*Datenschutzfolgenabschätzung*

UpDate!
Datenschutz by Esturias

# Datenschutz-Folgenabschätzung (DSFA)

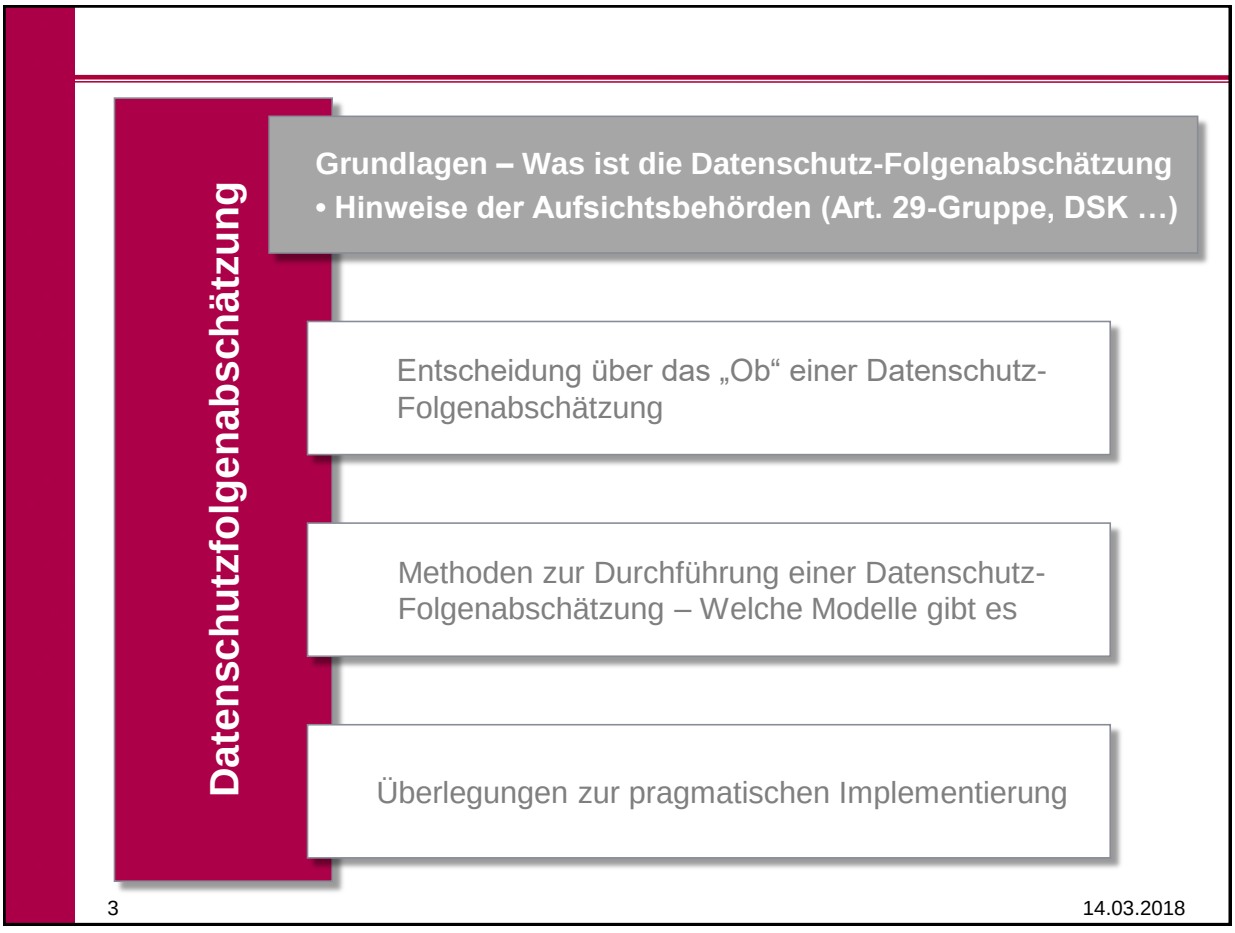
**Thomas Müthlein**
Geschäftsführer der DMC Datenschutz Management und Consulting GmbH und Co. KG, Frechen,
Vorstandsmitglied der GDD, Bonn

## *Datenschutzfolgenabschätzung*

**Thomas Müthlein**

- Seit 1990 im Datenschutz tätig: Geschäftsführer der GDD, Konzern-DSB, zertifizierter DSB (GDD), Datenschutzberater, Fach-Autor und Referent
- Mitglied des Vorstandes der GDD mit den Schwerpunkten Datenschutzpraxis, Outsourcing, Internationaler Datentransfer und Recht bei Telekommunikations- und Multimediaeinsatz
- Geschäftsführer der DMC Datenschutz Management & Consulting GmbH & Co. KG – Datenschutzberatung und -auditierung
- Zertifizierter Datenschutzauditor (DSZ) zur Auditierung nach dem Datenschutzstandard für die Auftragsdaten-verarbeitung DS-BvD-GDD-01
- Anerkannter Sachverständiger für IT-Produkte beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

2 14.03.2018


Datenschutzfolgenabschätzung
Grundlagen – Was ist die Datenschutz-Folgenabschätzung
• Hinweise der Aufsichtsbehörden (Art. 29-Gruppe, DSK …)
Entscheidung über das „Ob“ einer Datenschutz-Folgenabschätzung
Methoden zur Durchführung einer Datenschutz-Folgenabschätzung – Welche Modelle gibt es
Überlegungen zur pragmatischen Implementierung
3
14.03.2018

# Hinweise zur DSFA


- **Art. 29 Gruppe**
  WP 248 Rev. 01: Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.04.2017, Überarbeitung vom 04.10.2017
- **LDA Bayern**
  XV III - Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DS-GVO, vom 21.03.2017
- **DSK**
  Kurzpapier Nr. 5 - Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, vom 24.07.2017
- **Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt**
  White Paper: Datenschutzfolgenabschätzung - Ein Werkzeug für einen besseren Datenschutz, 3. Auflage
- **Gonscherowski / Herber / Robrahn / Rost / Weichelt**
  Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive"-Verfahrens (V 0.10), 2017
- **Frankreich: CNIL**
  PIA – An overview of the requirements and methology, 2017
  The open source PIA software helps to carry out data protection impact assessment, *06.12.2017, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment*
- **Irland: Data Protection Commissioner**
  Data Protection Impact Assessments (DPIA) - For Organisations, *http://gdprandyou.ie/data-protection-impact-assessments-dpia/*
- **GDD**
  GDD-Praxishilfe DS-GVO X, Voraussetzungen der Datenschutz-Folgenabschätzung, November 2017
- **Bitkom**
  Leitfaden - Risk Assessment & Datenschutz-Folgenabschätzung, 2017

4 14.03.2018

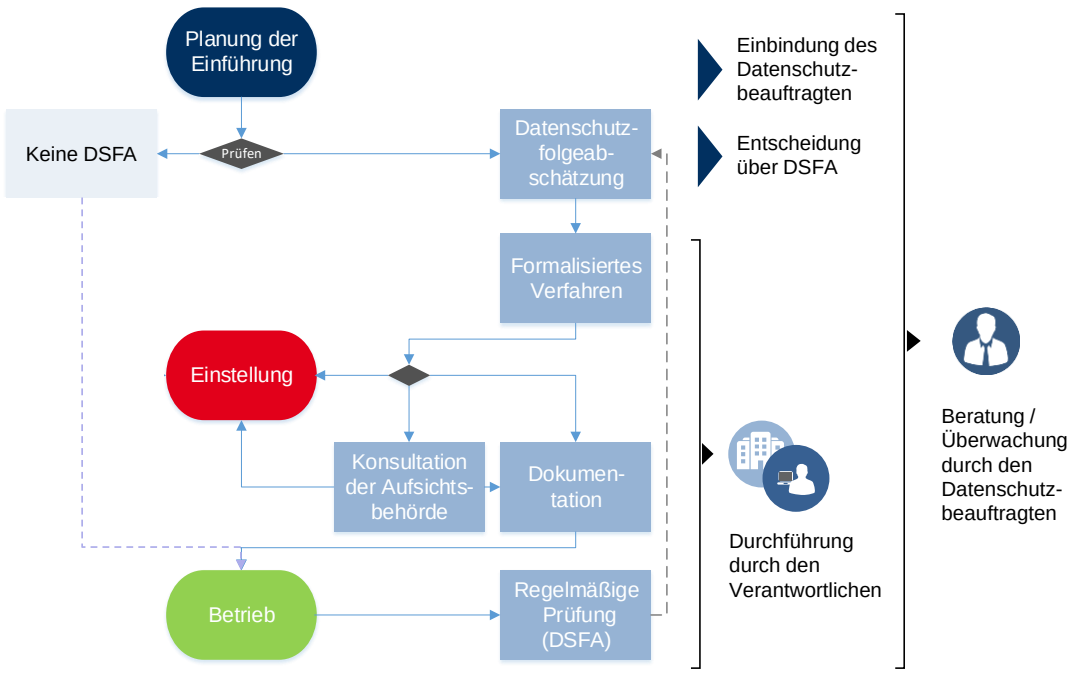
# Definition: DSFA


Eine Datenschutz-Folgenabschätzung (DSFA) ist ein **Prozess**, um das **Risiko** zu **erkennen**, zu **bewerten** und zu **bewältigen**, das für das **Individuum** in dessen unterschiedlichen Rollen (als Bürger, Kunde, Patient etc.) durch den **Einsatz einer bestimmten Technologie** oder eines Systems durch eine Organisation für **dessen Grundrechte** entsteht.

**Ziel** einer DSFA ist es, Kriterien des operationalisierten Grundrechtsschutzes zu definieren, die Folgen von personenbezogenen Verfahren möglichst umfassend zu erfassen sowie objektiv und nachvollziehbar mit Blick auf die verschiedenen Rollen und damit verbundenen Interessen so zu bewerten, dass **Angriffen durch Organisationen** mit **adäquaten Gegenmaßnahmen** begegnet werden kann.

5 14.03.2018

# Einführung / Änderung von Verfahren




6 14.03.2018

# Aspekte der DSFA

Sicherstellung der Beachtung aller Aspekte zur Durchführung der DSFA durch den Verantwortlichen

**Erforderlichkeit:** Risikobewertung, Festlegung durch Aufsicht, freiwillig

**Durchführung:** Verantwortlicher

**Zurateziehung:** Datenschutzbeauftragter

**Zeitpunkt:** „vorab“ / neu insbes. bei Änderung des Risikos

**Anforderungen:**

- systematische Beschreibung:
  - der geplanten Verarbeitungsvorgänge
  - der Zwecke der Verarbeitung
- Bewertung:
  - der Notwendigkeit
  - der Verhältnismäßigkeit
- Risikobewertung
- geplante Abhilfe(-/Sicherheits)maßnahmen
- Nachweise zur Einhaltung der Bestimmungen der DS-GVO

**Berücksichtigung:** Einhaltung genehmigter Verhaltensregeln

**Anhörung:** Standpunkt der Betroffenen („gegebenenfalls“)

**Dokumentation:** der Durchführung; der Gründe, wenn dem Rat des DSB nicht gefolgt wird (Form ist nicht geregelt)

**[Konsultationspflicht:** ggf. Zurateziehung der Aufsicht (formalisiert)]

Datenschutz-beauftragter:

… Überwachung ihrer Durchführung gemäß Art. 35

## CNIL: PIA – An overview of the requirements and methology

### PIA

An overview of the requirements and methodology

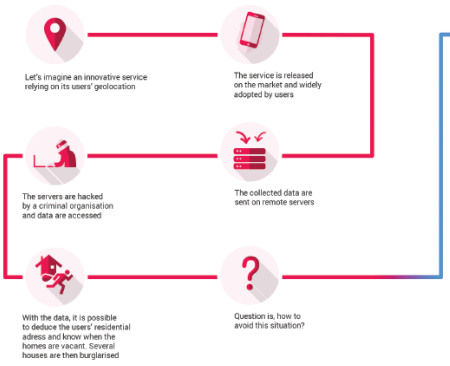
### 0. Launching a new processing

Every day in the digital realm, numerous services are created.

Those services usually rely on the processing of personal data aiming at fulfilling the needs of organisations or their users.

The supporting assets used to store the data have different levels of vulnerabilities toward feared events such as illegitimate acess, unwanted change, or disappearance of personal data.

Those risks are likely to have significant impacts on the users' privacy.




### 1. Considering the processing


For the data processor as well as the data subjects, those risks are unwelcome.

Before carrying out a processing, it is essential to analyse it to understand its inherent risks.

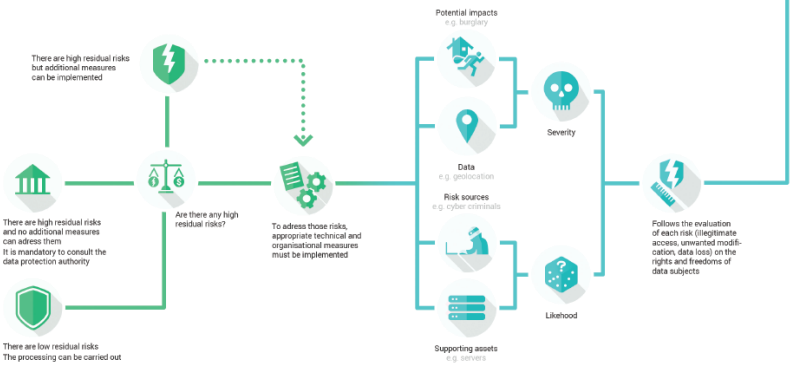
Several factors affect the riskiness of a processing, as the kind of data processed.

Generally speaking, if a processing meets two of the criteria listed, then it is likely to present high risks and would require to carry out a privacy impact assessment.

### 2. Evaluating the privacy risks

The assessment first establishes the context in which the processing is carried out, including its purpose and technical features.

In addition to studying the fundamental principles, made up of the necessity and proportionality of the processing, each risk has to be analysed to evaluate its severity and likehood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risks sources and the supporting assets.




### 3. Adressing the risks

Once the risks have been identified, it should be determined if they are acceptable given the existing and planned technical and organisational measures.

If it doesn't seem possible in regard of the foreseen measures, the data protection authority has to be consulted.

In any case, it is mandatory to implement the planned controls before carrying out the processing.




8

14.03.2018

## CNIL: PIA – An overview of the requirements and methology

0.

**Einführung eines neuen Prozesses**

Jeden Tag entstehen im digitalen Bereich zahlreiche Dienste.
Diese Dienste beruhen in der Regel auf der Verarbeitung personenbezogener Daten, um den Bedürfnissen von Organisationen oder ihren Nutzern gerecht zu werden.
Die für die Speicherung der Daten verwendeten unterstützenden Ressourcen weisen unterschiedliche Grade von Schwachstellen gegenüber gefürchteten Ereignissen auf, wie z. B. unrechtmäßigen Zugang, unerwünschte Änderungen oder das Verschwinden von personenbezogenen Daten.
Diese Risiken können erhebliche Auswirkungen auf die Privatsphäre der Nutzer haben.

Stellen wir uns einen innovativen Dienst vor, der sich auf die Geolokalisierung seiner Nutzer stützt.

Die gesammelten Daten werden auf Remote-Servern übertragen.

Der Dienst wird auf dem Markt freigegeben und von den Nutzern weithin akzeptiert.

Die Server werden von einer kriminellen Organisation gehackt und auf Daten zugegriffen.

Anhand der Daten ist es möglich, die Wohnadresse der Nutzer abzuleiten und zu erfahren, wann die Wohnungen frei sind. In mehrere Häuser wird dann eingebrochen.

Die Frage ist, wie man diese Situation vermeiden kann.

9 14.03.2018

## CNIL: PIA – An overview of the requirements and methology

Zunächst ist es wichtig, die Merkmale der Verarbeitung zu identifizieren.

- Bewertung / Scoring
- Automatisierte Entscheidungsfindung
- Systematische Überwachung
- Sensible Daten
- Großer Umfang
- Datenabgleich
- Verwundbarkeit der betroffenen Personen
- Neue Technologie
- Verhindern, dass die betroffene Person von einem Recht Gebrauch macht.

Die Verarbeitung erfüllt mehrere Kriterien und stellt wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen dar.

1.

**Berücksichtigung der Verarbeitung**

Sowohl für den Datenverarbeiter als auch für die betroffenen Personen sind diese Risiken unerwünscht.
Bevor eine Verarbeitung durchgeführt wird, ist es unerlässlich, sie zu analysieren, um die ihr innewohnenden Risiken zu verstehen.
Mehrere Faktoren beeinflussen das Risiko einer Verarbeitung, wie z.B. die Art der verarbeiteten Daten.
Generell gilt: Erfüllt eine Verarbeitung zwei der aufgeführten Kriterien, ist sie mit hohen Risiken verbunden und erfordert eine Datenschutzfolgenabschätzung.

10 14.03.2018

## CNIL: PIA – An overview of the requirements and methology


Die Bewertung erfolgt für jedes Risikos (unrechtmäßiger Zugriff, unerwünschte Änderung, Datenverlust) für die Rechte und Freiheiten der betroffenen Personen.

2.

**Bewertung der Datenschutzrisiken**

Die Bewertung legt zunächst den Kontext fest, in dem die Verarbeitung erfolgt, einschließlich des Zwecks und der technischen Merkmale. Neben der Untersuchung der Grundprinzipien, die sich aus der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung zusammensetzen, muss jedes Risiko analysiert werden, um seine Schwere und Wahrscheinlichkeit im Hinblick auf seine potenziellen Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen, die verarbeiteten Daten, die Risikoquellen und die unterstützenden Vermögenswerte zu bewerten.

11 14.03.2018

## CNIL: PIA – An overview of the requirements and methology

3.

**Umgang mit den Risiken**

Sobald die Risiken identifiziert sind, sollte festgestellt werden, ob sie angesichts der bestehenden und geplanten technischen und organisatorischen Maßnahmen akzeptabel sind.
Wenn es im Hinblick auf die vorgesehenen Maßnahmen nicht möglich erscheint, ist die Datenschutzbehörde zu konsultieren.
In jedem Fall ist es zwingend erforderlich, die geplanten Kontrollen vor der Durchführung der Verarbeitung durchzuführen.


12 14.03.2018

# DSFA in Kürze

| | |
|---|---|
| A. Was spricht eine DSFA an? | Einen einzelnen Verarbeitungsvorgang oder ein Satz ähnlicher Verarbeitungsvorgänge |
| B. Welche Verarbeitungsvorgänge unterliegen einer DSFA? | |
| a) Wann ist eine DSFA verpflichtend? | Wenn eine Verarbeitung „wahrscheinlich zu einem hohen Risiko führt“. |
| b) Wann ist keine DSFA erforderlich? | Wenn die Verarbeitung nicht "zu einem hohen Risiko führt" oder bereits genehmigt wurde oder eine gesetzliche Grundlage hat. |
| c) Was ist mit bereits bestehenden Verarbeitungsvorgängen? | DSFAs werden für Verarbeitungen benötigt, die nach Mai 2018 erstellt werden oder die sich danach erheblich ändern. (rev01: -> Vorabkontrolle) |

*Art. 29 Gruppe, WP 248*

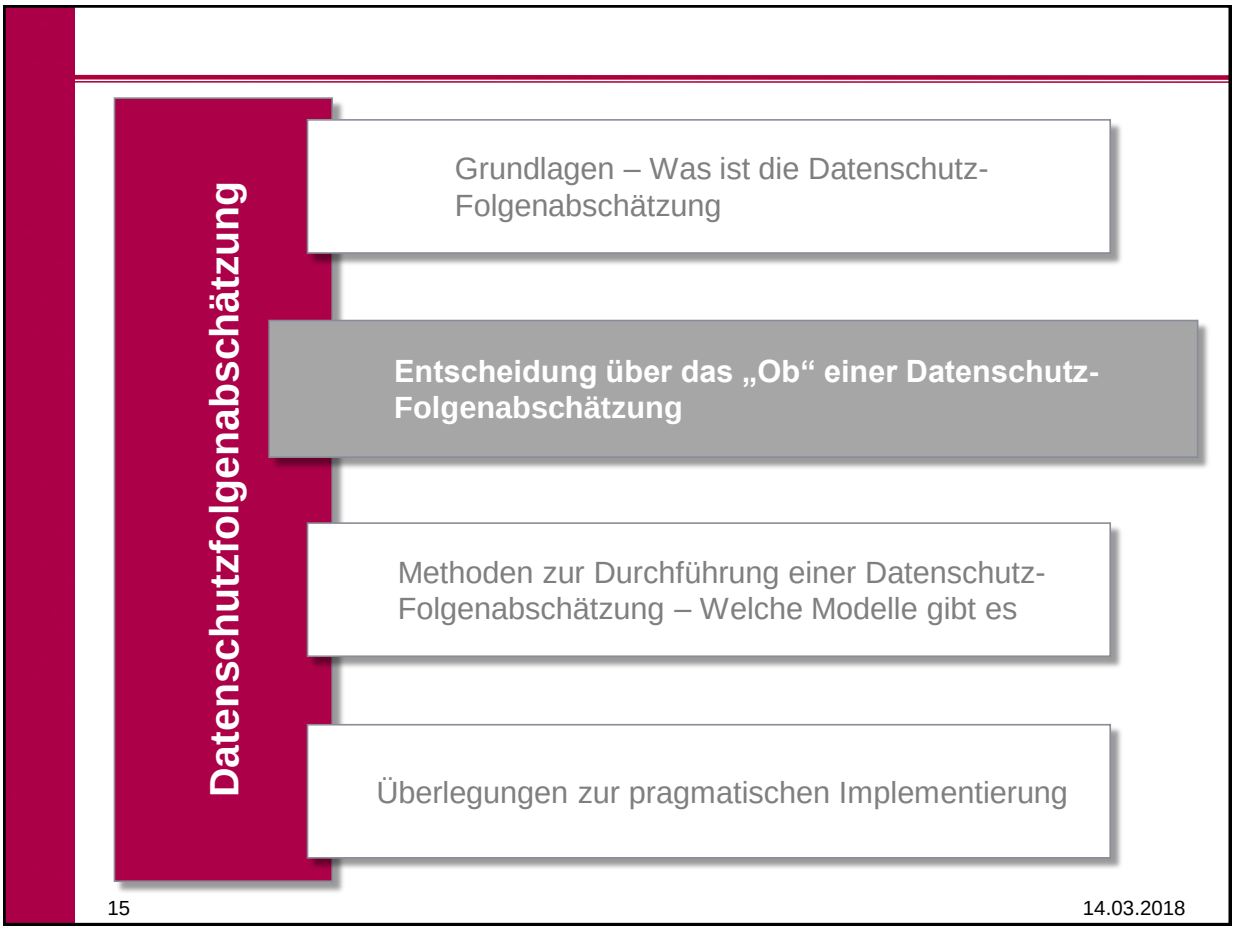
13 14.03.2018

# DSFA in Kürze

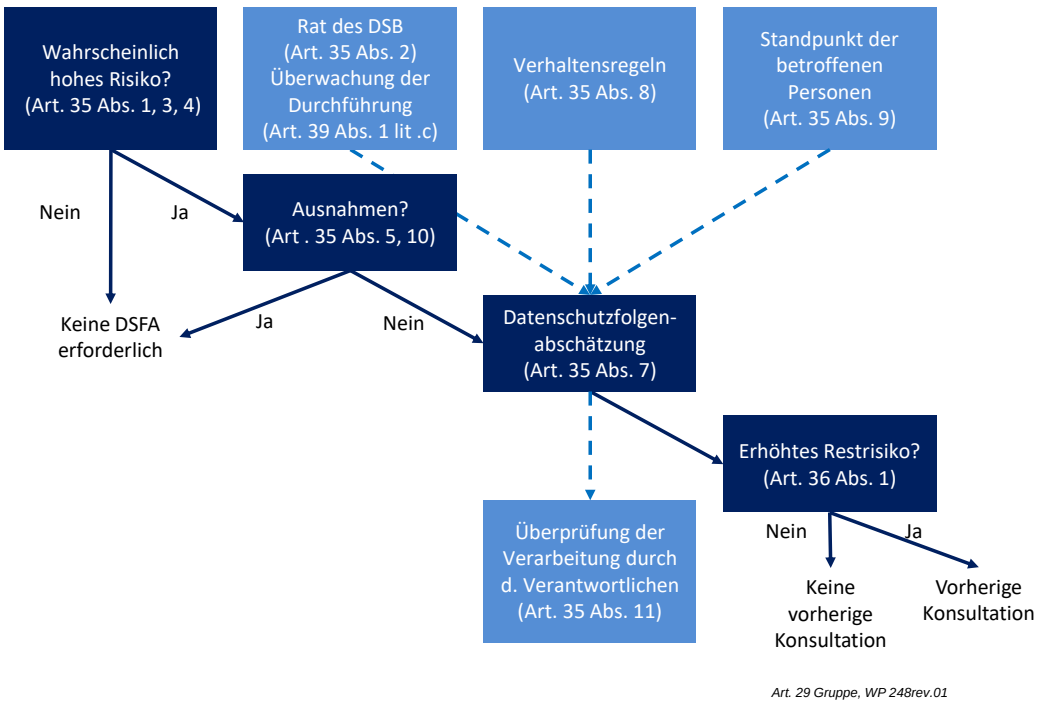
| | |
|---|---|
| C. Wie kann ich eine DSFA durchführen? | |
| a) Zu welchem Zeitpunkt sollte eine DSFA durchgeführt werden? | Vor der Verarbeitung |
| b) Wer ist verpflichtet, die DSFA durchzuführen? | Der Verantwortliche, mit dem DSB und dem Auftragsverarbeiter(n) |
| c) Welche Methodik ist zur Durchführung eine DSFA anzuwenden? | Verschiedene Methoden, aber gemeinsame Kriterien. |
| d) Sollte die DSFA veröffentlicht werden? | Ja, vollständig oder teilweise, und sie ist der Aufsicht-behörde bei vorheriger Konsultation mitzuteilen |
| D) Wann ist die Aufsichtsbehörde zu konsultieren? | Wenn die Restrisiken hoch sind |

*Art. 29 Gruppe, WP 248*

14 14.03.2018

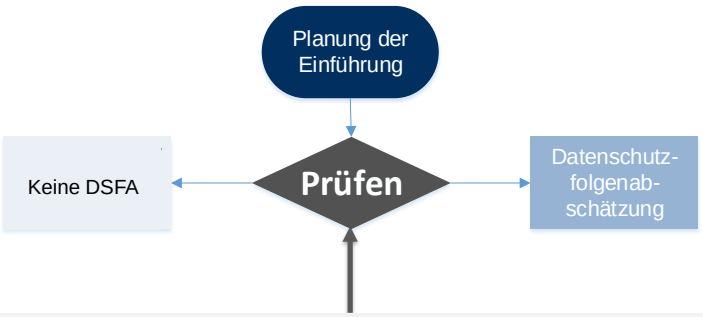

Datenschutzfolgenabschätzung
Grundlagen – Was ist die Datenschutz-Folgenabschätzung
Entscheidung über das „Ob“ einer Datenschutz-Folgenabschätzung
Methoden zur Durchführung einer Datenschutz-Folgenabschätzung – Welche Modelle gibt es
Überlegungen zur pragmatischen Implementierung
15
14.03.2018

# Ablauf der DSFA




16 14.03.2018

# Erforderlichkeit der DSFA



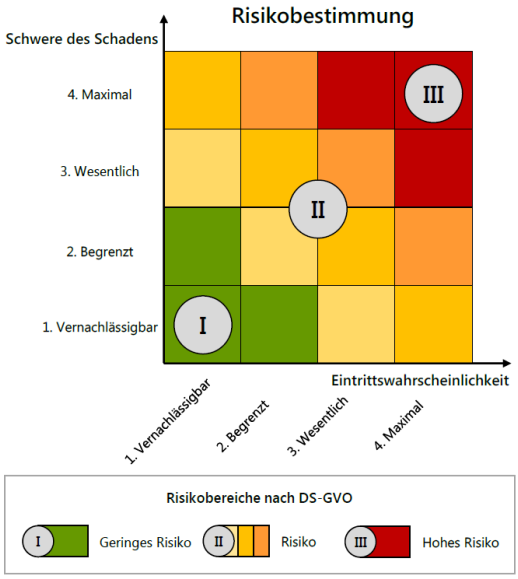

- **Grundsatz:**
  DSFA bei Verarbeitungen, die voraussichtlich ein hohes **Risiko** für den Betroffenen aufweisen
  **Gesetzliche Regelbeispiele:**
  - Systematische und umfassende Auswertung persönlicher Aspekte
  - Umfangreiche Verarbeitung besonderer Daten nach Art. 9, 10
  - Weiträumiger Überwachung öffentlich zugänglicher Bereiche
- **Hohes Risiko insbesondere durch**
  - die Verwendung neuer Technologien,
  - die Art der Verarbeitung
  - den Umfang der Verarbeitung
  - die Umstände der Verarbeitung
  - die Zwecke der Verarbeitung
- **Keine Ausnahmen**

Erforderlich:

Risikobewertung durch den Verantwortlichen für **jede** neue / (wesentlich) geänderte Verarbeitung (Artt. 5, 24 – Nachweispflicht)

17 14.03.2018

# Risikoanalyse - Schwellwertanalyse




Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („**Schwellwertanalyse**“). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist **die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren**.

*LDA Bayern - XV III Datenschutz-Folgenabschätzung (DSFA)*

18 14.03.2018

# Schwellwertanalyse nach WP 248rev.01

**Regelbeispiele*** (nach WP 248, Art. 29-Gruppe)

1. Bewertung (Profiling) oder Scoring,
2. Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher erheblicher Wirkung
3. Systematische Überwachung
4. Sensible Daten oder hochpersönliche Daten (s. insbes. Art. 9,10)
5. Datenverarbeitung in großem Umfang
6. Datensätze (insbes. aus verschiedenen Prozessen) werden abgeglichen (match) oder kombiniert
7. Daten über „schutzbedürftige“ (vulnerable) Personen (s. insbes. EG 75)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Die Verarbeitung an sich "verhindert, dass die betroffenen Personen ein Recht ausüben oder eine Dienstleistung oder einen Vertrag ausüben" (s. insbes. Art. 22 und EG 91)

Liegen zwei oder mehr Regelbeispiele vor, ist regelmäßig von einer DSFA auszugehen

** Die Regelbeispiele werden im WP 248rev.01 näher erläutert*

*Art. 29 Gruppe, WP 248 Rev. 1*

19

14.03.2018

# Anwendung der Regelbeispiele (Auszug)

| Beispiele für Verarbeitungen | Mögliche relevante Kriterien | DSFA erforderlich? |
|---|---|---|
| Das Sammeln von Daten aus öffentlichen social media Profilen, die von privaten Unternehmen genutzt werden sollen, um Profile für Kontaktverzeichnisse zu erzeugen. | • Bewertung oder Scoring<br>• Datenverarbeitung in großem Umfang | **Ja** |
| Eine E-Commerce-Website zeigt Anzeigen für Oldtimer Teile unter Verwendung eines begrenzten Profiling auf der Basis früheren Kaufverhaltens auf bestimmte Teilen der Website. | • Bewertung oder Scoring, aber nicht systematisch oder umfangreich | **Nicht notwendig** |

*Art. 29 Gruppe, WP 248rev.01*

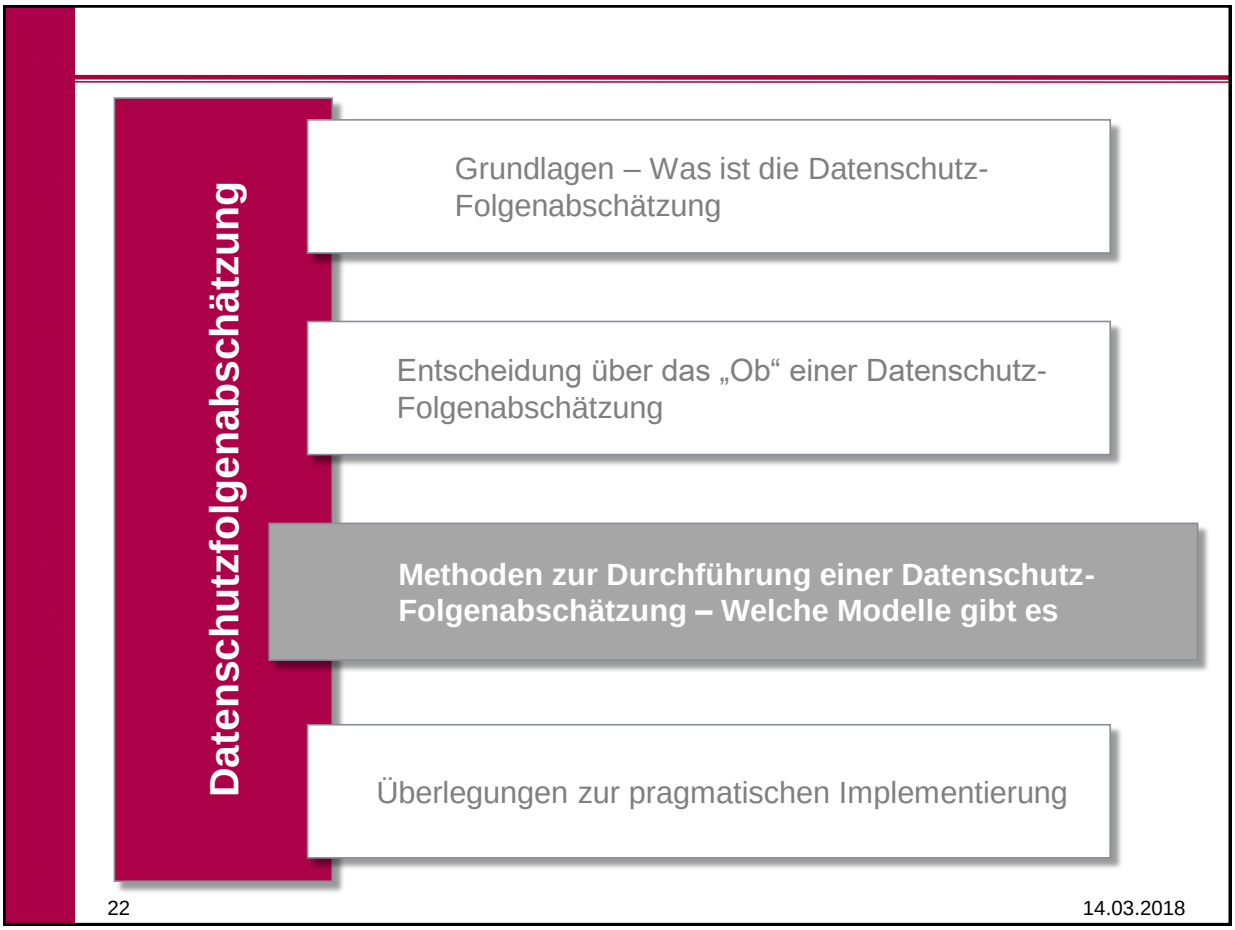
# Eine DSFA ist nicht erforderlich

| | |
|---|---|
| Kein hohes Risiko | Verarbeitung führt nicht zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen (Art. 35 Abs. 1) |
| DSFA für ähnliche Verarbeitungen | Für ähnliche Verarbeitungen wurde bereits eine DSFA durchgeführt wurde. Die Ergebnisse der durchgeführten DSFA können verwendet werden (Artikel 35 (1)); |
| Konkrete Rechtsgrundlage | Konkrete Rechtsgrundlage für die Verarbeitung im EU- oder Mitgliedstaatgesetz:<br>• Dort ist festgestellt, dass keine DSFA durchgeführt werden muss<br>• Gesetz regelt den konkreten Verarbeitungsvorgang und eine DSFA wurde bereits im Rahmen des Gesetzgebungsverfahrens durchgeführt (Artikel 35 Absatz 10). |
| Ausnahmeliste | Die Verarbeitung in einer Ausnahmeliste der Aufsichtsbehörde enthalten ist (Artikel 35 Absatz 5), aber nur, wenn die Verarbeitung strikt den in der Liste genannten einschlägigen Verfahren und Anforderungen entspricht |

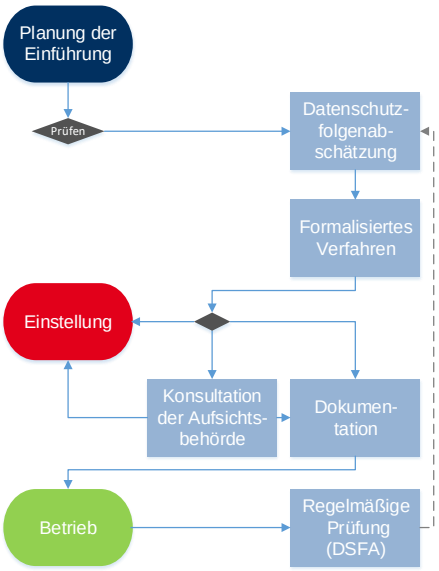
*Art. 29 Gruppe, WP 248rev.01*

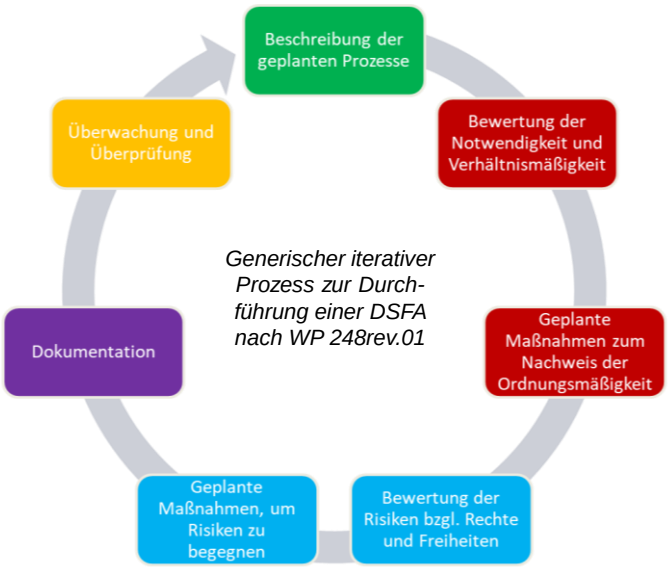
21

14.03.2018


Datenschutzfolgenabschätzung
Grundlagen – Was ist die Datenschutz-Folgenabschätzung
Entscheidung über das „Ob“ einer Datenschutz-Folgenabschätzung
Methoden zur Durchführung einer Datenschutz-Folgenabschätzung – Welche Modelle gibt es
Überlegungen zur pragmatischen Implementierung
22
14.03.2018

# Durchführung der DSFA




*Generischer iterativer Prozess zur Durch-führung einer DSFA nach WP 248rev.01*

*Art. 29 Gruppe, WP 248rev.01*

23

14.03.2018

# Bestandteile der DSFA

**Datenschutz-Folgenabschätzung enthält zumindest Folgendes**

- **Zwecke der Verarbeitung**, ggf. einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen
- systematische **Beschreibung** der geplanten Verarbeitungsvorgänge
- **Bewertung der Notwendigkeit** und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (**Risikonanalyse**)
- zur Bewältigung der Risiken geplante **Abhilfe(-/Sicherheits)maßnahmen**, einschließlich
  - Garantien
  - Sicherheitsvorkehrungen
  - Verfahren
- Maßnahmen, durch die der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden (**IKS**)

Erforderlich:

Vorgaben (Muster / Anleitungen) zur Durchführung durch den Verantwortlichen

# Methodik

Es gibt verschiedene Methoden, aber gemeinsame Kriterien. (*Art. 29 Gruppe, WP 248)*

**Beispiele für allgemeine Rahmen der EU:**

DE: Standard Datenschutzmodell, V.1.0 – Testversion, 2016.
*https://www.datenschutzzentrum.de/Uploads/SDM-Methodology_V1_EN1.PDF*

ES: Guía Para Una Evaluación de Impacto de la Protección de Datos Personales (EIPD), Agencia Española de Protección de Datos (AGPD), 2014.
*https://www.agpd.es/portalwebAGPD/canaldocumentacion/Publicaciones/Common/guias/Guia_EIPD.PDF*

FR: Privacy Impact Assessment (PIA), Kommission Nationale de l'informatique et des 1970er (CNIL), 2015.
*https://www.CNIL.fr/FR/Node/15798*

UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014.
*https://ICO.org.UK/Media/for-Organisations/Documents/1595/Pia-Code-of-Practice.PDF*

**Beispiele für EU branchenspezifische Rahmenbedingungen:**

Privacy and Data Protection Impact Assessment Framework for RFID Applications.
*http://ec.Europa.EU/Justice/Data-Protection/article-29/Documentation/Opinion-Recommendation/Files/2011/wp180_annex_en.PDF*

Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems.
*http://ec.Europa.EU/Energy/Sites/Ener/Files/Documents/2014_dpia_smart_grids_forces.PDF*

ISO: Ein internationaler Standard wird auch der ISO-Standard zu Methoden für die Durchführung einer DSFA (ISO/IEC 29134) sein.

*Art. 29 Gruppe, WP 248rev.01*

25 14.03.2018

# Deutschland



**Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive"-Verfahrens (V 0.10)**

Autoren: S. Gonscherowski, T. Herber, R. Robrahn[1], M. Rost, R. Weichelt
Kontakt: Martin Rost, uld32@datenschutzzentrum.de

**Inhalt**

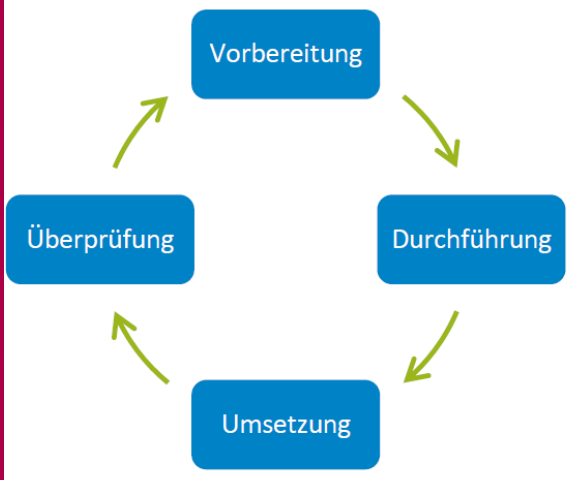


[1] Die Mitwirkung an der vorliegenden Datenschutz-Folgenabschätzung der Autoren Gonscherowski, Herber und Robrahn erfolgte im Rahmen von Forschungsprojekten, die mit Mitteln des Bundesministeriums für Bildung, und Forschung unter den Förderkennzeichen 16KIS0355 (VVV), 16 KIS0424 (PARADISE) sowie 16KIS0434 (SeDaFa) gefördert wurden. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

1

26 14.03.2018

# DSK – Hinweise zur Durchführung




## Vorbereitung

- Zusammenstellung des DSFA-Teams
- Prüfplanung
- Festlegung des Beurteilungsumfangs (Scope)
- Identifikation und Einbindung von Akteuren und betroffenen Personen
- Bewertung der Notwendigkeit/Verhältnismäßigkeit in Bezug auf Zweck
- Identifikation der Rechtsgrundlagen

27 *DSK - Kurzpapier Nr. 5 : Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO* 14.03.2018

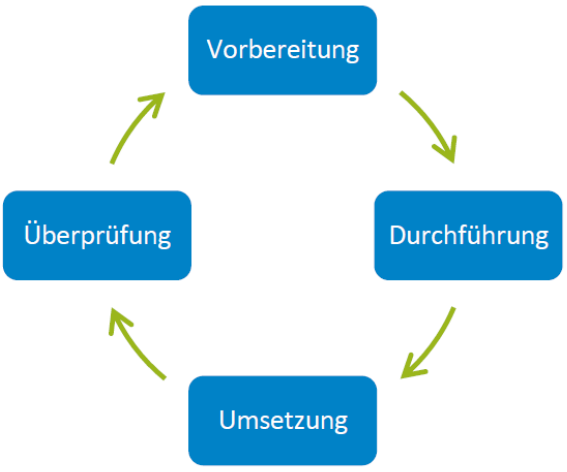
# DSK – Hinweise zur Durchführung


## Durchführung

- Modellierung der Risikoquellen
- Risikobeurteilung
- Auswahl geeigneter Abhilfemaßnahmen
- Erstellung des DSFA-Berichts

28 *DSK - Kurzpapier Nr. 5 : Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO* 14.03.2018

# DSK – Hinweise zur Durchführung




**Umsetzung**

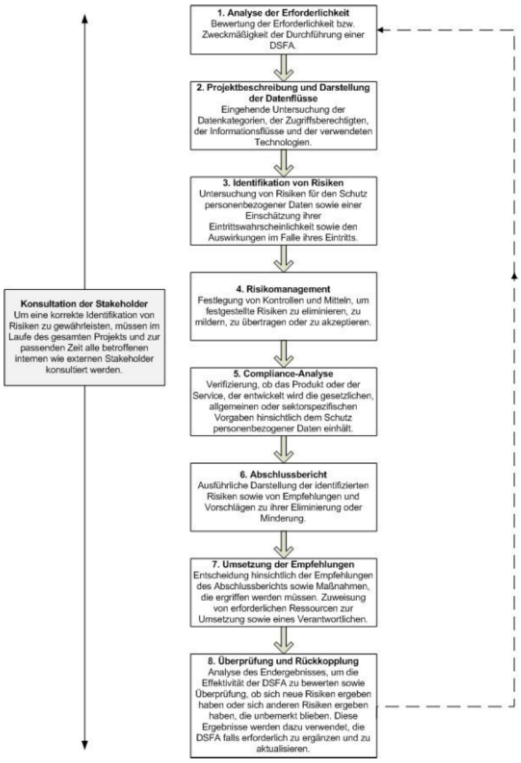
- Umsetzung der Abhilfemaßnahmen
- Test der Abhilfemaßnamen
- Dokumentation: Nachweis über die Einhaltung der DS-GVO
- Freigabe der Verarbeitungsvorgänge

**Überprüfung**

- Ggf. Überprüfung und Audit der DSFA
- Fortschreibung

29 *DSK - Kurzpapier Nr. 5 : Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO* 14.03.2018

# Spanien




**Die Datenschutz-Folgenabschätzung**
Zusammenfassung des Leitfadens der spanischen Aufsichtsbehörde "AEPD" - Guía para una Evaluación de Impacto en la Protección de Datos Personales"

*https://www.gdd.de/aktuelles/startseite/die-datenschutz-folgenabschaetzung-zusammenfassung-des-leitfadens-der-spanischen-aufsichtsbehoerde-aepd*

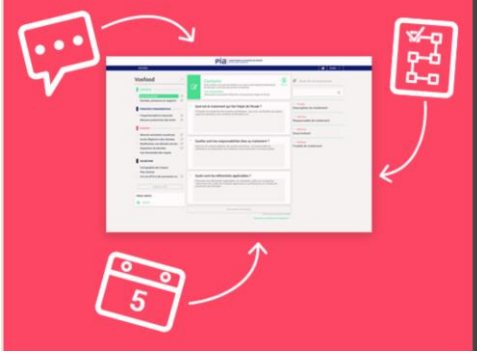
30 14.03.2018

# Frankreich

CNIL.

*To protect personal data, support innovation, preserve individual liberties*

pia | **analyse d'impact sur la protection des données**
privacy impact assessment

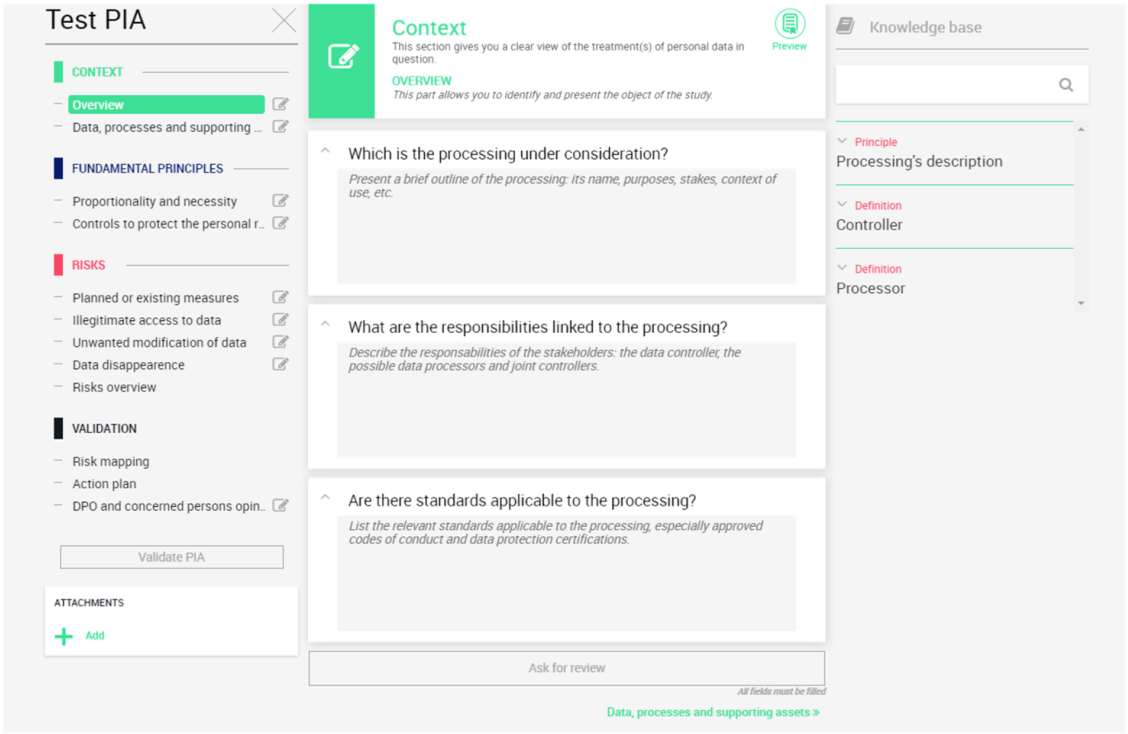


**A MODULAR TOOL:**

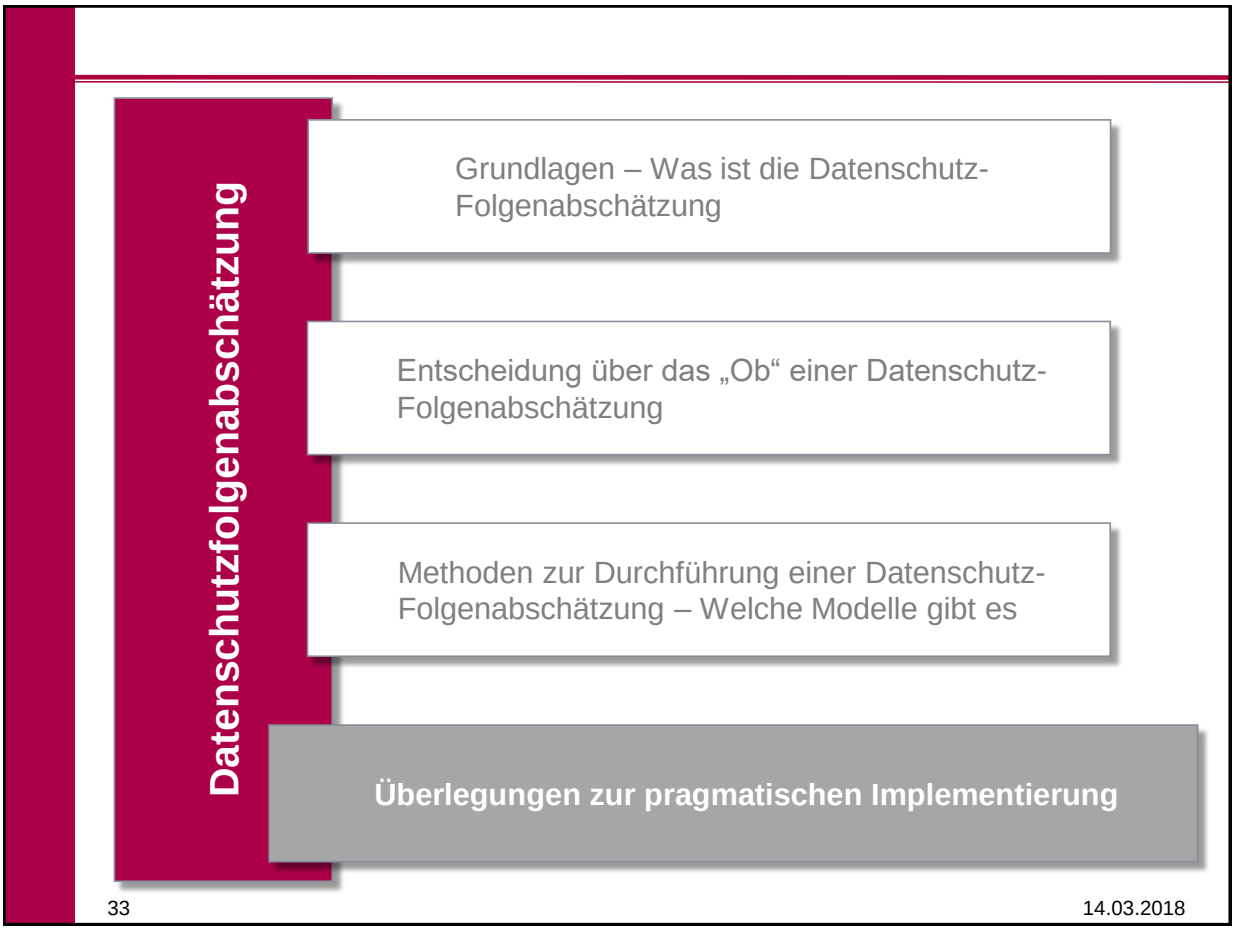
Designed to help you build your compliance, you can customise the tool contents to your specific needs or business sector, for example by creating a PIA model that you can duplicate and use for a set of similar processing operations. Published under a free licence, it is possible to modify the source code of the tool in order to add features or include it into tools used in your organisation.

*https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment*

## PIA Privacy Impact Assessment – CNIL 6.12.2017 Betaversion




32 14.03.2018


Datenschutzfolgenabschätzung
Grundlagen – Was ist die Datenschutz-Folgenabschätzung
Entscheidung über das „Ob“ einer Datenschutz-Folgenabschätzung
Methoden zur Durchführung einer Datenschutz-Folgenabschätzung – Welche Modelle gibt es
Überlegungen zur pragmatischen Implementierung
33
14.03.2018

# Prüfschritte GDD

**Erster Schritt: Rechtmäßigkeit**

Findet sich ein Erlaubnistatbestand für die geplante Verarbeitung?
Wenn nein: Prüfung beendet.

**Zweiter Schritt: Pflicht zur DSFA?**

- Ist die Verarbeitung gewhitelistet gem. Art. 35 Abs. 5 DS-GVO?
  Wenn ja: keine DSFA notwendig, Prüfung beendet.
- Liegt bereits eine vorweggenommene Folgenabschätzung im Sinne des Art. 35 Abs. 10 DS-GVO vor und hat der Mitgliedsstaat keine darüber hinausgehende DSFA angeordnet?
  Wenn ja: keine DSFA notwendig, Prüfung beendet.
- Liegt bereits eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohem Risiko im Sinne von Art. 35 Abs. 1 Satz 2 DSGVO vor?
  Wenn ja: keine DSFA notwendig, Prüfung beendet.
- Ist die Verarbeitung geblacklistet gem. Art. 35 Abs. 4 DS-GVO?
  Wenn ja: DSFA notwendig, weiter mit Schritt Drei

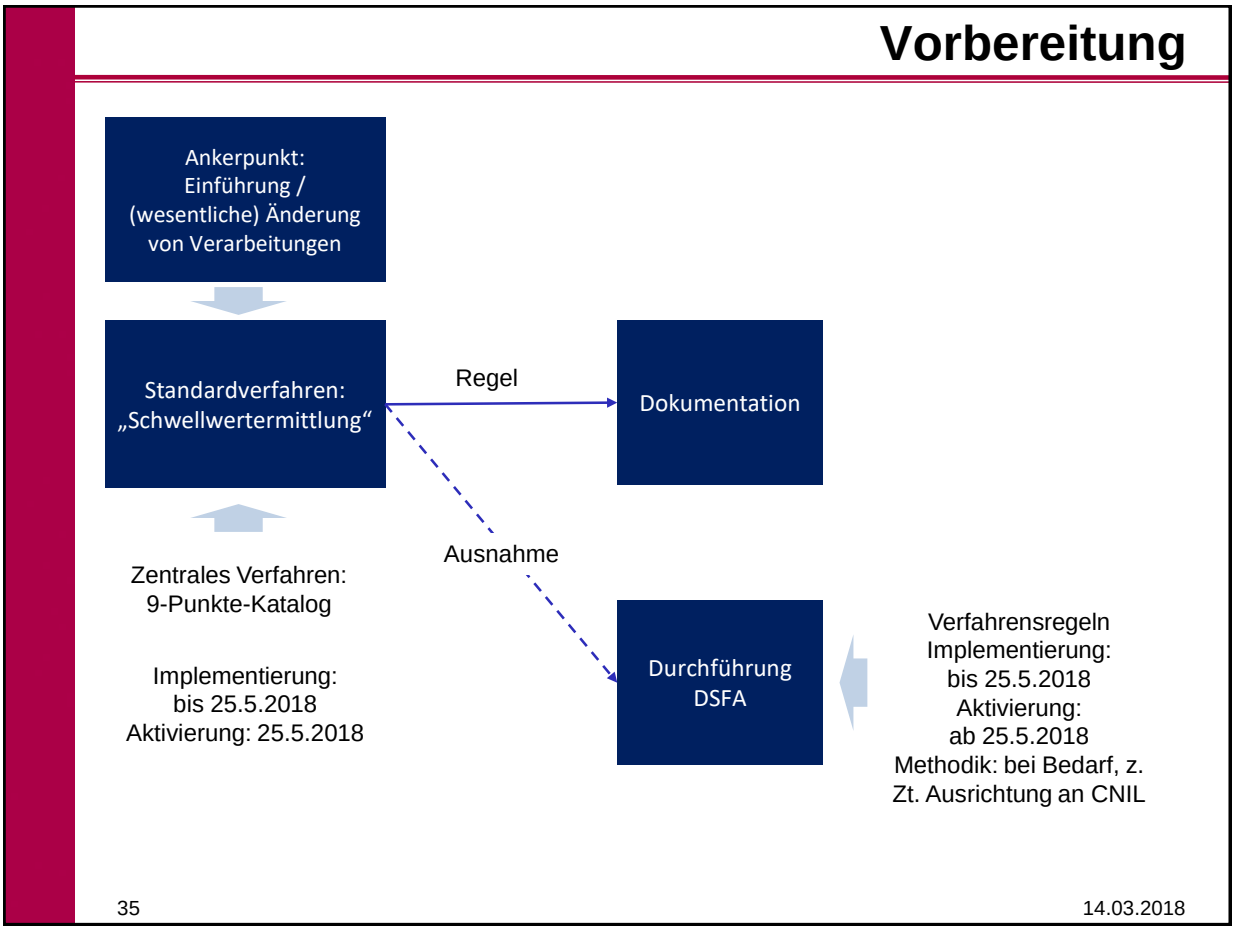
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen?

- Ist eine der Fallgruppen des Art. 35 Abs. 3 litt. a bis c DS-GVO erfüllt?
  Wenn ja: DSFA notwendig, weiter mit Schritt Drei.
- Ist ein sonstiges hohes Risiko im Sinne des Art. 35 Abs. 1 DS-GVO erkennbar? (Mögliche Anknüpfungspunkte: eigene Checkliste des DSB, eigene Checkliste des Fachbereichs, Checkliste nach WP 248 der Artikel-29-Gruppe)
  Wenn ja: DSFA notwendig, weiter mit Schritt Drei

**Dritter Schritt: Durchführung der DSFA**

Die DSFA besteht zumindest aus den in Art. 35 Abs. 7 litt a bis d DS-GVO niedergelegten Punkten. Derzeit sind mehrere Modelle in der Diskussion, wie bei einer DSFA am besten vorzugehen sei.

34 14.03.2018


Vorbereitung
Ankerpunkt:
Einführung /
(wesentliche) Änderung
von Verarbeitungen
Standardverfahren:
„Schwellwertermittlung“
Regel
Dokumentation
Ausnahme
Zentrales Verfahren:
9-Punkte-Katalog
Implementierung:
bis 25.5.2018
Aktivierung: 25.5.2018
Durchführung
DSFA
Verfahrensregeln
Implementierung:
bis 25.5.2018
Aktivierung:
ab 25.5.2018
Methodik: bei Bedarf, z.
Zt. Ausrichtung an CNIL
35
14.03.2018

# Organisatorische Regelungen

**Regelung zur Schwellwertermittlung:**

- Definition Ankerpunkt
- Verantwortlichkeit
- Vorbereitung Checkliste
- Gegen-Prüfung (insbes. White-/Blacklist)

**Durchführung einer Datenschutz-Folgenabschätzung:**

Vorbereitende Regelungen zu:

- Zu Durchlaufende Phasen einer Datenschutz-Folgenabschätzung (DSFA)
- Team für die Datenschutz-Folgenabschätzung
  - Verantwortung zur Zusammenstellung / Durchführung / Einbeziehung DSB
- Standpunkt der Betroffenen
  - BR, Studien etc.
- Methode zur Durchführung der DSFA
  - Offene Formulierung, Rückgriff auf CNIL
- DSFA-Bericht
  - Elemente, CNIL-Tool sieht Berichtsformat vor
- Konsultationsverfahren
  - Offene Formulierung
  - Genehmigungsvorbehalte der Unternehmensleitung?

36 14.03.2018

## Der DSB bei der Datenschutzfolgeabschätzung

**Es ist die Aufgabe des Verantwortlichen, nicht des DSB, eine Datenschutzfolgeabschätzung falls erforderlich durchzuführen**

Der Verantwortliche sollte den Rat des DSB insbesondere zu den folgenden Fragestellungen einholen:

- Ob eine Datenschutzfolgeabschätzung **durchzuführen** ist
- Mit welcher **Methodik** bei der Durchführung einer Datenschutzfolgeabschätzung vorgegangen werden soll
- Ob eine Datenschutzfolgeabschätzung in der Organisation durchgeführt wird oder ob diese **extern vergeben** wird
- Welche **Garantien** (einschließlich technisch-organisatorischer Maßnahmen) anzuwenden sind, um das Risiko für die Rechte und Interessen der betroffenen Personen zu mindern
- Ob eine Datenschutzfolgeabschätzung ordnungsgemäß durchgeführt und ob ihre **Schlussforderungen** (ob die Verarbeitung fortgeführt werden soll und welche Garantien angewendet werden) im Einklang mit der DS-GVO stehen. (Falls dem Rat des DSBs nicht gefolgt wird, sollte ausdrücklich dokumentiert werden, warum der Rat nicht berücksichtigt wurde.)

*Art. 29 Gruppe, WP 243rev.01*

37 14.03.2018

*Datenschutzfolgenabschätzung*

# Und was können wir für Sie tun?


**DMC Datenschutz Management & Consulting GmbH & Co. KG**

Zur Mühle 2-4, D-50226 Köln-Frechen

Telefon +49.2234.964944-0
Fax +49.2234.964944-19

E-Mail info@dmc-datenschutz.de
Internet www.dmc-datenschutz.de

38 14.03.2018