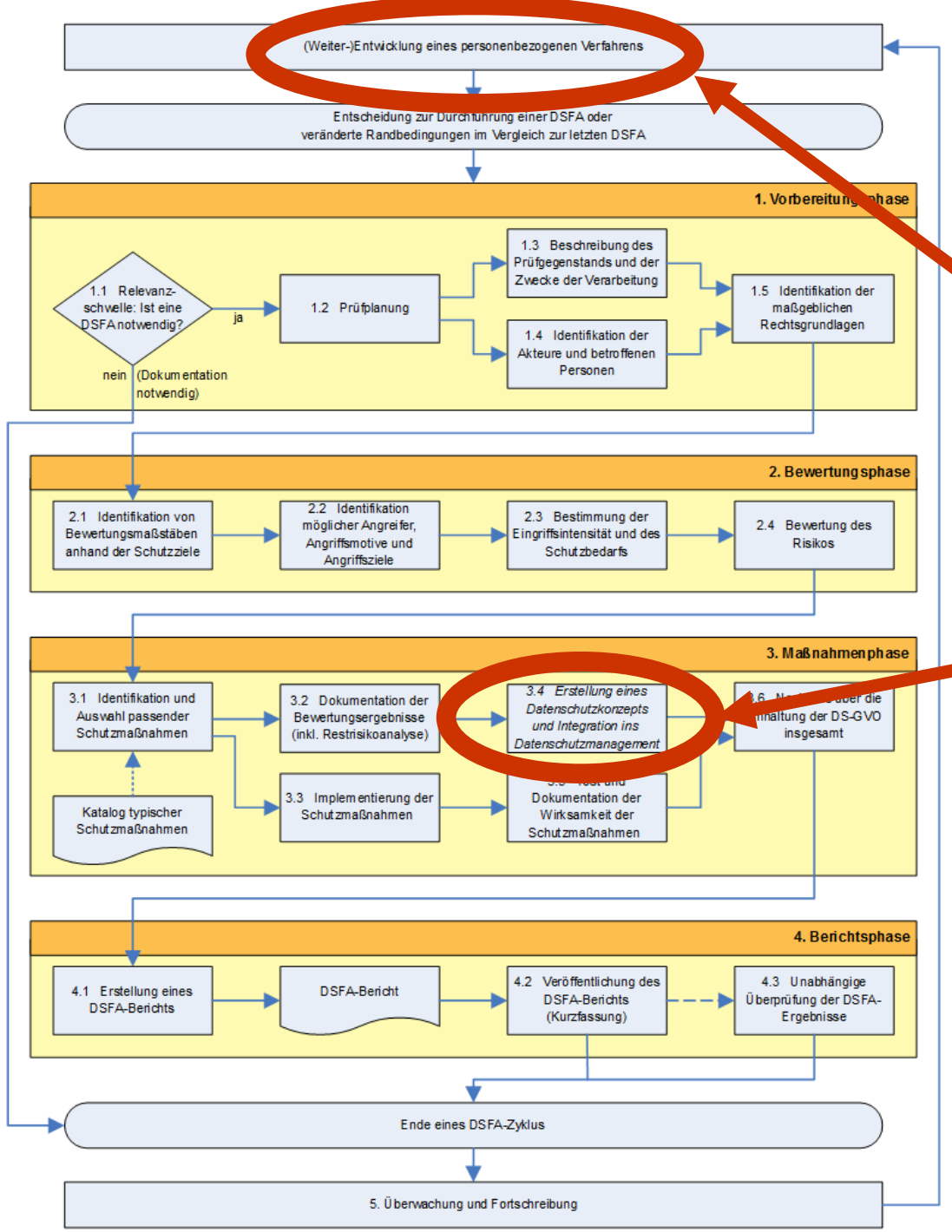
1. Vorbereitung
2. Bewertung
3. Maßnahmen
4. Bericht

Typische, zu explizierende Motive zur Durchführung einer DSFA:

1. Wissenschaftlich ->
   Aufdeckung objektiver Risiken
2. Marketing-DPIA ->
   Risiko-Verdeckung
3. Umsetzung der DS-GVO ->
   Zur Rechtfertigung eines Verfahrens

DSFA-Standardprozess

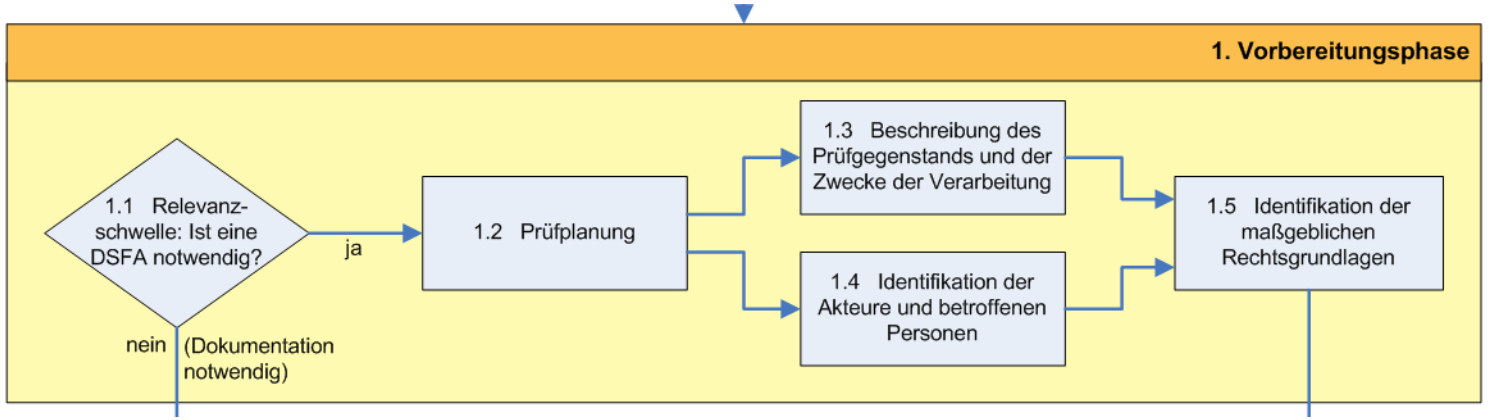
Änderungen durch die UAGSDM



1. Änderung des Titels auf
„(Weiter-)Entwicklung eines personenbezogenen Verfahrens“

2. Ergänzung des Maßnahmenbündels 3.4
„Erstellung eines Datenschutzkonzepts und
Integration ins Datenschutzmanagement“

DSFA-Standardprozess
1. Vorbereitungsphase



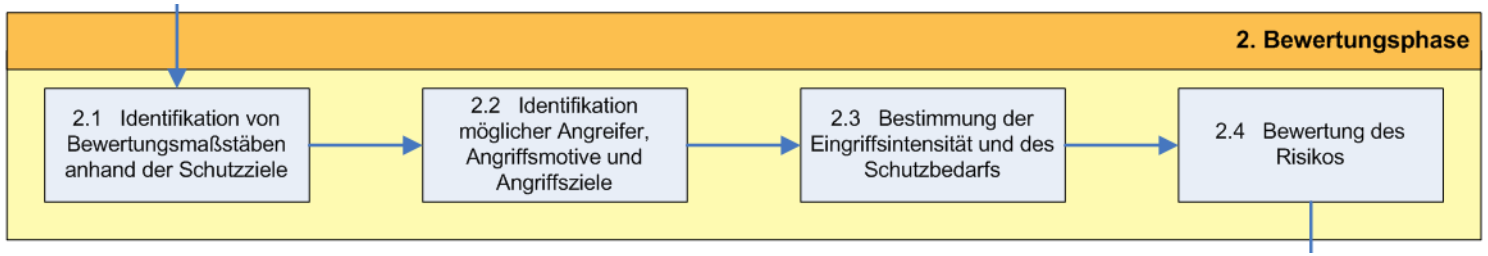
Vorbereitungsphase
1.1: **Relevanzschwelle**: Feststellung der Notwendigkeit einer DSFA

wenn DSFA durchzuführen ist:
1.2: **Prüfplanung**
1.3: **ToE klären**: Beschreibung des Prüfgegenstands und Zwecke der Verarbeitung,
1.4: Identifikation der **Akteure und betroffenen Personen**
1.5: Identifikation der maßgeblichen **Rechtsgrundlagen**

wenn DSFA nicht ausgeführt wird:
Dokumentation mit Begründung, eine DSFA nicht durchzuführen.

1.1 **Relevanzschwelle** wird vom Verantwortlichen festgelegt.
1.2 **Projektmanagement**
Methodik des Prüfens? SDM?
1.3 **ToE** einer DSFA betrifft ein Verfahren mit Zusammenschau von Daten, IT-Systemen und Prozessen.
1.4 **Akteure**
Identifikation der Akteure auf der Innenseite und der Betroffenen (Bürger, Kunde, Patient) auf der Außenseite einer Organisation.

2. Bewertungsphase: Angreifer und Schutzbedarfe



Bewertungsphase

2.1: Identifikation von **Bewertungsmaßstäben** anhand der Schutzziele

2.2: Identifikation möglicher **Angreifer**, Angriffsmotive und Angriffsziele

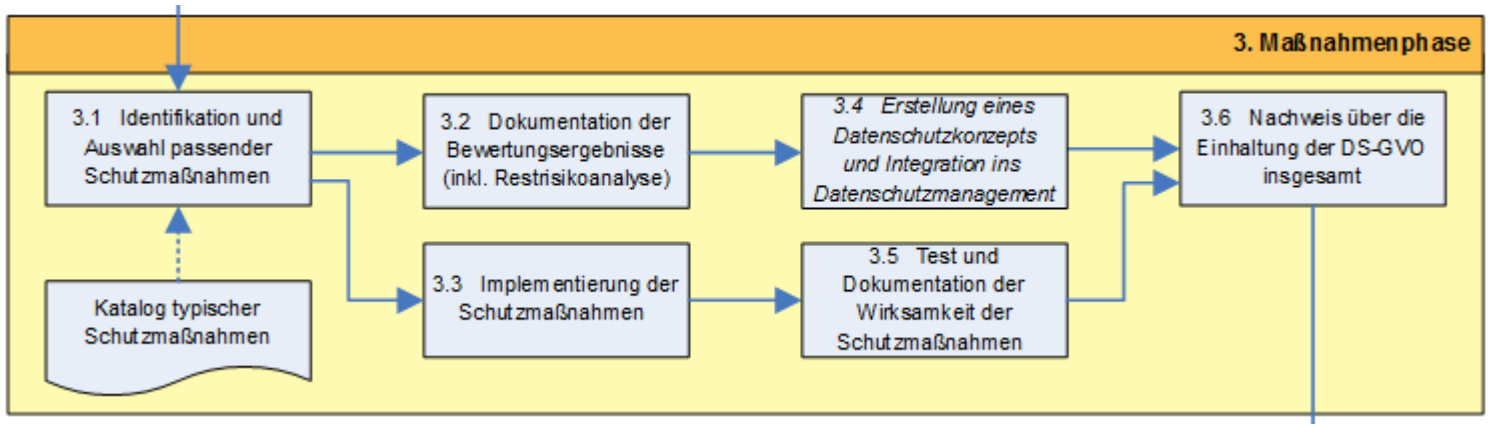
2.3: Bestimmung der Eingriffsintensität und des **Schutzbedarfs**

2.4: **Bewertung des Risikos**

Angreifer können sein:

- **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 (Zugang, Inhalte etc.) / Banken, Versicherungen / Wirtschaftsauskunfteien, Adress- und Datenhandel, Marktforschung / Werbung / Interessenvereinigungen, Verbände / Arbeitgeber)
- **Gesundheitswesen** (z.B. Krankenhäuser, Ärzte / gesetzliche und private Krankenversicherungen)
- **Forschung** (z.B. Medizinforschung, Sozialforschung, Universitäten)

DSFA-Standardprozess
3. Maßnahmenphase



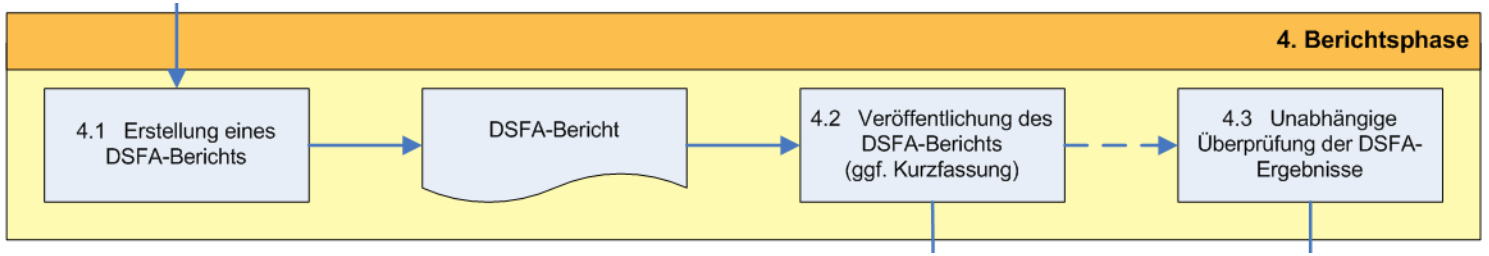
Maßnahmenphase

3.1: Identifikation und Auswahl passender **Schutzmaßnahmen**
3.2: Dokumentation der **Bewertungsergebnisse (inkl. Restrisikoanalyse)**
3.3: Implementierung der **Schutzmaßnahmen**
3.4: Erstellung eines **Datenschutzkonzepts** und Integration des Verfahrens in das **Datenschutz-Management**
3.5: **Test und Dokumentation der Wirksamkeit** der Schutzmaßnahmen
3.6: **Nachweis** über die Einhaltung der DS-GVO insgesamt.

Maßnahmen:

- Hier kommt die gesamte SDM-Methodik und der SDM-Referenzmaßnahmenkatalog ins Spiel.
- Managen der Übergänge der Projektphasen, an deren Ende jeweils spezifische Tests durchzuführen sind.
- Ob MP3.4 vor MP3.5 liegen muss oder die Reihenfolge umgekehrt sinnvoller ist oder MP3.4 noch ganz woanders positioniert sein sollte, wird die Praxis zeigen.

DSFA-Standardprozess
4. Berichtsphase



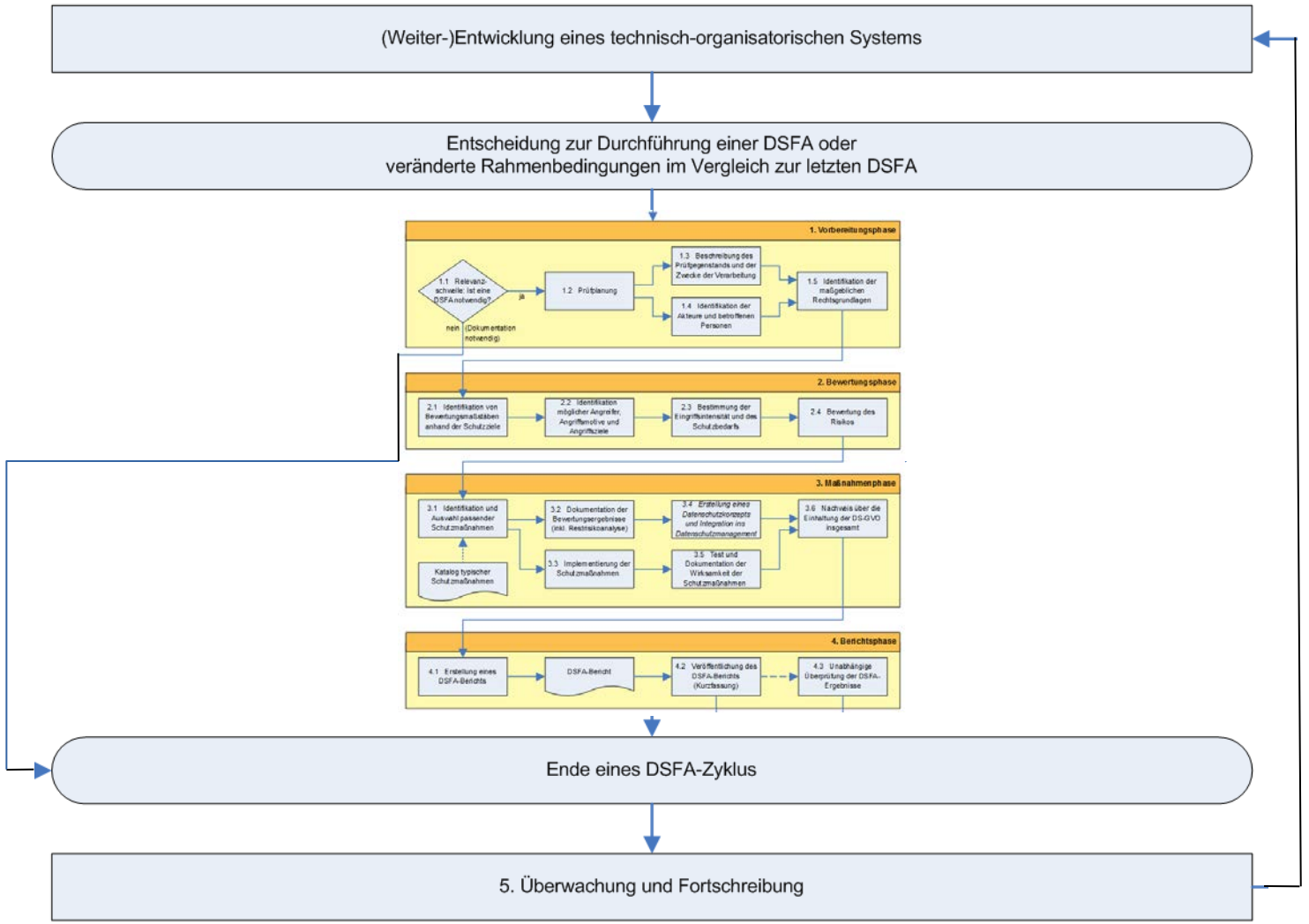
Berichtsphase

4.1: Erstellung eines **DSFA-Berichts**
4.2: **Veröffentlichung** des DSFA-Berichts (ggfs. Kurzfassung)
4.3: Unabhängige **Überprüfung** der DSFA-Ergebnisse

An wen ist der Bericht adressiert:

- an die Organisation(sleitung)?
- an die Betroffenen?
- an die Aufsichtsbehörden?
- an andere Organisationen (mit den zusammengearbeitet wird)?

DSFA-Standardprozess
4. Bericht



Eine **DSFA ist Bestandteil eines Datenschutzmanagementsystems.**

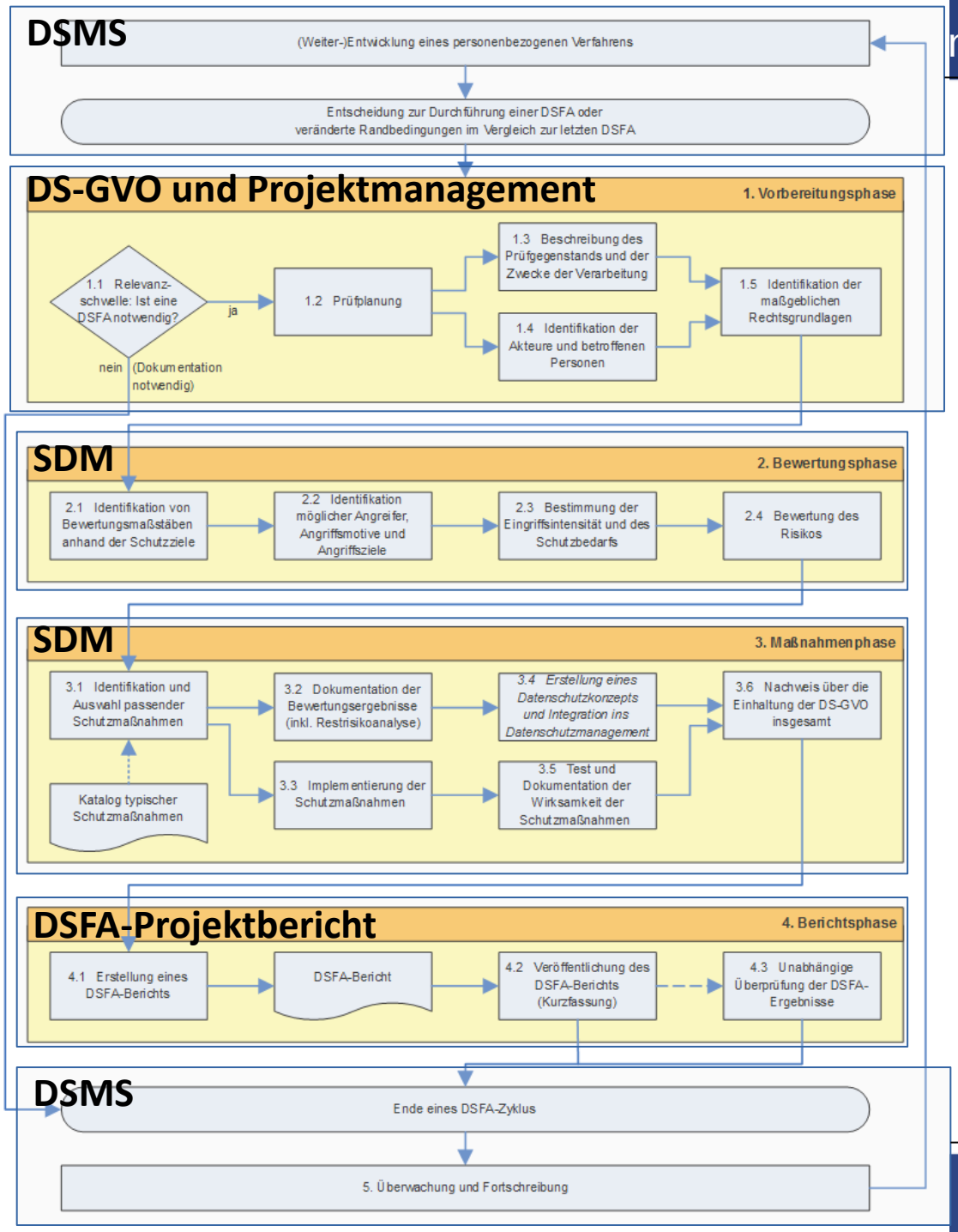
Ein DSMS klärt im Rahmen einer kontinuierlichen **Weiterentwicklung** der Organisation:

1. **Relevanzschwelle**: Veranlasst die Entscheidung zur Durchführung einer DSFA
2. **Kontinuität**: Überwachung und Fortschreibung der DSFA

Agenda

1. Datenschutz ist bereits verankert in der EU-Grundrechte-Charta
2. Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO
3. DS-GVO und Standard-Datenschutzmodell (SDM)
4. Ein standardisierter DSFA-Prozess
5. Hochzeit DSFA mit SDM

DSFA
SDM und DSMS



1 - Vorbereitung und Anforderungen

- Entscheidung: Art. 35 DS-GVO
- Projektmanagement aufsetzen
- ToE - Spezifikation des Verfahrens

2 - Bewertung mit Hilfe des SDM

- Kriterien: Set der Schutzziele
- Identifikation der Angreifer
- Festlegen: Eingriffsintensität, Schutzbedarf, Risiko

3 - Maßnahmenwahl mit SDM

- Dem standardisierten Schutzmaß-nahmenkatalog entnehmbar

4 - Berichtswesen

Datenschutz-Management System (Maßnahme aus SDM)

DSFA, SDM, DS-GVO

DSB-Konferenz 2015:
SDM-Handbuch, V0.9a
https://datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

Internationale PIA-Frameworks...

White Paper des Forums Privatheit (2016/03):
Datenschutz-Folgenabschätzung
https://www.forum-privatheit.de/

Datenschutz-Grundverordnung..

Bieker, F. / Hansen, M. / Friedewald, M., 2016/09: Die grundrechtskonforme Ausgestaltung der **Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung**; in:
RDV (Recht der Datenverarbeitung), Heft 4, 188-197

Datenschutz-Grundverordnung..

SDM - Maßnahmenkatalog (2016/11, Entwurf)

Vielen Dank für Ihre Aufmerksamkeit!

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

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