DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# EU-Datenschutz-Grundverordnung

- Technischer Datenschutz,
- Risikobewertung und die
- Datenschutz-Folgenabschätzung

Diplom-Informatiker
Werner Hülsmann
Datenschutzexperte – https://DSGVO.expert

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

## Gliederung



DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Diplom-Informatiker Werner Hülsmann

| | |
|---|---|
| 1982 – 1988 | Studium der Informatik an der TU Darmstadt - Schwerpunkt Datenschutzrecht |
| 1988 – 1991 | Softwareentwickler bei der Telenorma GmbH, Frankfurt (Main) |
| 1992 – 1999 | Wissenschaftlicher Mitarbeiter und Referatsleiter Technik beim Landesbeauftragten für Datenschutz der Freien Hansestadt Bremen |
| 1999 – 2001 | Datenschutz- und Technologieberatung bei ForBIT e.V. in Hamburg |
| Seit 1999 | selbständiger Datenschutzberater (Datenschutzconsulting.eu) |
| 2001 – 2003 | Projektmanager Dataprotection bei der Telegate AG (Martinsried) |
| 2003 – 2009 & seit 2014 | Vorstandsmitglied der Deutschen Vereinigung für Datenschutz (DVD) e.V., - www.datenschutzverein.de |
| Seit 2004 | Kooperationspartner des virtuellen Datenschutzbüros |
| 2004 | Gründung von Datenschutzwissen.de – Organisation und Leitung von Datenschutzseminaren |
| Seit 2004 | beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich/technisch) |
| Seit 2010 | Expert for legal and technical evaluations for the European Privacy Seal (http://www.european-privacy-seal.eu/) |
| Seit 2016 | Betrieb der Website https://dsgvo.expert |
| Seit 09/2017 | Member of the Commission Multistakeholder expert group to support the application of Regulation (EU) 2016/679 (GDPR) |

 Technischer Datenschutz 3

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Gliederung



 Technischer Datenschutz 4

# IT-Sicherheit und Datenschutz

- Häufig wird angenommen, dass es zur technischen Umsetzung des Datenschutzes ausreichend ist, IT-Sicherheitsmaßnahmen nach ISO 27001 oder einer anderen IT-Sicherheitszertifizierung vorzunehmen.
- Dabei wird übersehen, dass der Schutzzweck bei der IT-Sicherheit ein anderer ist, als beim Datenschutz.
- IT-Sicherheitsmaßnahmen sind eine gute Basis für die technische Umsetzung des Datenschutzes

➡ Aber: Die Umsetzung von IT-Sicherheitsmaßnahmen alleine reicht für die technische Umsetzung des Datenschutzes nicht aus!



## Abgrenzung IT-Sicherheit/Datenschutz


Quelle: LfDI Mecklenburg-Vorpommern, Mai 2017 

# IT-Sicherheit versus Datenschutz

Durch den Datenschutz werden die klassischen Schutz- bzw. Gewährleitungsziele der IT-Sicherheit

- Vertraulichkeit,
- Authentizität,
- Integrität und
- Verfügbarkeit

in Bezug auf personenbezogene Daten um die Gewährleistungsziele

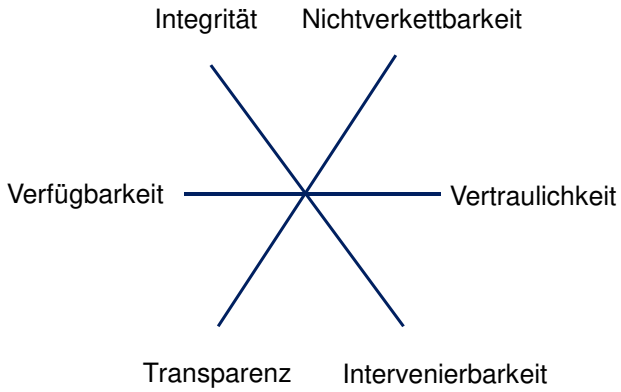
- Transparenz
- Nichtverkettbarkeit
- Intervenierbarkeit

erweitert.



# IT-Sicherheit versus Datenschutz




Quelle: LfDI Mecklenburg-Vorpommern, Mai 2017

Hinzu kommt durch Art. 5 Abs. 1 Buchstabe c DSGVO als siebtes Gewährleistungsziel der (bereits aus § 3a BDSG-alt bekannte) Grundsatz der Datenminimierung:

- Personenbezogene Daten müssen „c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“.

# Gliederung





# Technische und organisatorische Maßnahmen Fundstellen im BDSG-alt

- Im bisherigen BDSG waren die Fundstellen für die technischen und organisatorischen Maßnahmen relativ übersichtlich:
  - § 3a-BDSG-alt: Forderung nach Datenvermeidung und Datensparsamkeit
  - § 5 BDSG-alt: Verpflichtung auf das Datengeheimnis
  - § 9 BDSG-alt: Enthält die Anforderung technische und organisatorische Maßnahmen (TOM) zur Sicherstellung des Datenschutzes zu ergreifen
  - Anlage zu § 9 BDSG-alt: Acht Schutzziele der technischen und organisatorischen Maßnahmen

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Technische und organisatorische Maßnahmen Fundstellen in der DSGVO

- Art. 24 DSGVO: Anforderung, TOM zur Sicherstellung DSGVO-konformer Verarbeitung zu ergreifen.
- Art. 25 Abs. 1 DSGVO: Datenschutz durch Technikgestaltung
- Art. 25 Abs. 2 DSGVO: Datenschutz durch datenschutzfreundliche Voreinstellung.
- Art. 25 Abs. 3 DSGVO: Genehmigtes Zertifizierungsverfahren als Nachweis der Anforderungen aus Abs. 1 und 2
- Art. 25 Abs. 1 DSGVO: Datenschutzgrundsätze des Art. 5 sind Schutzziele der TOM
- Art. 32 Abs. 1 DSGVO: Weitere Schutzziele der TOM
- Art. 32 Abs. 2 DSGVO: Risikoabschätzung
- Art. 32 Abs. 3 DSGVO: Verhaltensregeln und Zertifizierungsverfahren als Nachweis der Umsetzung
- Art. 32 Abs. 4 DSGVO: Sicherstellung, dass Mitarbeiter Daten nur weisungsgebunden verarbeiten

 Technischer Datenschutz 11

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Unterschiede BDSG-alt und DSGVO

- Verstöße gegen § 3a (Datensparsamkeit und Datenminimierung und § 9 (nebst Anlage zu § 9, technische und organisatorische Maßnahmen) BDSG-alt stellen für sich genommen keinen Bußgeldtatbestand dar
- Verstöße gegen die Art. 25 und 32 DSGVO sind dagegen mit einem Bußgeld der Kategorie 10 Mio.€/2% bedroht.
- Verstöße gegen Art. 5 DSGVO sind mit einem Bußgeld der Kategorie 20 Mio. €/4% bedroht
- Art. 24 Abs. 2 DSGVO fordert von den Verantwortlichen (also den Arbeitgebern) erforderlichenfalls geeignete Datenschutzregelungen und –strategien einzuführen und umzusetzen
- Neu ist in der DSGVO die ausdrückliche Erwähnung, dass genehmigte Verhaltensregeln und Zertifizierungsverfahren dem Nachweis der Umsetzung dieser Anforderungen dienen können.
- Die Formulierungen und die Struktur der Schutzziele hat sich wesentlich geändert

 Technischer Datenschutz 12

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Gewährleistungsziele in der DSGVO

| Schutz- bzw. Gewährleistungsziel | Fundstelle DSGVO |
|---|---|
| Rechtmäßigkeit, Verarbeitung nach Treu und Glauben | Art. 5, Abs. 1 Buchst. a |
| Transparenz | Art. 5, Abs. 1 Buchst. a, Art. 13 und Art.14 |
| Zweckbindung | Art. 5, Abs. 1 Buchst. b |
| Datenminimierung | Art. 5, Abs. 1 Buchst. c |
| Speicherbegrenzung (Erforderlichkeitsgebot) | Art. 5, Abs. 1 Buchst. e |
| Richtigkeit | Art. 5, Abs. 1 Buchst. d |
| Integrität | Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b |
| Vertraulichkeit | Art. 5, Abs. 1 Buchst. f, Art. 32, Abs. 1 Buchst. b |
| Verfügbarkeit und Belastbarkeit beim Betrieb | Art. 32, Abs. 1 Buchst. b |
| Verfügbarkeit bei einem physischen oder technischen Zwischenfall | Art. 32, Abs. 1 Buchst. c |

 Technischer Datenschutz 13

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Datenschutz durch Technikgestaltung Art. 25 Abs. 1 DSGVO

- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen - wie z.B. Pseudonymisierung -, die dafür ausgelegt sind,
  - die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und
  - die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und
  - die Rechte der betroffenen Personen zu schützen
- Die technischen und organisatorischen Maßnahmen werden getroffen
  - unter Berücksichtigung des Stands der Technik
  - der Implementierungskosten und
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
  - der unterschiedlichen Eintrittswahr-scheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen

 Technischer Datenschutz 14

# Datenschutz durch Technikgestaltung Art. 25 Abs. 1 DSGVO

- Die Umsetzung des Grundsatzes „privacy by design“ wird durch technische und organisatorische Maßnahmen verwirklicht
  - hierzu ist der Verantwortliche gemäß Art. 24 DSGVO verpflichtet
  - die allgemeinen Grundsätze des Datenschutzes des Art. 5 DSGVO sind die Bezugspunkte, an denen sich die Maßnahmen ausrichten
  - der Verantwortliche hat alle Maßnahmen zu ergreifen, die ihm zumutbar sind
- In Bezug auf die Zumutbarkeit sind eine Reihe von Faktoren zu berücksichtigen:
  - der Stand der Technik
  - die Implementierungskosten
  - Art und Umfang sowie die Umstände und der Zweck der Datenverarbeitung
  - die Wahrscheinlichkeit des Eintretens von Risiken
  - die Schwere der Risiken für die Rechte und Freiheiten der Betroffenen



# Datenschutz durch datenschutzfreundliche Voreinstellungen – Art. 25 Abs. 2 DSGVO

- Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen,
  - dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungs-zweck erforderlich ist.
- Diese Verpflichtung gilt für
  - die Menge der erhobenen personenbezo-genen 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.
- Vgl. auch Erwägungsgrund 78

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Sicherheit der Verarbeitung Art. 32 Abs. 1 DSGVO

- Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- Dies geschieht 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 des Risikos für die Rechte und Freiheiten natürlicher Personen

 Technischer Datenschutz 17

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Sicherheit der Verarbeitung Art. 32 Abs. 1 DSGVO

- Die technischen und organisatorischen Maßnahmen schließen unter anderem Folgendes ein:
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

 Technischer Datenschutz 18

# Sicherheit der Verarbeitung Art. 32 Abs. 2 DSGVO

- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere
  - durch unbeabsichtigte oder unrechtmäßige Vernichtung,
  - Verlust,
  - Veränderung oder
  - von unbefugter Offenlegung bzw. von unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden



# Sicherheit der Verarbeitung Art. 32 Abs. 3 DSGVO

Um die Erfüllung der in Art. 32 DSGVO genannten Anforderungen nachzuweisen können, können

- genehmigte Verhaltensregeln (Art. 40 DSGVO) oder
- genehmigte Zertifizierungsverfahren (Art. 42 DSGVO)

herangezogen werden.

# Sicherheit der Verarbeitung Art. 32 Abs. 4 DSGVO

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass

- ihnen unterstellte natürliche Personen, personenbezogene Daten nur weisungsgebunden verarbeiten

➡ Aus der „Verpflichtung auf das Datengeheimnis“ aus § 5 BDSG-alt wird eine „Verpflichtung auf den Datenschutz“

 Technischer Datenschutz 21



# Beispiele für Folgerungen

- Software und Systeme müssen über datenschutzfreundliche Voreinstellungen verfügen.
- Einwilligungen* müssen standardmäßig deaktiviert sein
- Freiwillige Datenfelder müssen als solche gekennzeichnet sein
- Unternehmen sollten auf Softwarehersteller und Dienstleister hinwirken, dass von diesen angebotene Software und Dienstleistungen datenschutzkonform entwickelt werden
  - Dies kann durch entsprechende Anforderungen bei der Ausschreibung oder der Angebotseinholung unterstützt werden
- Es ist künftig erforderlich, die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren und den Nachweis zu erbringen, dass sie regelmäßigen daraufhin überprüft werden, ob sie noch ausreichend sind und noch dem Stand der Technik entsprechen.

*) zur Freiwilligkeit von Einwilligungen im Beschäftigungsverhältnis wird auf § 28 Abs. 2 BSDG-neu verwiesen.

 Technischer Datenschutz 22

# Handlungsbedarf

- Prüfen, ob in allen Anwendungen nur die Daten erhoben werden, die für die jeweiligen Zwecke erforderlich sind.
- Prüfen, ob in Eingabemasken und Formulare freiwillige Angaben deutlich als solche gekennzeichnet sind.
- Prüfen, ob in Eingabemasken Ankreuzfelder für Einwilligungen und Nutzungszustimmungen nicht vorangekreuzt sind
- Prüfen ob sichergestellt ist, dass Daten, die nur Aufgrund einer Einwilligung verarbeitet werden dürfen auch nur bei vorliegender wirksamer Einwilligung verarbeitet werden.
- Prüfung, ob die technischen und organisatorischen Maßnahmen – inklusive der entsprechenden Dienstanweisungen – dem aktuellen Stand der Technik entsprechen sowie unter Berücksichtigung der neu formulierten Schutzziele sowie der Risiken angemessen und ausreichend sind
- Gegebenenfalls Anpassung der Maßnahmen.

 Technischer Datenschutz 23

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Handlungsbedarf

- Prüfung und gegebenenfalls Aktualisierung der Dokumentation der technischen und organisatorischen Maßnahmen zum Datenschutz.
- Sicherstellen, dass eine regelmäßige Überprüfung dieser Maßnahmen erfolgt
- Sollte bisher noch Datensicherheitskonzept erstellt worden sein, empfiehlt sich folgende Vorgehensweise:
  - Schutzbedarfsfeststellung (diese ist zu dokumentieren)
  - Risikobewertung (diese ist ebenfalls zu dokumentieren)
  - Festlegen, welche technischen und organisatorischen Maßnahmen erfor-derlich sind
  - Umsetzung der Maßnahmen
  - Dokumentation der erforderlichen und der getroffenen Maßnahmen.

 Technischer Datenschutz 24

# Gliederung







# Risiken und die DSGVO

Das Thema Risiken hat in Bezug auf die DSGVO zumindest zwei Aspekte

1. **Unternehmerische Risiken**, die sich aus Datenschutzverstößen ergeben können, wie z.B.
   1. Bußgeldzahlungen
   2. Schadensersatzforderungen
   3. Reputations- und Imageverlust
   4. Kundenabwanderung

2. Berücksichtigung der **Risiken**, die sich aus der Verarbeitung personenbezogener Daten **für die Grundrechte und Freiheiten der betroffenen Personen** ergeben können.

## Risikobewertung in der DSGVO

- An vielen Stellen in der DSGVO ist von der Berücksichtigung der **Risiken für die Freiheiten und Grundrechte der betroffenen Personen** die Rede.
  - Art. 24 Abs. 1 - Verantwortung des für die Verarbeitung Verantwortlichen - Erwägungsgründe 74, 75, 76 und 77
  - Artikel 25 Abs. 1 - Datenschutz durch Technikgestaltung und durch datenschutz-freundliche Voreinstellungen
  - Artikel 27 Abs. 2 - Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern
  - Erwägungsgrund 81 (zu Art 28 Auftragsverarbeiter)
  - Artikel 30 Abs. 5 - Verzeichnis von Verarbeitungstätigkeiten
  - Artikel 32 Abs. 1 und 2 - Sicherheit der Verarbeitung – Erwägungsgrund 81



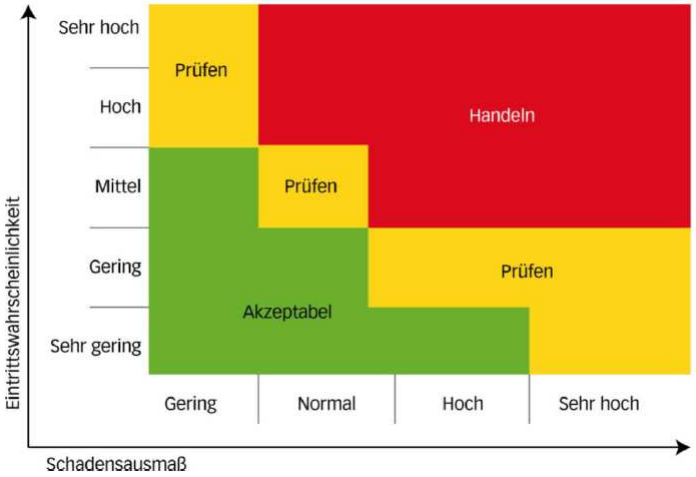
DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

## Risikobewertung in der DSGVO

- Artikel 33 Abs. 1 - Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde – Erwägungsgrund 87
- Artikel 34 Abs. 1, 3 und 4 - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person – Erwägungsgründe 86 und 87
- Artikel 35 Abs. 1, 7 und 11 - Datenschutz-Folgenabschätzung – Erwägungsgründe 84, 90, 91
- Artikel 36 Abs. 1 und 2 - Vorherige Konsultation (der Aufsichtsbehörde) – Erwägungsgründe 94 und 96
- Artikel 39 Abs. 2 - Aufgaben des Datenschutzbeauftragten
- Erwägungsgrund 98 zu Artikel 40 – Verhaltensregeln

=> Eine Abschätzung der Risiken für die Grundrechte und Freiheiten der betroffenen Personen ist für jede Verarbeitung personenbezogener Daten erforderlich!

# Risiko-Matrix




Eine solche Risikomatrix kann als Basis für die Entscheidung, ob eine Datenschutz-Folgenabschätzung erforderlich ist oder nicht genutzt werden.

Quelle: Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit





# Die Datenschutz-Folgenabschätzung

- Die Datenschutz-Folgenabschätzung (DS-FA) nach Art. 35 DSGVO kann im weitesten Sinne als Nachfolgeregelung der bisherigen Vorabkontrolle gesehen werden.
- Ein wesentlicher Unterschied:
  - Die bisherige Vorabkontrolle nach dem BDSG-alt wird von dem/der Datenschutzbeauftragten durchgeführt. Diese/r entscheidet damit über die Zulässigkeit eines vorabkontrollpflichtigen Verfahrens
  - Die DS-FA nach der DSGVO wird vom Verantwortlichen (bisheriger Begriff: „verantwortliche Stelle“) also dem Arbeitgeber durchgeführt
  - Der/Die Datenschutzbeauftragte berät den Arbeitgeber nur noch bei der DS-FA
- Ein weiterer Unterschied:
  - Das BDSG-alt enthält keine Regelungen zur Ausgestaltung der Vorabkontrolle (vgl. § 4d Abs. 5 und 6 BDSG-alt).
  - Art. 35 Abs. 7 DSGVO regelt, welche Punkte eine DS-FA enthalten muss

# Die Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 1 DSGVO durchzuführen, wenn

- „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“ hat,

und ist gemäß Art. 35 Abs. 3 „insbesondere in folgenden Fällen erforderlich:

- 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;
- 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
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;“

Gemäß § 35 Abs. 4 erstellen die Datenschutzaufsichtsbehörden „eine Liste der Verarbeitungs-vorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist “.

 Technischer Datenschutz 31



# Inhalte der Datenschutz-Folgenabschätzung

- „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvor-gänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1
- 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.“

 Technischer Datenschutz 32

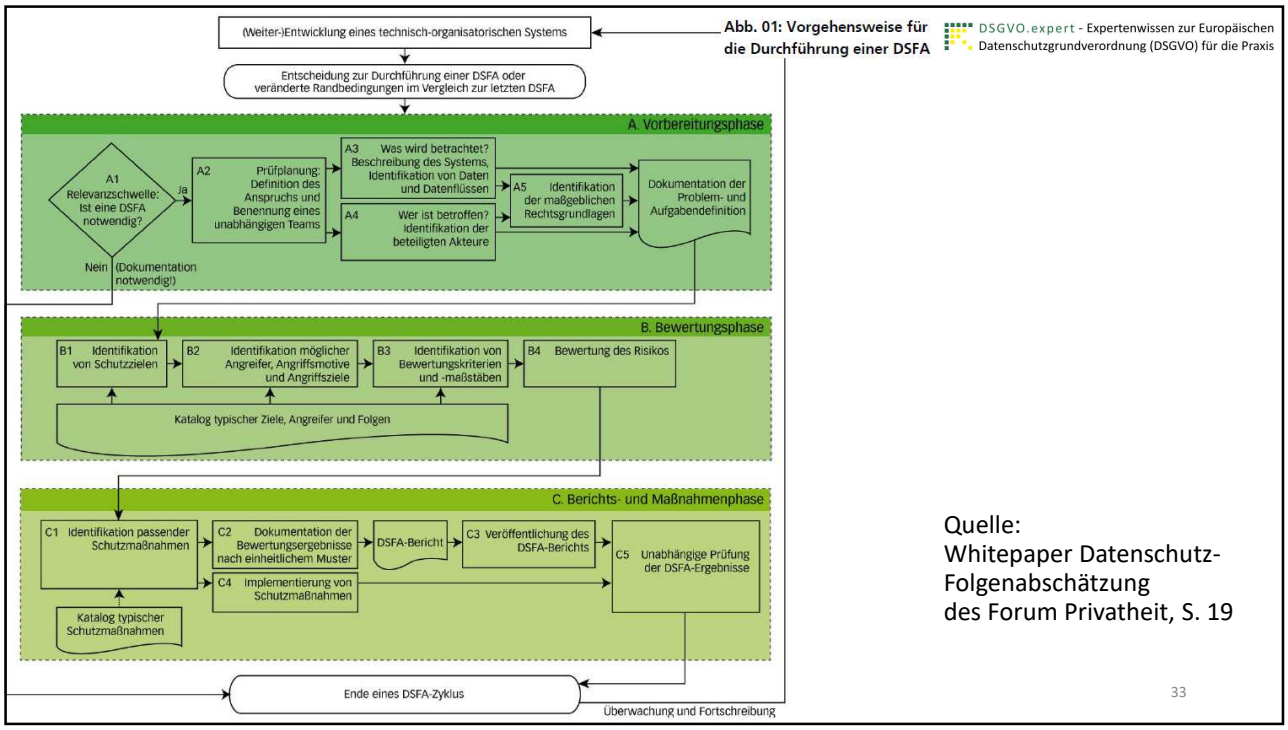



**Abb. 01: Vorgehensweise für die Durchführung einer DSFA**

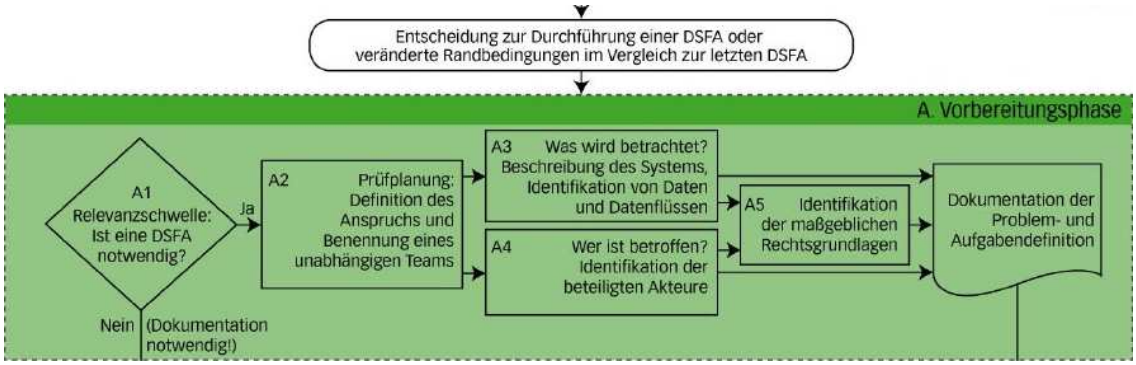
DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

Quelle:
Whitepaper Datenschutz-Folgenabschätzung
des Forum Privatheit, S. 19

33

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Durchführung der DS-FA

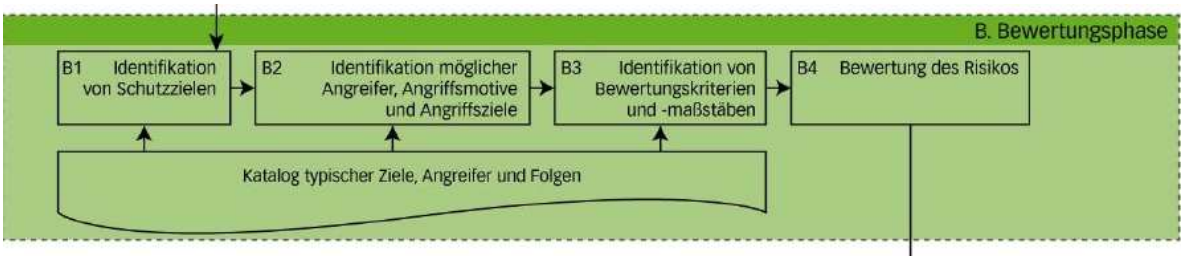



Quelle: Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit

34

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Durchführung der DS-FA

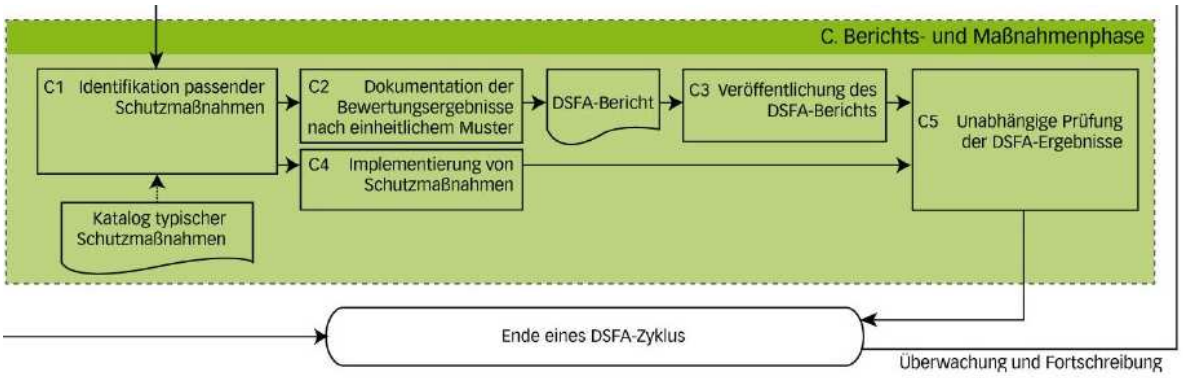



Quelle: Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit

35

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

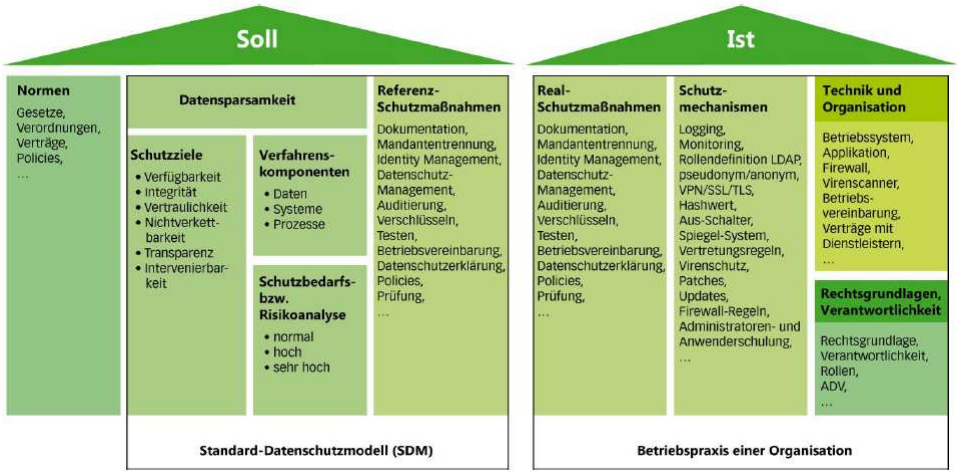
# Durchführung der DS-FA




Quelle: Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit

36

# Durchführung der DS-FA




Quelle: Whitepaper Datenschutz-Folgenabschätzung des Forum Privatheit





# Die DS-FA und genehmigte Verhaltensregeln

- „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.“ (Art. 35 Abs. 8 DS.GVO)
- Sofern für einen Unternehmensverband derartige genehmigte Verhaltensregeln existieren, die auch den Umgang mit Beschäftigtendaten regeln, hat der Arbeitgeber die dortigen Vorgaben einzuhalten.
- Da derartige Verhaltensregeln von der zuständigen Datenschutz-Aufsichtsbehörde genehmigt wurden, können etwaige darin enthaltenen Regelungen zum Umgang mit Beschäftigtendaten als datenschutzkonform und akzeptabel angesehen werden.

## Standpunkt der Betroffenen und DS-FA

- „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.“ (Art. 35 Abs. 9 DSGVO)
  - Bei der Einführung neuer IT-technischer Systeme, die eine Überwachung der Beschäftigten ermöglichen, muss der Verantwortliche – also der Arbeitgeber – bei der Durchführung der Datenschutz-Folgenabschätzung
    - den Standpunkt Betriebs- oder Personalrates einholen.
  - Die Mitbestimmungsrechte der Personalvertretung werden dadurch nicht berührt.
  - Bei Verarbeitungstätigkeiten, bei denen die personenbezogenen Daten von VerbraucherInnen verarbeitet werden, ist deren Standpunkt, z.B. über Verbraucherschutzverbände oder Datenschutzverbände, die VerbraucherInnen vertreten einzuholen



## Vorabkontrollen und DS-FA

- Eine Datenschutz-Folgenabschätzung für Verarbeitungen, die bereits vor dem Stichtag 25. Mai 2018 begonnen wurden, ist aus Sicht der Aufsichtsbehörden dann nicht erforderlich ist,
  - wenn für diese Verarbeitungen bereits eine Vorabkontrolle nach § 4d Abs. 5,6 BDSG-alt erfolgt ist und
  - das Ergebnis derart dokumentiert wurde, dass das Ergebnis der Vorabkontrolle nachvollziehbar ist.
- Daher empfiehlt es sich, noch nicht erfolgte aber erforderliche Vorabkontrollen bis zum 25. Mai 2018 nachzuholen, da der Aufwand für eine Vorabkontrolle in der Regel niedriger ist als für eine DS-FA.

# Vorabkontrollen und DS-FA und Bußgelder

- Die Nichtdurchführung einer erforderlichen Vorabkontrolle stellt selbst noch Ordnungswidrigkeit dar, kann aber zu einer bußgeldbewehrten (bis zu 300.000 €) unzulässigen Verarbeitung personenbezogener Daten führen.
- Die Nichtdurchführung einer erforderlichen DS-FA ist für sich alleine schon ein Bußgeldtatbestand der mit bis zu 10 Mio. € bzw. 2 % vom weltweiten Jahresumsatz geahndet werden, je nach dem welcher Betrag der höhere ist, geahndet werden kann
- Ergibt sich darüber hinaus noch eine unzulässige Datenverarbeitung kann diese mit einem Bußgeld bis zu 20 Mio. € bzw. 4 % vom weltweiten Jahresumsatz geahndet werden, je nach dem welcher Betrag der höhere ist.





# Handlungsbedarf

- Es ist zu prüfen, ob für alle Verfahren, für die bereits nach geltendem Recht eine Vorabkontrolle erforderlich ist und ob diese in ausreichendem Detailgrad dokumentiert wurden (Stichwort: Nachvollziehbarkeit des Ergebnisses)
- Für alle Verfahren, bei denen die bereits nach geltendem Recht erforderliche Vorabkontrolle noch nicht durchgeführt wurde, sollte diese zeitnah (bis spätestens 24. Mai 2018) nachgeholt und in ausreichendem Detailgrad dokumentiert werden.
- Ab 25. Mai 2018 ist sicherzustellen, dass bei der Einführung neuer Verarbeitungs-tätigkeiten und wesentlichen Änderungen bestehender Verarbeitungstätigkeiten geprüft wird, ob eine DS-Folgenabschätzung erforderlich ist. Diese Entscheidung ist mitsamt dem Ergebnis der erforderlichen DS-Folgenabschätzung zu dokumentieren und bei Bedarf gegenüber der Datenschutzaufsichtsbehörde nachzuweisen.

DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

# Gliederung



DSGVO.expert - Expertenwissen zur Europäischen Datenschutzgrundverordnung (DSGVO) für die Praxis

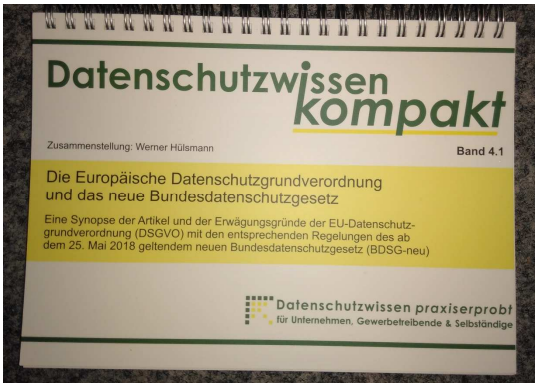
# Hilfsmittel zur Umsetzung

- Das Standard-Datenschutzmodell (SDM) der Datenschutzaufsichtsbehörden
  - Zu finden unter: https://www.datenschutzzentrum.de/sdm/
- Whitepaper „DATENSCHUTZ-FOLGENABSCHÄTZUNG – Ein Werkzeug für einen besseren Datenschutz“ des Forum Privatheit
  - Zu finden unter: https://www.forum-privatheit.de – Publikationen und Downloads bzw. direkt unter https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf
- **Diese und weitere Links** finden Sie auch unter https://dsgvo.expert/MatDS-FA
- Checklisten für die Vorabkontrolle zu finden unter:
  - https://www.datenschutz.hessen.de/tf001.htm
  - http://www.lfd.niedersachsen.de/technik_und_organisation/vorabkontrolle/vorabkontrolle-56138.html
  - https://www.saechsdsb.de/informationen-oeb/formulare-saechsdsb-oeb

## Literatur zur DSGVO

- Synopse mit Artikeln der DSGVO, den dazugehörigen Erwägungsgründen und den entsprechenden Regelungen des BDSG-neu: https://efweha-verlag.de/bd41








## Noch Fragen?

Werner Hülsmann – Datenschutzwissen.de

- Münchener Str. 101 / Geb. 01
  85737 Ismaning
  Tel.: 089 / 51 30 569-7, FAX: -8
- Pappelhof 12
  14478 Potsdam
  Tel. 0331 / 58 50 39 31

Mobil: 0177 / 28 28 681

E-Mail: wh@datenschutzwissen.de

https://DSGVO.expert & https://datenschutzwissen.de