Band 2 unserer GRC Reihe

„Fit für die EU Datenschutzgrundverordnung“

Mathias Reinis

PRIVACY IMPACT ASSESSMENT

Datenschutz-Folgenabschätzung nach ISO/IEC 29134
und ihre Anwendung im Rahmen der EU-DSGVO

mit Schlagwortverzeichnis

2. Auflage 2018

Concept | Factory
Governance – Risk – Compliance

Inhaltsverzeichnis

- Vorwort
- Einleitung
  - Für wen ist dieses Buch gedacht?
  - Der Aufbau dieses Buches
- Kapitel 1 - Das Umfeld zur Norm
  - 1.1 ISO/IEC Normenreihe zum Datenschutz
  - 1.2 Die Datenschutz-Folgenabschätzung in der Datenschutzgrundverordnung
  - 1.3 Position der Aufsichtsbehörden
  - 1.4 Datenschutz als Schutz der Privatsphäre
- Kapitel 2 - Die Richtlinie ISO/IEC 29134 im Überblick
  - 2.1 Aufbau der ISO/IEC 29134
  - 2.2 Zielgruppen der Norm
  - 2.3 Einsatzfelder
  - 2.4 Beziehung zu Management-Systemen
- Kapitel 3 - Kernkonzepte der ISO/IEC 29134
  - 3.1 Geschäftsprozess als Ausgangspunkt
  - 3.2 Verantwortung
  - 3.3 Gestaltungsfreiheit und Offenheit
  - 3.4 Informationsqualität
  - 3.5 Lebenszyklus-Betrachtung
  - 3.6 Partizipation Betroffener und interessierter Kreise

3.7 Prozess und Dokumentation
3.8 Bewertung und Behandlung
3.9 Publikation und Aktualität
Kapitel 4 – Die Datenschutz-Folgenabschätzung als Prozess
4.1 Gruppen und Rollen im Prozess
4.2 Der Ablauf in Phasen
Phase 1 – Wesentlichkeitsprüfung
Phase 2 – Aufsetzen einer Datenschutz-Folgenabschätzung
Phase 3 – Informationserhebung
Phase 4 – Einbindung von Anspruchsgruppen
Phase 5 – Ermitteln und bewerten der Risiken
Phase 6 – Festlegung der Risikobehandlung
Phase 7 – Dokumentieren und veröffentlichen
Phase 8 – Überprüfung und Anpassung an Änderungen
Kapitel 5 - Governance der Datenschutz-Folgenabschätzung
Kapitel 6 – Eingangsinformationen
6.1 Systemanforderungen
6.2 Systementwurf.
6.3 Betriebliche Pläne und Verfahren
Kapitel 7 – Risiko-Ermittlung
7.1 Erkennen der Risiken
7.2 Untersuchen der Risiken
7.3 Teilaufgabe Risikoschätzung
Kapitel 8 –Risikobewertung

Kapitel 9 – Behandlung der Risiken
9.1 Wahl der Behandlungsoption
9.1.1 Risikominderung
9.1.2 Risikobehandlung
9.1.3 Risikovermeidung
9.1.4 Risikoübertragung
9.2 Festlegen der Einzelmaßnahmen
9.3 Aufstellen des Behandlungsplans
9.4 Ausführen des Risikobehandlungsplans
Kapitel 10 – Berichtslegung
Anlage: Wichtige Grundsätze zum Datenschutz
A.1 ISO/IEC 29100 Privacy Principles
Einwilligung und Wahlfreiheit
Zweck, Legitimität und Bestimmung
Beschränkung der Erhebung
Datensparsamkeit
Verwendung, Speicherung und Beschränkung der Offenlegung
Genauigkeit und Qualität
Offenheit, Transparenz und Benachrichtigung
Individuelle Mitwirkung und Zugang
Verantwortlichkeit
Informationssicherheit
Datenschutz-Compliance
A.2 Grundsätze in der EU-DSGVO
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Zweckbindung
Datenminimierung
Richtigkeit
Speicherbegrenzung
Integrität und Vertraulichkeit
Rechenschaftspflicht
A.3 Grundsätze im BDSG neu (2018)
Literaturverzeichnis
Stichwortverzeichnis

Abbildungsverzeichnis

Abbildung 1: Arbeitsprogramm ISO/IEC JTC1 SC27 WG5

Abbildung 2: Inhaltlicher Aufbau der ISO/IEC 29134 Richtlinie für Datenschutz-Folgenabschätzungen

Abbildung 3: Die Kernkonzepte der ISO/IEC 29134

Abbildung 4: Übersicht der Prozessphasen

Abbildung 5: Muster einer Risiko-Landkarte

Abbildung 6: Vom erkannten Risiko zum umgesetzten Behandlungsplan

Vorwort

Als das ISO/IEC Subkomitee SC27 in seiner Arbeitsgruppe 5 im Herbst 2012 mit der Arbeit am Dokument „29134 Privacy impact assessment - Methodology“ begann, hatte das Europaparlament dem Entwurf für eine Neuregelung des Datenschutzes in Form einer unmittelbar in allen Mitgliedsländern geltenden Grundverordnung zugestimmt.

Obwohl es bis zu deren Verabschiedung noch fast vier Jahre dauern sollte, war bereits erkennbar, dass die bisher auf Einhaltung von formalen Einzelsachverhalten abstellende Gesetzgebung sich zu einer umfassenderen Verantwortung der verarbeitenden Stellen für die mit der Verarbeitung entstehenden Risiken und Folgen für den Betroffenen wandeln wird.

Zu Beginn konnte die Arbeitsgruppe vor allem auf Anleitungen aus dem kanadischen und anglikanischen Raum zurückgreifen. Neben bewährten und erprobten Grundstrukturen wurden aber auch Unzulänglichkeiten erkannt, denen mit der neuen Norm abgeholfen werden sollte.

Insgesamt fand die laufende Arbeit das Interesse von mehr als 50 im Projekt vertretenen Ländern und Liaison-Organisationen, zu denen unter anderem die Europäische Artikel 29 Gruppe, ISACA und ISC^2 gehörten. Die Norm wurde Ende Juni 2017 als **„ISO/IEC 29134:2017 Information technology – Security techniques –**

Guidelines for privacy impact assessment“ veröffentlicht.

Das vorliegende Buch versteht sich als Kommentar und Anleitung für den Einsatz dieser Norm im Rahmen der ab dem 25.Mai 2018 in Kraft tretenden Europäischen Datenschutzgrundverordnung EU-DSGVO. Die Norm wird erläutert, auszugsweise zitiert und kommentiert. Eine Wiedergabe des vollständigen Wortlautes kann aus urheberrechtlichen Gründen hier nicht erfolgen. Den englischen Originaltext können Sie direkt bei der ISO oder beim deutschen Beuth-Verlag beziehen.

Im September 2017

Mathias Reinis

Einleitung

Herzlich Willkommen! Mit diesem Buch halten Sie eine Anleitung in der Hand, die Ihnen beim Aufbau eines Risikomanagements zum Datenschutz - und konkret bei der Durchführung einer Datenschutz-Folgenabschätzung - helfen möchte. Das erste Kapitel führt Sie zunächst in die Normenwelt zum Datenschutz bei ISO/IEC ein und erläutert die Rolle der Datenschutz-Folgenabschätzung in der Europäischen Datenschutz-Grundverordnung EU-DSGVO.

In den weiteren Kapiteln setzt sich das Buch mit der Richtlinie „ISO/IEC 29134 Guidelines for Privacy Impact Assessment“ auseinander. Obwohl die Richtlinie bislang nur in Englisch veröffentlicht wurde, sind alle Ausführungen in Deutsch abgefasst.

Das zweite Kapitel geht auf den formellen Aufbau der Richtlinie ein, erläutert ihre Zielgruppen, ihr Einsatzfeld und ihre Beziehung zu Management-Systemen.

Im dritten Kapitel werden die zentralen Konzepte für eine Datenschutz-Folgenabschätzung nach der Richtlinie erläutert. Hierbei werden Voraussetzungen und Erwartungen beschrieben, die diese Folgenabschätzung von einer Checklistenprüfung unterscheiden und den neuen Ansatz für einen risikobasierenden Datenschutz darstellen.

Der phasenweise Ablauf einer Datenschutz-Folgenabschätzung und die zu involvierenden Rollen sind Gegenstand des vierten Kapitels. Unter der Überschrift

Governance geht das fünfte Kapitel auf die Rahmenbedingungen ein, die ein Unternehmen für die wiederholte Durchführung von Datenschutz-Folgenabschätzungen schaffen soll.

Kapitel sechs erläutert die Eingangsinformationen, die für eine Datenschutz-Folgenabschätzung bereitgestellt werden sollten.

Kapitel sieben beschreibt die Ermittlung von Risiken, zu deren Bewertung dann das Kapitels acht Anleitung gibt. Im Kapitel neun geht es um die Behandlung der erkannten und bewerteten Risiken.

Im zehnten Kapitel geht es um den Inhalt der Dokumentation einer Datenschutz-Folgenabschätzung und deren auszugsweise oder zusammenfassende Veröffentlichung.

Für wen ist dieses Buch gedacht?

Das Buch ist genau das richtige für Sie, wenn Sie bereits mit dem Datenschutz im Kern vertraut sind und sich jetzt über die neuen Herausforderungen aus der EU-DSGVO auseinander setzen möchten.

Insbesondere richtet es sich an das obere und mittlere Management von öffentlichen Einrichtungen und Unternehmen, die auf Grundlage ihrer Verarbeitungsvorgänge ein Risikomanagement für den Datenschutz einrichten wollen oder müssen, sowie an Aufgabenträger, die in der öffentlichen Einrichtung oder dem Unternehmen für die fachliche Anwendung, den IT-Betrieb, die Informationssicherheit oder den Datenschutz zuständig sind.

Ferner kann es dem interessierten Verbraucher darstellen, auf welcher Grundlage sein Geschäftspartner die Risiken für die ihm überlassenen personenbezogenen Daten ermitteln und bewerten sollte.

In der Forschung und Entwicklung Tätigen kann es einen Weg eröffnen, die Diskussion um eine ethische Verantwortbarkeit ihrer Ergebnisse im Hinblick auf personenbezogenen Daten mit der Datenschutz-Folgenabschätzung zu untermauern.

Der Aufbau dieses Buches

Erwartungen der EU-DSGVO oder der aufsichtführenden Stellen zum Thema des Kapitels werden jeweils in einem Kasten aufgeführt. Beispiel:

> Was die EU-DSGVO sagt:
>
> *Hat eine Form der Verarbeitung [...] 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.*

Zitate werden in diesem Buch jeweils mit der folgenden Schrift und kursiv verwendet.

Beispiel für ein Zitat

Sofern englische Textpassagen auf Deutsch zitiert werden, geht deren Übersetzung auf den Verfasser dieses Buches

zurück.

Die nachfolgenden Abkürzungen werden in diesem Buch verwendet:

BDSG	Bundesdatenschutzgesetz
EU-DSGVO	Europäische Datenschutz-Grundverordnung
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

Zum Ende vieler Abschnitte, ob Kapitel oder Unterkapitel, wird in einem grauen Kasten auf die Stellen in Normen oder anderen Quellen verwiesen, die den gemachten Ausführungen zu Grunde liegen.

Beispiel:

ISO/IEC 29134: Kapitel 6.2 und 6.3

Wird auf Abschnitte innerhalb dieses Buches verwiesen, so wird der Verweis mit einem Pfeil eingeleitet und in Fettschrift hervorgehoben.

Beispiel:

- **Kapitel 7.3**

Kapitel 1 – Das Umfeld zur Norm

1.1 ISO/IEC Normenreihe zum Datenschutz

Die Arbeiten zur Standardisierung im Datenschutz werden von der Internationale elektrotechnischen Kommission IEC und der Internationalen Standardisierungsorganisation ISO im gemeinsamen technischen Komitee JTC1, und dort in der Arbeitsgruppe 5 WG5 des Unterkomitees 27 SC27, durchgeführt.

Abbildung 1 auf der Folgeseite zeigt einen Überblick über die Stand September 2017 bei der Arbeitsgruppe 5 in Erarbeitung befindlichen und die bereits veröffentlichten ISO/IEC Normen zum Datenschutz. Die Darstellung gliedert sich in sechs Abschnitte, in denen die Arbeitsdokumente jeweils eingeordnet sind. Die erste Gruppe heißt Anwendungsgebiete (Application areas) und enthält zwei Vorstudien (Study periods SP), eine mit Blick auf die Anbieter von Smartphone Apps und die andere zu Intelligenten Wohnstädten (Smart cities).

Als grundsätzliches Rahmenwerk sind das bereits 2011 veröffentlichte Dokument ISO/IEC 29100 Privacy Framework und das fortgeschriebene „stehende“ Dokument SD2 Privacy references list anzuführen. Insbesondere das Privacy Framework wird für die Datenschutz-Folgenabschätzung noch eine besondere Rolle spielen.

Der dritte Abschnitt stellt die Management-Verfahren zum Datenschutz dar. Hier findet sich die Richtlinie 29134 zur Datenschutz-Folgenabschätzung, das in Erarbeitung befindliche Dokument 27552 zur Erweiterung des Informationssicherheits-Managementsystems ISO/IEC 27001 zu einem Datenschutz-Management und zwei Anwendungsregeln zum Datenschutz, die eine für Verantwortliche (29151) und die zweite für Auftragsverarbeiter in der Cloud (27018). Die Anwendungsregeln zur Informationssicherheit (27002) werden von der Schwester-Arbeitsgruppe 1 WG1 verantwortet und sind als Maßnahmen der Datensicherheit auch für den Datenschutz informativ aufgeführt.

Der vierte Abschnitt enthält Anleitungen zur Implementierung des Datenschutzes. Das Reifegradmodell für den Datenschutz (29190) ist bereits veröffentlicht, die Anleitung zu Kenntnis und Einwilligung (29184) und der Bericht zu einem ingenieurmäßigen Datenschutz (27550) sind noch im entstehen.

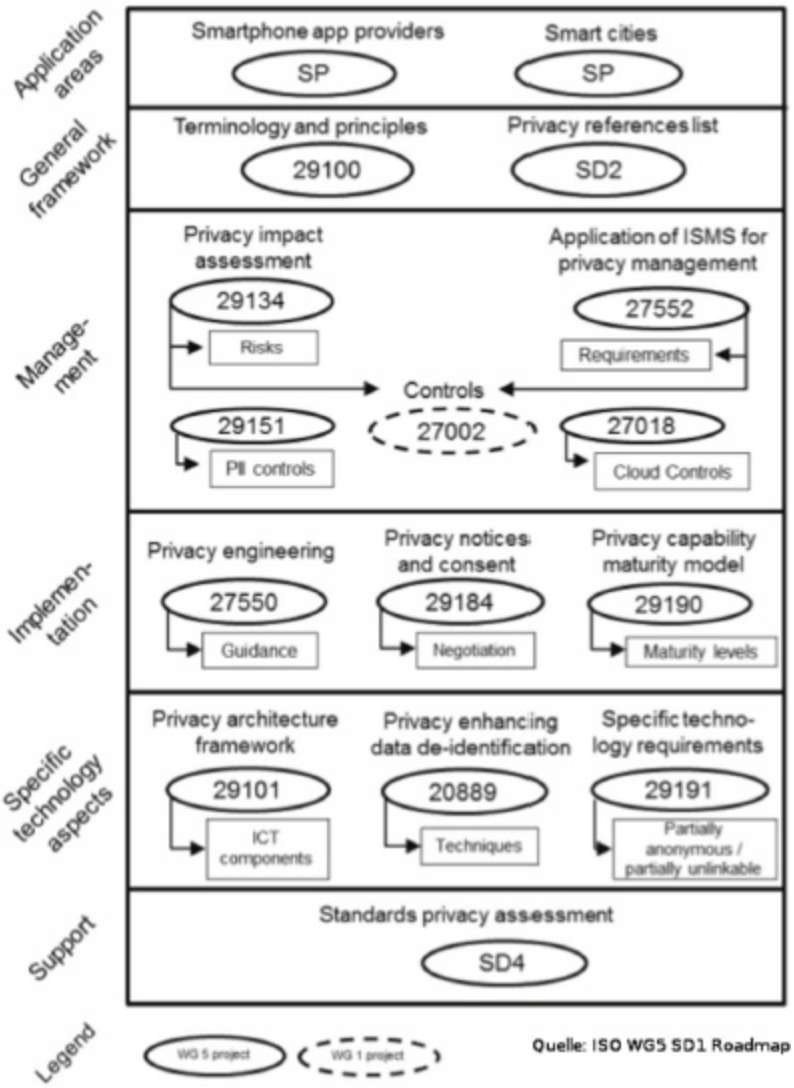

Abbildung 1: Arbeitsprogramm ISO/IEC JTC1 SC27 WG5

Mit spezifischen technologischen Aspekten setzen sich die Dokumente des fünften Abschnittes auseinander. Eine ausführliche Architekturempfehlung enthält die Norm 29101. Ein streckenweise anonymisiertes Anmeldeverfahren wird in der Norm 29191 beschrieben. Das entstehende Dokument 20889 beschäftigt sich mit Techniken zum entziehen des Personenbezugs aus Daten.

Der sechste Abschnitt ist zur Unterstützung anderer Normungsgremien gedacht. Das hier enthaltene, stehende Dokument SD4 gibt Hinweise zur Behandlung von

personenbezogenen Daten in den Verfahren und Technologien der entstehenden Normen.

Das Unterkomitee 27 der gemeinsamen Arbeitsgruppe JTC1 von ISO/IEC trifft sich in halbjährlichen Zyklen mit seinen Arbeitsgruppen. Die Dauer von der Annahme eines neuen Vorhabens bis zur Veröffentlichung des Ergebnisses beträgt erfahrungsgemäß zwischen vier und fünf Jahren.

1.2 Die Datenschutz-Folgenabschätzung in der Datenschutzgrundverordnung

Folgt man der Begründung des Parlaments und Rates der Europäischen Union im Erwägungsgrund 89, geht dem risikobasierenden Ansatz und der Datenschutz-Folgenabschätzung die Erkenntnis voraus, dass die mit der vorherigen Datenschutzrichtlinie 95/46/EG erwartete grundsätzliche Meldepflicht sich als bürokratisch und ineffizient erwiesen hat.

Ein wirksameres Verfahren verspricht man sich darin, sich *vorrangig mit denjenigen Arten von Verarbeitungsvorgängen [zu] befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen.*

Durch EU-DSGVO verwendet dabei die Einzahl „Risiko“ und definiert damit implizit ein Gesamtrisiko, statt differenziert auf einzelne Risikoursachen einzugehen. Dieses Risiko sollte der Verantwortliche im Erwägungsgrund 90 vor der Verarbeitung mittels Datenschutz-Folgenabschätzung bewerten, indem er „unter Berücksichtigung der Art, des

Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos“ dessen spezifische Eintrittswahrscheinlichkeit und Schwere bestimmt.

Mit der Erwartung, *diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll,* verlässt die EU-DSGVO das klassische Verständnis einer Folgenabschätzung. Statt mittels wissenschaftlicher Analyse zu einer feststellenden Bewertung zu kommen, rückt die praktische Abhilfe gegen das Risiko, die operative Verpflichtung zu dieser Abhilfe und der Nachweis der Compliance zur EU-DSGVO selbst mit in das Aufgabenfeld der Datenschutz-Folgenabschätzung hinein.

Da dem Einsatz der Datenschutz-Folgenabschätzung bereits die Erwartung eines hohen Risikos voraus gestellt wurde, bleibt der Erwägungsgrund 91 mit vielen dehnbaren und unkonkreten Formulierungen die Antwort dafür schuldig, wann dieses hohe Risiko vorauszusetzen ist. Statt dessen werden die Dimensionen

- Menge der personenbezogenen Daten,
- geografische Reichweite,
- Zahl möglicherweise betroffener Personen,
- Sensibilität,
- Innovation und
- Auswirkung für Rechte und Freiheiten der Person

bemüht, ohne genaue Anhaltspunkte für eine jeweiligen Schwellwert zu nennen.

Für die konkrete Situation von

- Entscheidungen aus automatisierten Profilingverfahren, die
- Verarbeitung von den in der Verordnung definierten besonderen Kategorien personenbezogener Daten,
- Daten über Straf- und Sicherungsmaßnahmen und
- für die öffentliche Überwachung mit „optoelektronischen Vorrichtungen“ (Videotechnik)

soll die Datenschutz-Folgenabschätzung verbindlich vorgeschrieben sein. Ein weiteres Kriterium soll die Auffassung der zuständigen Aufsichtsbehörde sein.

Ausgenommen von der verpflichtenden Datenschutz-Folgenabschätzung soll jedoch die Verarbeitung von Patientendaten und anwaltlichen Mandanten in kleinen Praxen und Kanzleien sein.

Die Datenschutz-Folgenabschätzung nach der EU-DSGVO muss keine individuelle und fokussierte Aufgabe für eine einzelne Verarbeitung sein. Laut Erwägungsgrund 92 ist auch die gemeinsame Durchführung durch mehrere Verantwortliche bis hin zu einer Datenschutz-Folgenabschätzung für alle gleichartigen Verarbeitungen in einem Marktsegment denkbar.

Wenn mit den aus der Datenschutz-Folgenabschätzung abgeleiteten und wirtschaftlich vertretbaren technischen Maßnahmen das Gesamtrisiko nicht auf ein annehmbares Niveau herab gemildert werden kann, erwartet die EU-

DSGVO (in Erwägungsgrund 94), dass der Verantwortliche vor Aufnahme der Verarbeitung die zuständige Aufsichtsbehörde konsultiert.

Die konkreten Vorgaben der EU-DSGVO an eine Datenschutz-Folgenabschätzung finden sich in Artikel 35 und 36 der Verordnung und lauten wie folgt:

Artikel 35

Datenschutz-Folgenabschätzung

1. *Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.*

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

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 einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber*