Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO XIV

Die Datenschutz-Folgenabschätzung

Zusammenfassung des Leitfadens der spanischen Aufsichtsbehörde „AEPD“
– Guía para una Evaluación de Impacto en la Protección de Datos Personales

Die Datenschutz-Folgenabschätzung

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

Die praktische Durchführung der Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO ist derzeit zum Teil noch unklar.[1] Der Arbeitskreis der GDD „Datenschutz International“ möchte daher bestehende Ansätze für eine Folgenabschätzung beleuchten, um die europäischen Diskussionen hierzu voranzubringen. Die jeweilige Darstellung ist eine Zusammenfassung. Sie enthält Ideen und Anregungen, die für die Durchführung einer Datenschutz-Folgenabschätzung nach der DS-GVO verwendet werden können.

Die erste Darstellung der Serie widmet sich dem Ratgeber zur Datenschutz-Folgenabschätzung der spanischen Aufsichtsbehörde „AEPD“ aus dem Jahr 2014, auf den auch im WP248 der Artikel-29-Datenschutzgruppe verwiesen wird.

[1] Hinweise zur Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung finden sich in der GDD-Praxishilfe X - Voraussetzungen der Datenschutz-Folgenabschätzung, abrufbar unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf.

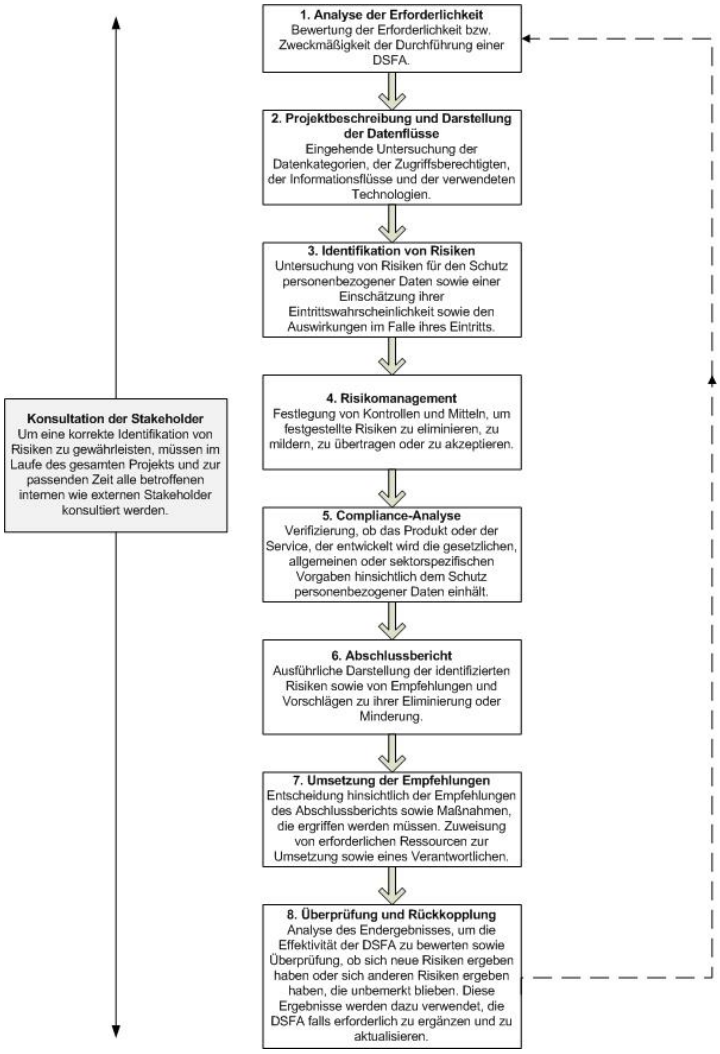
Allgemeines

Die spanische Aufsicht hat sich bereits im Jahr 2014 mit einer systematischen Bewertung der Auswirkungen auf den Schutz personenbezogener Daten in Form einer Datenschutz-Folgenabschätzung befasst und die Ergebnisse in einem Leitfaden zusammengefasst. Eine systematische Bewertung von Datenschutzrisiken ist in den Augen der Behörde unabdingbar, um den sich ständig weiter entwickelnden Technologien und dem damit verbundenen massiven Umgang mit personenbezogenen Daten wirksam zu begegnen, das Vertrauen der Betroffenen in die Datenverarbeitung des Verantwortlichen zu stärken und Verantwortliche mehr in die Pflicht zu nehmen.

Hierbei sei es wichtig, Fragestellungen zum Schutz personenbezogener Daten bereits in der initialen Projektphase zu klären und zu bewerten, um zu verhindern, dass bereits laufende Projekte, die sich nach einer späteren Begutachtung als unzulässig darstellen oder bereits Rechte von Betroffenen verletzen, unter hohen Kosten datenschutzkonform ausgestaltet werden müssen. Hierbei könnte die Datenschutz-Folgenabschätzung einen wichtigen Beitrag leisten.

Phasen einer Datenschutz-Folgenabschätzung

Jede Datenschutz-Folgenabschätzung beginnt mit einer **Analyse** in Gestalt der **Identifikation und Klassifikation der personenbezogenen Daten**. Hieran schließt sich der folgende Prozess an:



Beteiligte

An der Durchführung einer Datenschutz-Folgenabschätzung ist in der Regel ein **interdisziplinäres Team** beteiligt mit Ansprechpartnern im Projekt und der Leitungsebene. Eine Unterstützung durch das obere Management ist für den Erfolg der Durchführung wichtig. Unverzichtbare Beteiligte sind:

- Projektverantwortlicher mit Entscheidungsbefugnissen
- Datenschutzbeauftragter oder Verantwortliche für den Datenschutz bzw. Berater
- Verantwortlicher für die Informationssicherheit
- Vertreter der Informations- und Kommunikationstechnik
- Vertreter von Fachbereichen oder Geschäftsfeldern, die vom Projekt am meisten betroffen sind

Inhalte

Elementare Inhalte einer Datenschutz-Folgenabschätzung sind:

- **Projektbeschreibung**, einschließlich einer Beschreibung seines Nutzens und der damit verbundenen Möglichkeiten für das Unternehmen.
- **Identifikation datenschutzrelevanter Aspekte** des Projekts, einschließlich solcher, die empfänglich für ein erhöhtes Risiko für den Betroffenen sind oder die Einhaltung gesetzlicher Vorgaben erschweren (z.B. eine Profilbildung, die Verarbeitung besonderer Arten personenbezogener Daten, Entscheidungen oder Handlungen, die Auswirkungen auf die Betroffenen haben oder Verarbeitungen, die im besonderen Maße in die Privatsphäre eingreifen).
- **Eine detaillierte Beschreibung**
  - der Mittel der Datenverarbeitung und der verwendeten Technologien, insbesondere solche, die ein höheres Risiko für die Persönlichkeitsrechte der Betroffenen mit sich bringen,
  - der Datenkategorien sowie der damit verbundenen Zwecke ihrer Verarbeitung, der Notwendigkeit ihrer Verarbeitung und den Kategorien von betroffenen Personen,
  - der Empfänger der Datenkategorien und die Zwecke sowie Notwendigkeiten für einen solchen Zugriff,
  - der Datenflüsse, einschließlich Erhebung, Weitergabe innerhalb der Organisation sowie Übermittlungen an Empfänger außerhalb der Organisation sowie Weiterübermittlungen an andere Organisationen.
- Falls erforderlich, können zusätzliche Informationen oder Schaubilder verwendet werden, um Aspekte wie beispielsweise die Zugangskontrolle oder die Aufbewahrung oder Löschung von personenbezogenen Daten zu illustrieren.

Risikomanagement

Das Modell der spanischen Aufsichtsbehörde unterteilt das Risiko für den Schutz personenbezogener Daten von betroffenen Personen in insgesamt **11 Kategorien**. Hierbei wird der Schwerpunkt auf die Nichteinhaltung gesetzlicher Risiken des noch gültigen spanischen Datenschutzgesetzes „LOPD“ gelegt. Die identifizierten Risikokategorien werden im Folgenden teilweise dargelegt und mit einer Beschreibung ausgewählter einzelner Risiken sowie etwaiger Gegenmaßnahmen versehen.

- **Allgemeine Risiken**

  Zu den allgemeinen Risiken zählen **Reputationsschäden** ebenso, wie **wirtschaftliche Einbußen** durch eine unzulässige Datenverarbeitung. Erforderliche Gegenmaßnahmen bestehen insbesondere in einer klaren und transparenten Aufgabenzuweisung zur Einhaltung der gesetzlichen Vorgaben. Ebenso muss ein angemessener Umgang mit der vorhandenen Informations- und Kommunikationstechnologie gewährleitet sein. Zu den allgemeinen Risiken soll aber auch ein nicht vorhandenes **Expertenwissen zum Datenschutz** zählen, das z.B. mittels der Bestellung eines **Datenschutzbeauftragten** kompensiert werden kann. Das Risiko einer verspäteten Einbindung des Datenschutzbeauftragten in die Projekte der verantwortlichen Stelle kann durch seine Positionierung in der Entwicklungsphase begegnet werden. Kanäle zum Betroffenen müssen ebenfalls eingerichtet sein, um dem Risiko fehlender Informationen zu begegnen.

- **Legitimation einer Verarbeitung bzw. Übermittlung personenbezogener Daten**

  Im Rahmen der Legitimation von Datenverarbeitungen bestehen die allgemeinen Risiken eines **Zweckverbrauchs**, einer **nicht eindeutigen Rechtsgrundlage** sowie einer **unwirksamen Einwilligung des Betroffenen.** Hierzu soll auch das Erschweren der Ausübung von **Widerspruchsrechten** zählen. Im Zuge einer **Datenerhebung von Dritten** muss sowohl die Datenübermittlung durch den Dritten als auch der Erhalt der personenbezogenen Daten rechtmäßig sein. Bei der Durchführung von **Werbekampagnen** mit Daten von Dritten, bei denen Zielgruppen selektiert werden müssen, muss dem Risiko einer unrechtmäßigen Datenverarbeitung durch das Einholen einer Einwilligung des von der Selektion Betroffenen begegnet werden.

- **Internationale Datenflüsse**

  Dem Risiko der **behördlichen Zugriffe in Drittländern** ist durch Vertragsklauseln, die eine Informationspflicht begründen, falls es zu solchen Zugriffen kommt, zu begegnen. Auch die besondere

Problemstellung bei einem Datenhosting bei Dritten sowie dem Cloud-Computing ist zu berücksichtigen. Die **Auftragskontrolle** muss durch den Datenimporteur ermöglicht werden können, so über die Bereitstellung von Aufstellungen seiner weiteren Auftragsverarbeiter inklusive Standort, die Möglichkeit der Einsichtnahme in relevante Dokumentationen sowie die Möglichkeit der Durchführung von Audits. Auch **Kommunikationskanäle zu den Betroffenen** sind zu realisieren. Möglicherweise besteht die Pflicht zur **Genehmigung** des Drittlandstransfers.

- **Transparenz der Datenverarbeitung**

  Betroffene müssen über die Verwendung und die Zwecke personenbezogener Daten **informiert werden**. Insbesondere wenn es sich um den Einsatz von Cookies handelt.

  Dem Risiko einer **verstreuten Information** von Betroffenen über eine Webseite ist wirksam zu begegnen. Hierbei sollten verschiedene **Informationsebenen** eingeführt werden, die für Betroffene leicht zugänglich sind. Mit Blick auf eine leichtere Verständlichkeit können **Icons oder andere grafische Symbole** verwendet werden.

- **Datenqualität**

  Nicht relevante Daten hinsichtlich der avisierten Zwecke dürfen nicht angefordert werden. Umfassende **Datenflussdiagramme** helfen, dass Daten nicht angefordert werden, die später in keinem Prozess verwendet werden. **Doppelt geführte Datenbestände** mit unterschiedlichen oder widersprüchlichen Daten, die zu fehlerhaften Entscheidungen führen können, sind abzustellen. Daher muss die **Aktualisierung von Datenbeständen** zu einer Information an alle Systeme sowie Abteilungen führen, die zur Verwendung der Daten befugt sind.

  Bei der Verarbeitung personenbezogener Daten für **historische, wissenschaftliche oder statistische Zwecke** sollte, falls möglich, auf eine anonyme oder auf eine von einer betroffenen Person entkoppelte Verarbeitung zurückgegriffen werden. Auch die **Pseudonymisierung** kann als wirksame Maßnahme eingesetzt werden, um dafür zu sorgen, dass ein Zugang zur Identität von Betroffenen nur einem begrenzten Nutzerkreis möglich ist.

  Um eine Verarbeitung personenbezogener Daten **ohne feste Zweckbindung oder zu inkompatiblen Zwecken** zu verhindern, bedarf es einer eindeutigen Information über die beabsichtigten Verwendungszwecke, so über eine Datenschutzerklärung.

  Im Zuge von **wirtschaftlichen, sozialen oder arbeitsrechtlichen Entscheidungen** auf Basis personenbezogener Daten, insbesondere bei besonders schützenswerten Personengruppen wie Kindern, mental Erkrankten oder bei Erkrankungen, die eine soziale Ausgrenzung begründen können, müssen Informationen über die Kriterien der Entscheidungsfindung zur Verfügung gestellt werden und den Betroffenen die Möglichkeit gegebenen werden, die Entscheidung anzufechten sowie die Überprüfung dieser Entscheidung durch eine natürliche Person zu verlangen. Ebenfalls muss über die eingesetzten Mittel bzw. Garantien informiert werden, um den notwendigen Ausgleich zwischen dem berechtigten Interesse des Verantwortlichen und den Rechten der Betroffenen herzustellen.

  Um fehlerhafte Schlussfolgerungen auf Basis von **Techniken der künstlichen Intelligenz (insbesondere das Data Mining)**, der Gesichtserkennung und biometrischer Analysen auszuschließen, bedarf es Mechanismen und Verfahren, die schnell und effizient Fehler im Zuge der Anwendung der Technologien beheben können. Anfechtungsmöglichkeiten sowie (Rechts-)Behelfe für den Betroffenen gehören hierzu. Alternative Mittel, um mit falschen negativen Befunden und falschen positiven Befunde im Zuge der **Identifikation und Authentifizierung mittels biometrischer Daten** umzugehen, sind vorhanden. Eindeutige Prozesse und angemessene Werkzeuge sorgen dafür, dass Daten, die für die Zweckerreichung nicht mehr erforderlich sind, gelöscht werden.

- **Besonders geschützte Daten**

  Fehler beim Einholen einer **Einwilligungserklärung** sind zu vermeiden. Prozesse, die garantieren, dass die Einwilligung ausdrücklich (sowie schriftlich, falls geboten) eingeholt worden ist, müssen bestehen. Hierzu gehören Prüfmöglichkeiten für bestehende Verarbeitungen. Einer unzureichenden Anonymisierung personenbezoge-

ner Daten bei der Verfolgung von **Forschungszwecken** muss durch geeignete Techniken begegnet werden, die eine faktische Anonymisierung gewährleisten können oder zumindest das Risiko einer Re-Identifizierung auf ein Minimum reduzieren.

- **Vertraulichkeit von Daten**

  Um die Vertraulichkeit von Daten zu wahren, bestehen Sensibilisierungsmaßnahmen hinsichtlich der Pflicht eines Beschäftigten zum vertraulichen Umgang mit Daten, die ihm/ihr im Rahmen einer Tätigkeit offenbart werden. Sanktionsmaßnahmen bestehen, um **Verstöße gegen einen vertraulichen Umgang** zu ahnden. Ebenso wird darüber informiert, dass Verstöße hinsichtlich eines vertraulichen Umgangs mit Daten den zuständigen Behörden angezeigt werden, was mit strafrechtlichen Konsequenzen verbunden sein kann. Prozesse **zur Vernichtung ausrangierter Datenträger** mit personenbezogenen Daten bestehen.

- **Auftragsdatenverarbeitung**

  Ein Vertrag zur Auftragsdatenverarbeitung nach den Vorgaben der Datenschutzgesetze wird geschlossen. Dem Risiko einer **nicht sorgfältigen Auswahl von Dienstleistern** wird durch eingerichtete Prozesse begegnet, die das Vorhandensein von **Garantien** für die Vertragserfüllung sicherstellen können, so beispielsweise die Einhaltung von Verhaltensregeln, eine Zertifizierung sowie einer nachgewiesenen Liquidität. **Prüfrechte und Prüfmechanismen** wurden vertraglich vereinbart. Auftragsverarbeiter werden regelmäßig kontrolliert, um die vertraglichen Vereinbarungen zu überprüfen. Die Kontrolle des Verantwortlichen von **Subunternehmern** muss gewährleistet sein.

- **Betroffenenrechte**

  Es müssen Systeme sowie Prozesse implementiert sein, die den Betroffenen einen einfachen, direkten und mit angemessenen Schutzmaßnahmen versehenen **Zugang zu ihren personenbezogenen Daten** gestatten sowie die Ausübung der Betroffenenrechte insgesamt (**Berichtigung, Löschung, Widerspruch**) ermöglichen. Verantwortlichkeiten für die Bearbeitung von Betroffenenbegehren müssen definiert sein. Die Beschäftigten müssen geschult sein, wie mit der Ausübung von Betroffenenrechten umzugehen ist.

- **Datensicherheit**

  Ein **Sicherheitsverantwortlicher** wird durch die Geschäftsleitung ernannt und bereits in die Entwicklung von Projekten einbezogen. Organisatorische Maßnahmen zur **Zugangs- bzw. Zugriffskontrolle** beinhalten strenge Vorgaben für einen Datenzugriff nach dem „need to know" Prinzip. Eine „Clean Desk Policy" sorgt dafür, dass die Möglichkeit eines unbefugten Zugangs zu Daten minimiert wird. Prozesse sorgen dafür, dass **Berechtigungen** für einen Zugang bzw. Zugriff auf Daten bei einem Ausscheiden eines Mitarbeiters, der Versetzung oder im Falle einer geänderten Stellenbeschreibung entzogen werden. Ressourcen mit personenbezogenen Daten, die über Telekommunikationsnetze erreichbar sind, werden **inventarisiert**.

  Hard- und Software sorgen dafür, dass die Datensicherheit effizient in der Organisation implementiert ist und rechtliche Vorgaben des Datenschutzes eingehalten werden. Falls erforderlich, werden Intrusion Detection, Intrusion Prevention und Data Loss Prevention Systeme installiert. Die Beschäftigten sind hinsichtlich ihrer Installation, Charakteristika und Auswirkungen auf den Schutz personenbezogener Daten zu informieren. **Protokolle** sorgen dafür, dass Nutzerhandlungen einer Person zugewiesen werden können. Bei der Passwortvergabe wird dafür gesorgt, dass solche Kennungen keine Informationen über den Nutzer offenbaren (z.B. Geburtsdatum, Kreditkartennummer etc.). Angemessene **Verschlüsselungsmaßnahmen** sorgen dafür, dass Daten, die über Telekommunikationsnetze gespeichert bzw. weitergegeben werden, geschützt sind.

  Datenpannen werden dem Betroffenen einschließlich Hinweisen zur Vermeidung solcher Risiken gemeldet. Ebenso wird die zuständige behördliche Kontrollinstanz, falls gesetzlich vorgeschrieben, informiert. **Testverfahren** mit personenbezogenen Echtdaten sind zu vermeiden, insbesondere, wenn es sich um besonders schüt-

zenswerte Daten handelt oder solche, die die Aspekte der Persönlichkeit eines Betroffenen offenbaren. **Sichere Kanäle** sind etabliert, die für eine Identitätsprüfung von Nutzern sorgen (Benutzername, Passwort etc.). Beschäftigte sind über sie betreffende notwendige Sicherheitsmaßnahmen zu informieren. Dies schließt Informationen über die Konsequenzen einer Nichtbeachtung mit ein.

Alle Maßnahmen zur Begegnung von Risiken für den Schutz personenbezogener Daten müssen **regelmäßig überwacht** werden, damit diese effektiv sind und den Zwecken, für die sie implementiert wurden, noch entsprechen. Im Falle von **Zweckänderungen** sind die Maßnahmen entsprechend anzupassen.

Bericht

Die Ergebnisse einer Datenschutz-Folgenabschätzung sollten in der Organisation **veröffentlicht werden**, es sei denn es bestehen rechtliche Restriktionen diesbezüglich. Die Veröffentlichung kann beispielsweise über die eigene Webseite erfolgen. Essenzielle **Bestandteile des Berichts** sind:

- Datum und Version des Berichts
- Eindeutige Bezeichnung des Projekts sowie die verantwortlichen Personen der Datenschutz-Folgenabschätzung einschließlich ihrer Kontaktdaten
- Wesentliche Ergebnisse der Datenschutz-Folgenabschätzung
- Allgemeine Beschreibung der zugrunde gelegten Prüftechnik
- Ergebnis der Analyse der Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung einschließlich einer Begründung
- Allgemeine Beschreibung des Projekts (es könnten weitere relevante Dokumente des Projekts beigefügt werden)
- Detaillierte Beschreibung der Datenflüsse
- Identifizierte Risiken
- Identifikation der Stakeholder oder der vom Projekt Betroffenen (intern sowie extern) und die Ergebnisse der Konsultationen dieser Personengruppen
- Analyse der Einhaltung der gesetzlichen Bestimmungen sowie identifizierte Abweichungen und Lösungsvorschläge
- Empfehlungen der Verantwortlichen zur Durchführung der Datenschutz-Folgenabschätzung sowie einer Aufzählung der durchgeführten Maßnahmen bzw. vorgeschlagenen Maßnahmen für die Designphase, um die Risiken für die Rechte und Interessen der Betroffenen sowie der Risiken für die Organisation zu eliminieren oder zu verhindern, zu verringern, zu verlagern oder zu akzeptieren.

Weitere Inhalte des Prüfberichts sind möglich, so beispielsweise in Gestalt einer **Kosten-Nutzenanalyse** der vorgeschlagenen Maßnahmen. Im Übrigen sollte auf eine einfache und klare Sprache im Bericht geachtet werden. Hierzu bietet sich ein **Glossar** der verwendeten Fachbegriffe an.

Der finale Bericht muss der **Geschäftsleitung** der Organisation **zur Verfügung gestellt werden**, damit sie die notwendigen Entscheidungen hinsichtlich der bestehenden Empfehlungen sowie der vorgeschlagenen Maßnahmen trifft. Hintergrund der Vorlage ist, dass die Geschäftsleitung letztlich die Entscheidung hinsichtlich der einzuleitenden Maßnahmen trifft.

Ferner ist die Person bzw. Personengruppe festzulegen, die die **Implementierung** der empfohlenen Maßnahmen **überwacht**. Und, damit die Aufwände effizient sind, muss diese Person bzw. Personengruppe mit der notwendigen Befugnis zur Erfüllung der Aufgaben ausgestattet und ihr die Möglichkeit gegeben werden, die **Fortschritte und Schwierigkeiten** ihrer Arbeit an die **Geschäftsleitung zu kommunizieren**.

Da die Maßnahmen verschiedenartig ausfallen können (organisatorisch, technisch, vertraglich etc.), existiert keine abschließende Methode, wie die Maßnahmen auszuführen sind. Jede Organisation muss entscheiden, welche Methode die geeigneteste für sie ist. Bei der Beauftragung von **Dienstleistern** sind Kontrollmechanismen zu etablieren, um sicherzustellen, dass der Dienstleister die Maßnahmen tatsächlich umsetzt.

Überprüfung der Ergebnisse

Nach den Empfehlungen aus der Datenschutz-Folgenabschätzung und nach der Implementierung von Maßnahmen ist zu überprüfen, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird. Hierzu ist es erforderlich, dass das jeweilige Projekt **im operativen Betrieb** analysiert wird, ob die festgestellten Risiken korrekt ausgeräumt wurden und dass keine neuen Risiken bestehen oder unbeachtet blieben, was

mit einem **erneuten Durchschreiten der Phasen einer Datenschutz-Folgenabschätzung** verbunden wäre. Änderungen bei den implementierten Maßnahmen oder im Falle neuer Funktionalitäten sorgen dafür, dass die Datenschutz-Folgenabschätzung überprüft werden muss. Diese Überprüfung kann extensiver oder von geringerem Umfang sein, je nach Umfang der Änderungen. Bei der Entwicklung und Durchführung einer Datenschutz-Folgenabschätzung muss der **PDCA-Lebenszyklus** eines Managementsystems (Plan, Do, Check, Act) Beachtung finden.

Anlagen

Modell zur Beschreibung der Datenflüsse

ID	Beschreibung	Ursprung der Daten	Ziel(e) der Daten	Datenkategorien	Zweck	Rechtfertigungsgrund
1						
2						
3						
...						

Risikomanagement

ID	Beschreibung des Risikos	Grad der Auswirkung, falls das Risiko eintritt	Eintrittswahrscheinlichkeit	Vorgeschlagene Maßnahmen	Auswirkungen nach Implementierung der vorgeschlagenen Maßnahmen	Eintrittswahrscheinlichkeit nach Implementierung der vorgeschlagenen Maßnahmen
1						
2						
3						
...						

Grad der Auswirkung auf die Rechte und Interessen der Betroffenen bzw. der Organisation

- *Sehr hoch*
- *Hoch*
- *Mittel*
- *Niedrig*
- *Sehr niedrig*

Möglich wäre auch eine numerische Bestimmung der Auswirkungen (z.B. 0-10).

Grad der Auswirkung, falls das Risiko eintritt

- *Sehr hoch (81%-100%)*
- *Hoch (61%-80%)*
- *Mittel (41%-60%)*
- *Niedrig 21%-40%)*
- *Sehr niedrig (0%-20%)*

Muster für den Bericht einer Datenschutz-Folgenabschätzung

A. Identifizierung/Name des Projekts

I. Kennziffer

II. Beschreibung

III. Projektverantwortliche und Kontaktdaten

IV. Berichtsdatum

V. Version

B. Management Summary

I. Kurzbeschreibung des Projekts

II. Identifizierte Hauptrisiken

III. Übersicht der wichtigsten vorgeschlagenen Maßnahmen zur Risikominimierung

C. Analyse der Notwendigkeit einer Datenschutz-Folgenabschätzung

I. Ergebnis der Analyse

II. Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung

D. Detaillierte Projektbeschreibung

I. Berücksichtigung aller relevanten Informationen zum Projekt (mit der Möglichkeit begleitende Dokumente anzufügen)

II. Detaillierte Beschreibung der Datenflüsse

E. Ergebnis der Konsultationen

I. Identifikation der Stakeholder (interne und externe) oder der vom Projekt betroffenen Personen

II. Beiträge der konsultierten Parteien (können als Anlagen dem Bericht beigefügt werden)

III. Übersicht der wichtigsten im Rahmen der Konsultation festgestellten Risiken

F. Identifikation und Umgang mit festgestellten Risiken

I. Detaillierte Identifikation von Risiken

II. Auswirkung und Eintrittswahrscheinlichkeit eines jeden identifizierten Risikos

III. Risikomanagement: Getroffene Entscheidungen für jedes Risiko, Kontrollziele und Kontrollmaßnahmen sowie vorgeschlagene Maßnahmen

G. Analyse der Rechtmäßigkeit der Verarbeitung

I. Allgemeine Zusammenfassung der Rechtmäßigkeit

II. Festgestellte Defizite und Lösungsvorschläge

H. Schlussfolgerungen

I. Schlussbewertung

II. Empfehlungen der Verantwortlichen für die Datenschutz-Folgenabschätzung

III. Zu realisierende technische Maßnahmen im Rahmen des Projektdesigns, um Risiken für die Rechte und Interessen der Betroffenen zu eliminieren, zu verhindern, zu verringern, zu übertragen oder zu akzeptieren

IV. Zu realisierende organisatorische Maßnahmen im Rahmen des Projektdesigns, um Risiken für die Rechte und Interessen der Betroffenen zu eliminieren, zu verhindern, zu verringern, zu übertragen oder zu akzeptieren

I. Anhang: Einführung und allgemeine Beschreibung des Bewertungsprozesses

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises International erstellt.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (Februar 2018)