Entwicklung einer Methode für die Datenschutz-Folgenabschätzung: Erläuterung und Auslegung der Anforderungen der DSGVO

d.pia.lab Strategiepapier Nr. 1/2019

Dariusz KLOZA, Niels VAN DIJK, Simone CASIRAGHI, Sergi VAZQUEZ MAYMIR,
Sara RODA, Alessia TANAS und Ioulia KONSTANTINOU
Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)

Dieses Strategiepapier legt die Grundlage für die Entwicklung einer Methode für die Datenschutz-Folgenabschätzung (DSFA) in der Europäischen Union (EU). Zunächst wird als Grundvoraussetzung eine generische Methode für die Folgenabschätzung entwickelt, die zugeschnitten auf den jeweiligen Kontext in zahlreichen Gebieten der Praxis wie Umwelt, Technologieentwicklung oder Regulierung (Abschnitt 2) verwendet werden könnte. Aufbauend auf dieser generischen Methode und in Auslegung der Anforderungen der Datenschutzgrundverordnung (DSGVO) legt dieses Strategiepapier die Grundlage für eine spezifische Methode für das Verfahren der DSFA in der EU, die ebenfalls an den jeweiligen Verwendungszweck anzupassen ist (Abschnitt 3). In diesem Strategiepapier sollen insbesondere zwei entscheidende Aspekte der spezifischen Methode, die sich bisher als am umstrittensten erwiesen haben, geklärt werden: Die Bewertungstechniken (insbesondere Notwendigkeits- und Verhältnismäßigkeitsprüfung und Risikoabschätzung) und die Einbeziehung von Interessenträgern (einschließlich Öffentlichkeitsbeteiligung) in den Entscheidungsfindungsprozess. In Abschnitt 4 werden die Ergebnisse zusammengefasst und es wird zu weiterführenden Vorgaben, Klarstellungen und Anpassungen aufgerufen. Dieses Strategiepapier richtet sich in erster Linie an politische Entscheidungsträger, die Methoden für die Folgenabschätzung entwickeln, Praktiker, die diese Methoden an den jeweiligen spezifischen Kontext ihrer Verwendung anpassen, und Experten, die auf Grundlage dieser Methoden Bewertungen vornehmen.

1 EINLEITUNG

1.1 KONTEXT

Die Datenschutzgrundverordnung (DSGVO) ist das Kerninstrument der überarbeiteten Datenschutzregelung der Europäischen Union (EU). Die Verordnung stellt eine Reihe neuer Lösungen in den Vordergrund, deren Ziel es unter anderem ist, immer dann ein „gleichmäßiges und hohes Datenschutzniveau für natürliche Personen“ (Erwägungsgrund 10) sicherzustellen, wenn ihre personenbezogenen Daten verarbeitet werden. Zu diesen Lösungen gehört auch die Verpflichtung des für die Datenverarbeitung Verantwortlichen, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, bevor personenbezogene Daten verarbeitet werden. Die DSFA ist immer dann erforderlich, wenn die beabsichtigte Datenverarbeitung „ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ (Artikel 35 Abs. 1) beinhalten kann, und wird durchgeführt, um den „Schutz personenbezogener Daten [sicherzustellen] und [den] Nachweis dafür [zu erbringen], dass diese Verordnung eingehalten wird“ (Artikel 35 Abs. 7 Buchstabe d)).

Die DSFA ist eine Unterform der Folgenabschätzung (FA) und im weiteren Sinne eine Variante des Privacy Impact Assessments (PIA). Allgemein gesprochen ist Folgenabschätzung eine Bewertungstechnik zur Analyse der möglichen Konsequenzen einer Initiative für ein bestimmtes gesellschaftliches Anliegen oder gesellschaftliche Anliegen (d.h. eine Angelegenheit oder Angelegenheiten, die von Interesse oder Bedeutung ist/sind), um, sollte die Initiative diese Anliegen gefährden, eine informierte Entscheidung zu treffen, ob und unter welchen Umständen die Initiative durchgeführt wird; die Folgenabschätzung stellt mithin in erster Linie ein Mittel dar, um diese Anliegen zu schützen.

Die Verpflichtung, eine DSFA durchzuführen, spiegelt den risikobasierten Ansatz zum Schutz personenbezogener Daten im reformierten EU-Rechtsrahmen sowie die Stärkung des in ihm enthaltenen Grundsatzes der Rechenschaftspflicht (Artikel 5 Abs. 2) wieder. Angesichts der Erfahrungen mit Bewertungstechniken in anderen Bereichen der Praxis (z.B. Folgenabschätzung in den Bereichen Umwelt, Technologie oder Regulierung) ist davon auszugehen, dass die DSFA ein wirksames Werkzeug für die Einhaltung und Durchsetzung des Datenschutzes/Datenschutzrechts werden wird.

Zugleich wird das Verfahren der DSFA schrittweise auch in anderen Instrumenten des EU-Rechtsrahmens für den Schutz personenbezogener Daten angeordnet. Neben der DSGVO ist die verbindliche Durchführung des Verfahrens der DSFA bisher auch in der Richtlinie 2016/680 über den Schutz personenbezogener Daten in Strafsachen (Artikel 27), der Verordnung 2018/1725 über den Schutz personenbezogener Daten bei der Verarbeitung durch die Organe, Einrichtungen und sonstigen Stellen der Union (Artikel 39 und 89) und in der Richtlinie 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Erwägungsgrund 53) verankert. Der Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation) würde, sollte sie mit dem aktuellen Wortlaut verabschiedet werden, ebenfalls in bestimmten Situationen eine DSFA erforderlich machen (Artikel 6). (Zuvor hatte die EU PIA und DSFA auf freiwilliger Basis im Bereich der Funkfrequenzkennzeichnung (RFID) und der intelligenten Energienetze getestet.) Parallel hat der Europarat in seinem modernisierten „Übereinkommen Nr. 108“ ein gesetzliches Mandat für eine vergleichbare Verpflichtung (Artikel 10 Abs. 2) vorgesehen. Außerhalb von Europa werden verschiedene Formen des PIA und der DSFA u.a. in Australien, Japan,

 | ISSN 2565-9936

Kanada, Neuseeland, Südafrika, Südkorea und den USA praktiziert. Zugleich verlangen internationale Organisationen wie das Internationale Komitee des Roten Kreuzes ein solches Bewertungsverfahren in ihrer Satzung.

Diese rechtlich verbindlichen Verpflichtungen, das Verfahren der DSFA in der EU durchzuführen, werfen eine Reihe von Fragen auf, die sich z.B. durch neue Kernkonzepte, auf denen die DSFA beruht (z.B. Risiko für ein Recht), die gelegentliche Schwammigkeit der in den Rechtsinstrumenten verwendeten Terminologie (z.B. „umfangreich“ oder „systematisch“) und relativ hohe Geldbußen im Falle der Nichtbefolgung oder Fehlanwendung ergeben. Auch erlaubt die Tatsache, dass nur die wichtigsten Punkte der DSFA geregelt wurden, ein hohes Maß an Flexibilität, die allerdings auf Kosten der Rechtssicherheit geht und daher Leitlinien zur Auslegung und normative Vorgaben erfordert. (Die Europäische Kommission bezeichnete diesen Ansatz während der Einbringung des Vorschlags für die Reform des Rechtsrahmens für den Schutz personenbezogener Daten als „gesetzlichen Anker“ („legal hook“) und erläuterte, dass der Gesetzgeber nur die Mindestanforderungen auszuführen habe. Detailliertere Angaben müssten, falls erforderlich, z.B. seitens der betreffenden Industriebranchen oder Regierungen erfolgen. Nur wenn diese fehlschlügen oder unzureichend seien, solle der Gesetzgeber eingreifen.) 2017 erließ die damalige Artikel-29-Datenschutzgruppe übergeordnete Leitlinien zur DSFA in der EU und zur Bestimmung, ob ein Datenverarbeitungsvorgang „wahrscheinlich ein hohes Risiko“ mit sich bringt. Die Leitlinien erläuterten einige Punkte hinsichtlich sowohl des Rahmens als auch der Methode (z.B. Schwellwertanalyse) der Folgenabschätzung, behandelten aber andere Aspekte nur oberflächlich (z.B. die Notwendigkeits- und Verhältnismäßigkeitsprüfung oder die Einbeziehung von Interessenträgern). Auch von akademischer und beruflicher Seite wurde hier bisher nicht mehr Klarheit geschaffen. Einer der Aspekte betrifft die Methode, d.h. die Gesamtheit der für die Durchführung der Folgenabschätzung erforderlichen Schritte. Das vorliegende Strategiepapier ist diesem Aspekt gewidmet.

1.2 HINTERGRUND

Die Folgenabschätzung setzt sich typischerweise aus zwei Hauptelementen zusammen, dem „Rahmen“ und der „Methode“. Ein *Rahmen* ist etwas, „was einer Sache ein bestimmtes [äußeres] Gepräge gibt“ oder Ordnungselement für etwas, das in diesem Zusammenhang als Strategie der Folgenabschätzung zu bezeichnen ist und die Voraussetzungen und Grundsätze dieser definiert und beschreibt. Eine *Methode*, also ein „auf einem Regelsystem aufbauendes Verfahren zur Erlangung von [wissenschaftlichen] Erkenntnissen oder praktischen Ergebnissen“, betrifft die Praxis der Folgenabschätzung und definiert die einander nachfolgenden oder sich wiederholenden Schritte, die durchlaufen werden, um ein solches Verfahren durchzuführen. Eine Methode entspricht jeweils einem Rahmen und kann als praktische Umsetzung des Rahmens betrachtet werden. Dieser Aufbau („Architektur“) wird häufig durch *Leitlinien* (Handbücher, Anleitungen) und *Muster* ergänzt, die den Bewertungsvorgang näher erläutern und helfen, den gesamten Prozess zu strukturieren und eine abschließende Aussage (in Form eines *Berichts*) zu treffen, um ihn zu dokumentieren.

Es gibt bereits zahlreiche Rahmen und Methoden für die Durchführung von Folgenabschätzungen in vielen Bereichen der Praxis für unterschiedliche Anwendungsfälle und in unterschiedlicher Qualität. Der stetige Bedarf für neue Rahmen und Methoden ergibt sich durch den Grundsatz der Rezeptivität der Folgenabschätzung, d.h. sowohl der Rahmen als auch die Methode müssen ständig verbessert werden, wenn Folgenabschätzung (durch Lernen aus den eigenen Erfahrungen oder aus den Erfahrungen anderer Bewertungstechniken) ihrem Ziel besser gerecht werden, gezielter auf gesellschaftliche Veränderungen reagieren sowie neue Betätigungsfelder der Praxis für die Folgenabschätzung erschließen soll (wie z.B. eine kürzlich vorgeschlagene „algorithmische Folgenabschätzung“).

1.3 STRUKTUR

In diesem Strategiepapier legt das d.pia.lab die Grundlage für eine spezifische Methode für die Durchführung von DSFA in der EU. Als Voraussetzung dafür schlägt es eine generische Methode der Folgenabschätzung vor, die – zugeschnitten auf den spezifischen Kontext (z.B. Industrie- oder Governance-Sektor) – in zahlreichen Bereichen der Praxis wie Umwelt, Technologie oder Regulierung verwendet werden könnte (Abschnitt 2).

Die generische Methode ist ein aus 16 Grundsätzen bestehender Rahmen für die Folgenabschätzung in zahlreichen Bereichen der Praxis, die im vorherigen Strategiepapier des d.pia.lab (2017) entwickelt wurde. Die zweite (spezifische) Methode ist speziell auf den Bereich des Datenschutzes zugeschnitten und betrifft konkret das Verfahren der DSFA in der EU. Sie wird ausgehend von den Vorschriften der DSGVO von der generischen Methode abgeleitet (Abschnitt 3). Auch diese Methode muss an den jeweiligen Kontext ihrer Verwendung angepasst werden. Bei der Entwicklung der letztgenannten Methode hat sich das d.pia.lab auf besonders umstrittene Themen wie die Einbeziehung von Interessenträgern (einschließl. Öffentlichkeitsbeteiligung) in den Entscheidungsfindungsprozess oder in der Debatte vernachlässigte Themen, die sich bisher in der Praxis als schwierig erwiesen haben, wie die Notwendigkeits- und Verhältnismäßigkeitsprüfung und die Bewertung des Risikos für die Rechte und Freiheiten natürlicher Personen, konzentriert. Diese beiden Methoden stützen sich auf die kritische Bewertung und vergleichende Analyse der existierenden Rahmen und Methoden für die Folgenabschätzung und die damit in verschiedensten Bereichen der Praxis gewonnenen Erfahrungen, v.a. betreffend den Schutz der Privatsphäre, den Schutz personenbezogener Daten (informationelle Selbstbestimmung), Technologieentwicklung, Umwelt, Regulierung und Menschenrechte.

Dieses Strategiepapier richtet sich an zwei Hauptempfängergruppen. Da Methoden für die Folgenabschätzung an den Kontext ihrer Verwendung angepasst werden müssen, sind die Hauptempfänger politische Entscheidungsträger, insbesondere Datenschutzbehörden (DSB) auf EU-Ebene und in den Mitgliedstaaten, die Methoden für DSFA entwickeln müssen, die auf ihren innerstaatlichen Kontext zugeschnitten sind. Dieses Strategiepapier richtet sich außerdem an Interessenträger, die die Methoden zur DSFA an einen bestimmten Verwendungskontext anpassen, und letztlich auch an die Verantwortlichen, die den Bewertungsprozess durchführen. Zugleich soll die generische Methode für die Folgenabschätzung ebenso in zahlreichen Bereichen verwendet werden können, in denen Folgenabschätzungen durchgeführt werden.

2 EINE GENERISCHE METHODE FÜR DIE FOLGENABSCHÄTZUNG

Die vorgeschlagene generische Methode für die Folgenabschätzung wurde auf Grundlage einer vergleichenden und kritischen Analyse der wiederkehrenden Etappen von Bewertungsmethoden, die in zahlreichen Bereichen Verwendung finden, entwickelt und um die Erfahrungen des d.pia.labs ergänzt. Zugleich greift die generische Methode den aus 16 Grundsätzen bestehenden Rahmen auf, der im Strategiepapier des d.pia.lab aus 2017 vorgestellt wurde.

Die generische Methode legt die Grundlage für die spezifische Methode für die Folgenabschätzung in zahlreichen Bereichen der Praxis. Die generische Methode besteht aus zehn Etappen (sechs aufeinanderfolgenden Etappen, drei Etappen, die sich auf den gesamten Vorgang beziehen, und eine nachgelagerten Etappe), wobei jede sich in fünf Phasen unterteilt. Einige dieser Etappen folgen einer logischen Reihenfolge, wohingegen andere sich von den im Rahmen genannten Grundsätzen ableiten. Folgende Etappen sind vorgesehen:

Phase I: Vorbereitung des Bewertungsprozesses

1) *Screening (Schwellwertanalyse)*. Durch diese Etappe lässt sich ermitteln, ob für die geplante Initiative bzw. das Bündel ähnlicher Initiativen in einem gegebenen Kontext eine Folgenabschätzung gerechtfertigt oder erforderlich ist. Das Screening erfolgt aufgrund einer ersten, ausreichend ausführlichen und sowohl technischen als auch kontextbezogenen Beschreibung der betreffenden Initiative. Die Ermittlung erfolgt anhand von Schwellwertkriterien, die sich in interne (d.h. interne Politik der Organisation), externe (d.h. in gesetzlichen oder sonstigen rechtlichen Anforderungen enthaltene Kriterien) und *ad hoc*-Kriterien, wie z.B. durch die öffentliche Meinung entstandener Druck, unterteilen lassen. Sollte ein Bewertungsprozess weder gerechtfertigt noch erforderlich sein, wird der gesamte Vorgang mit der begründeten Feststellung abgeschlossen, dass mit keinen erheblichen Auswirkungen zu rechnen ist.

2) *Scoping*. Diese Etappe dient aufbauend auf der Erstbeschreibung zur Identifikation:

   a) eines gesellschaftlichen Anliegens oder gesellschaftlicher Anliegen, die von einer geplanten Initiative betroffen sein können, wie Schutz der Privatsphäre, Schutz personenbezogener Daten, (angewandte) Ethik oder die natürliche und menschliche (biophysikalische) Umgebung und die zugehörigen gesetzlichen oder sonstigen rechtlichen Anforderungen; diese Anliegen sind ein Richtwert des Bewertungsverfahrens;

   b) der Interessenträger, die die beabsichtigte Initiative beeinflussen, von ihr beeinflusst oder betroffen oder an ihr interessiert sein oder von ihr Kenntnis haben könnten, sowie des Grads ihrer Beteiligung;

   c) der Techniken (Methoden im engeren Sinne) zur Folgenabschätzung und Beurteilung der Beteiligung von Interessenträgern, einschließlich Öffentlichkeitsbeteiligung, an Entscheidungsprozessen, die das gesamte Bewertungsverfahren hindurch verwendet werden;

   d) sonstiger Bewertungstechniken, die über das Verfahren der Folgenabschätzung hinausgehend notwendig oder gerechtfertigt sein können, um zum Beispiel die Vollständigkeit der im Entscheidungsprozess verwendeten Informationen zu gewährleisten (z.B. Technologiebewertung oder Umweltverträglichkeitsprüfung).

   Nicht alle Elemente oder Personen sind zwangsläufig zu Beginn des Bewertungsverfahrens identifizierbar, weshalb in regelmäßigen Abständen eine Neubestimmung erfolgen muss.

3) *Planung und Vorbereitung*. Diese Etappe definiert die für die Durchführung des Bewertungsprozesses zu verwendende Aufgabenbeschreibung. Hierzu zählen unter anderem:

   a) dessen Ziele;
   b) die Kriterien für die Zulässigkeit negativer Auswirkungen;
   c) die notwendigen Ressourcen (d.h. Zeit, Geld, Arbeitskraft, Wissen, Expertise, Räumlichkeiten und Infrastruktur);
   d) die Verfahren und Zeitrahmen des Bewertungsprozesses;
   e) der Bewerter oder das Bewertungsteam (intern oder extern), ihre Rollen und Verantwortlichkeiten sowie die Sicherstellung ihrer beruflichen Unabhängigkeit und
   f) die Kontinuität des Bewertungsprozesses.

Phase II: Bewertung

4) *Beschreibung*. Im Rahmen dieser Etappe erfolgt aufbauend auf der vorhergehenden Beschreibung (siehe Etappe 1) eine zweiteilige Darstellung der geplanten Initiative. Zunächst eine *kontextbasierte Beschreibung*, die sich typischerweise untergliedern lässt in

   a) einen Überblick über die geplante Initiative(n) und über die Trägerorganisation;
   b) den Kontext der Umsetzung der Initiative;
   c) die Notwendigkeit der Initiative;
   d) mögliche Interferenz(en) mit (dem) gesellschaftlichen Anliegen und
   e) die zu erwartenden Vor- und Nachteile.

   In einem zweiten Schritt folgt eine technische *Beschreibung*. Im Falle einer Umweltverträglichkeitsprüfung (UVP) berücksichtigt diese z.B. die betroffenen Komponenten der biophysikalischen Umgebung und im Falle der DSFA z.B. die verschiedenen Kategorien personenbezogener Daten und ihrer Ströme im Rahmen eines Verarbeitungsvorgangs.

5) *Beurteilung der Auswirkungen*. Im Rahmen dieser Etappe werden die Auswirkungen der geplanten Initiative anhand der vorher festgelegten Techniken beurteilt. Diese Auswirkungen beziehen sich auf die/das gesellschaftliche(n) Anliegen, die von der geplanten Initiative betroffen sein können, und auf die Interessenträger, die weitestgehend außerhalb der Trägerorganisation anzusiedeln sind. Typischerweise besteht diese Beurteilung mindestens aus einer detaillierten Ermittlung, Analyse und Bewertung der Auswirkungen. Die Beurteilungstechniken können von Risikoanalyse (qualitativer und quantitativer Risikoanalyse oder einer Kombination beider), Szenario-Analyse (Planung anhand von Szenarien) und Technikvorausschau bis hin zur Prüfung der Einhaltung geltender Rechtsvorschriften, von Techniken zur rechtlichen Auslegung, einer Bewertung der Verhältnismäßigkeit und Notwendigkeit, bis hin zu einer Kosten-Nutzen-Analyse und einer Analyse der Stärken, Schwächen, Chancen und Risiken (SWOT-Analyse) reichen.

Phase III: Empfehlungen

6) *Empfehlungen*. Im Rahmen dieser Etappe werden konkrete, detaillierte Maßnahmen (Kontrollen, Schutzmaßnahmen, Lösungen etc.), ihre Empfänger, Prioritäten und der Zeitrahmen, in dem sie umgesetzt werden sollen, vorgeschlagen, mit dem Ziel, die negativen Auswirkungen der geplanten Initiative zu minimisieren und, wenn möglich, positive Auswirkungen zu maximieren. Der Bewerter begründet die Einteilung in negative und positive Auswirkungen, da diese Unterscheidung kontextgebunden und somit subjektiv ist. Der Bewerter zieht Bilanz über die bereits umgesetzten Maßnahmen. Auf dieser Grundlage trifft die Führungsspitze der Trägerorganisation nach Abschluss der Bewertung eine Entscheidung dahingehend, ob und unter welchen Bedingungen die Initiative durchgeführt wird. (Die Trägerorganisation kann die Empfehlungen jedoch auch schrittweise im Laufe des Beurteilungsprozesses umsetzen). Von einer Initiative wird normalerweise komplett abgesehen, wenn die negativen Folgen inakzeptabel sind; eine solche Initiative würde nur im Ausnahmefall durchgeführt werden, was ausreichend zu begründen wäre.

Phase IV: Fortwährende Etappen

7) *Einbeziehung von Interessenträgern, einschließlich Öffentlichkeitsbeteiligung, in den Entscheidungsfindungsprozess.* Dies ist eine fortwährende, übergreifende Etappe, die den gesamten Prozess hindurch durchlaufen wird und in deren Rahmen Interessenträger, einschließlich der Öffentlichkeit und/oder ihrer Vertreter, am Bewertungsprozess beteiligt werden.

   Im weitesten Sinne ist ein Interessenträger („Stakeholder“) jemand, der ein Interesse an etwas hat, unabhängig davon, ob er sich seines Interesses bewusst ist oder das Interesse direkt zum Ausdruck gebracht wird. Im Zusammenhang mit Folgenabschätzung

handelt es sich um jemanden, der aktuell oder möglicherweise in der Zukunft die beabsichtigte Maßnahme (ggf.) positiv und/oder negativ beeinflusst, von ihr beeinflusst wird oder betroffen oder an ihr interessiert ist oder sein könnte. Zugleich kann ein Interessenträger jemand sein, der über besonderes Wissen und Expertise hinsichtlich der Initiative verfügt, d.h. ein Experte. Das Konzept der Interessenträger ist somit weit gefasst und umfasst die Öffentlichkeit (Laien etc.), Entscheidungsträger, Experten usw. Interessenträger können Einzelpersonen oder kollektive Einheiten sein, unabhängig davon, ob sie formell (gesetzlich) anerkannt sind oder nicht (z.B. gesellschaftliche Gruppen, Gemeinschaften, Nationen, die Öffentlichkeit im weiteren Sinne, Organisationen der Zivilgesellschaft etc.). Es gibt zahlreiche (Gruppen von) Interessenträgern, die in interne (z.B. Angestellte, Arbeitsausschuss) und externe (z.B. Kunden oder Nichtregierungsorganisationen), primäre (d.h. diejenigen, die ein direktes Interesse an der Initiative haben, wie Investoren) und sekundäre (d.h. diejenigen, die ein indirektes Interesse, aber großen Einfluss haben, wie z.B. der Staat) Interessenträger unterteilt oder nach ihren Eigenschaften (Macht, Legitimität und Dringlichkeit) unterschieden werden können.

Die Einbeziehung von Interessenträgern ist ein wesentlicher Bestandteil des Bewertungsprozesses und wird normalerweise nur in Ausnahmefällen unterlassen. Ist die Einbeziehung von Interessenträgern weder gerechtfertigt noch notwendig, ist diese Entscheidung zu begründen und zu dokumentieren. Ist die Einbeziehung von Interessenträgern verpflichtend, verfügt der berechtigte Interessenträger über Rechtsmittel, die dem Grad der Einbeziehung im betreffenden Bewertungsverfahren entsprechen, sollte die Einbeziehung verwehrt werden oder unzureichend sein. In jedem Fall verletzt die Einbeziehung von Interessenträgern keine Geheimhaltungspflichten (Staats- oder Geschäftsgeheimnisse) und bringt auch keine negativen Auswirkungen für die Teilnehmer mit sich (z.B. Ausbeutung).

Der Grad der Einbeziehung von Interessenträgern kann variieren zwischen: (a) reiner Information und Aufklärung über eine geplante Initiative (niedriger Grad); (b) Diskussionen und Befragungen, im Rahmen derer die Standpunkte der Interessenvertreter eingeholt und berücksichtigt werden (mittlerer Grad); (c) gemeinsame Entscheidung der Interessenvertreter und der Trägerorganisation über die Bereitstellung der betreffenden Initiative und schließlich partnerschaftliche Umsetzung der Initiative (hoher Grad).

Es gibt eine Vielzahl von Techniken für die Einbeziehung von Interessenträgern: Diese reichen von Informationsschreiben zu Interviews, von Fragebögen und Umfragen zu Fokusgruppen, Diskussionsrunden, Workshops und Bürgergutachten, einschließlich Strukturierungstechniken wie eines „World Café“ oder „Delphi“. Eine geeignete Technik oder Kombination verschiedener Techniken wird in Abhängigkeit des gewünschten Grads der Stakeholder-Beteiligung, der geplanten Initiative, des Kontexts der Umsetzung der Initiative und der Ressourcen der Trägerorganisation gewählt.

Die Einbeziehung von Interessenträgern kann verschiedene Vorteile für den Beurteilungsprozess (z.B. Erhöhung der Qualität, Glaubwürdigkeit und Legitimität) und das Ergebnis (z.B. besser informierte Entscheidungsprozesse) mit sich bringen, wobei diese gegen die Nachteile abzuwägen sind, wie z.B. die Frage der Repräsentativität (Über- oder Unterrepräsentanz), Fairness (z.B. Manipulation, „Astroturfing“), Zurückhaltung, Kommunikationsbarrieren, Konflikte zwischen öffentlichen und privaten Interessen sowie die Zurverfügungstellung beträchtlicher Ressourcen im Rahmen des gesamten Prozesses der Stakeholder-Beteiligung.

8) *Dokumentation*. Im Rahmen dieser fortlaufenden, übergreifenden Etappe werden den gesamten Prozess hindurch sämtliche während des Bewertungsprozesses unternommenen Vorgänge nachvollziehbar dokumentiert, indem sie in schriftlicher oder anderer dauerhafter Form erstellt und gespeichert werden. Dazu gehört auch die Erstellung eines Abschlussberichts über den Bewertungsprozess (bzw. ggf. die Feststellung, dass wesentliche Auswirkungen ausgeblieben sind). Sämtliche Dokumente zu einem bestimmten Bewertungsprozess, die vorzugsweise in elektronischer Form erstellt werden, können der Öffentlichkeit zugänglich gemacht, zentral registriert und/oder auf Anfrage (unter Wahrung des berechtigten Interesses der Vertraulichkeit) zur Einsicht vorgelegt werden.

9) *Qualitätskontrolle*. Im Rahmen dieser fortlaufenden, übergreifenden Etappe wird den gesamten Prozess hindurch die Einhaltung eines bestimmten Leistungsstandards entweder intern (z.B. durch Fortschrittskontrolle oder Überprüfung durch die Trägerorganisation) oder extern (z.B. durch eine unabhängige Regulierungsbehörde im Wege eines Audits oder durch ein zuständiges Gericht) oder auf beiden Ebenen geprüft. Die Qualitätskontrolle kann gleichermaßen während und/oder nach dem Bewertungsprozess stattfinden.

Phase V: Überprüfung

10) *Überprüfung*. Im Rahmen dieser Etappe wird entschieden, ob der gesamte Prozess oder ein Teil desselben erneut durchgeführt werden soll. Diese Etappe kann jedes Mal durchlaufen werden, wenn sich die geplante Initiative (vor oder nach ihrer Einführung) ändert oder wenn sich die Umstände ändern, in denen sie durchgeführt werden soll oder bereits durchgeführt wird. Diese Etappe gewährleistet zudem die Kontinuität des Bewertungsprozesses, z.B. für den Fall, dass die Initiative einer anderen Organisation übertragen wird.

Die obengenannte Methode zur Abschätzung der Folgen der Initiative für eine bzw. mehrere gesellschaftliche Anliegen ist allgemeiner Natur und muss auf die Besonderheiten und Bedürfnisse des betreffenden Praxisbereichs, der beteiligten Akteure (einschließlich der Öffentlichkeit) und des Anwendungskontextes zugeschnitten werden. So basiert die Folgenabschätzung im Bereich des Schutzes personenbezogener Daten in der EU auf einem spezifischen Ansatz, zumindest während des sog. *Screenings* (Schwellwertkriterien), des *Scopings* (z.B. Auflistung gesellschaftlicher Anliegen), der *Beurteilung der Auswirkungen* (z.B. Bewertungstechniken und Liste möglicher Folgen), der *Einbindung von Interessenträgern, einschließlich der Beteiligung der Öffentlichkeit, in die Entscheidungsfindung* (z.B. Interessengruppen und Methoden für ihre Einbeziehung) sowie der Etappe der *Empfehlungen*.

EINSCHLÄGIGE BESTIMMUNGEN DER DSGVO

Artikel 35

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. […]

7. Die Folgenabschätzung enthält zumindest Folgendes:

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

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

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen […]; und

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

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

Artikel 36

1. Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung […] hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

2. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung […] nicht im Einklang mit [der] Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter […] entsprechende schriftliche Empfehlungen und kann ihre […] Befugnisse ausüben.

3 Eine Methode zur Datenschutz-Folgenabschätzung in der Europäischen Union

Die nachfolgend beschriebene spezifische Methode, die nach der DSGVO für die Datenschutz-Folgenabschätzung (DSFA) in der EU erforderlich ist, wurde im Lichte der zahlreichen Bestimmungen von Artikel 35 und 36 und der generischen Methode ausgelegt. Die DSGVO verpflichtet den für die Datenverarbeitung Verantwortlichen, die Folgenabschätzung durchzuführen, und, falls erforderlich, den Auftragsverarbeiter, den für die Datenverarbeitung Verantwortlichen zu unterstützen. Der für die Datenverarbeitung Verantwortliche ist für den Bewertungsprozess zur Rechenschaft zu ziehen.

Die Verordnung sieht in diesem Zusammenhang sieben Etappen vor:

1) *Screening (Schwellwertanalyse)*: Um festzustellen, ob ein DSFA-Verfahren gesetzlich vorgeschrieben ist, müssen die geplanten Datenverarbeitungsvorgänge auf der Grundlage einer Erstbeschreibung dieser Vorgänge und einer rudimentären Risikobewertung anhand der folgenden sechs Kriterien geprüft werden:
   - *Kriterium 1 – Eintrittswahrscheinlichkeit eines hohen Risikos (allgemein)*: Ganz allgemein bestimmt die Verordnung, dass bei Datenverarbeitungen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, ein DSFA-Verfahren anhand vier qualitativer Kriterien durchzuführen ist – der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung personenbezogener Daten. Insbesondere Datenverarbeitungsvorgänge unter Einsatz neuer Technologien sind ein spezifischer Auslöser für den Bewertungsprozess (Artikel 35 Abs. 1). Diese Kriterien werden jedoch nicht näher definiert. Dazu könnten beispielsweise die Verarbeitung besonderer Kategorien personenbezogener Daten, Daten im Hinblick auf strafrechtliche Verurteilungen und Straftaten, Daten im Zusammenhang mit Sicherheitsmaßnahmen oder biometrische Daten (d.h. die Art der Verarbeitungsvorgänge), die Menge der verarbeiteten Daten, die geografische Reichweite und die Anzahl der betroffenen Personen (d.h. der Umfang), die Verwendung einer bestimmten Art von Technologie oder das Einsatzgebiet (z.B. öffentlich zugänglich) (d.h. die Umstände) oder Daten für die Erstellung von Profilen oder eine automatisierte Entscheidungsfindung (d.h. der Zweck) gehören (siehe Erwägungsgrund 91). Die damalige Artikel-29-Datenschutzgruppe empfahl in ihrer Stellungnahme zur Frage, ob die Verarbeitung „wahrscheinlich ein hohes Risiko mit sich bringt“ (2017), die Risikobewertung (Vorliegen eines hohen Risikos) anhand von neun Kriterien vorzunehmen; diese beinhalten etwa die Frage der Übereinstimmung oder der Kombinationsmöglichkeit der Datensätze oder ob die Datenverarbeitung schutzbedürftige Personen betrifft. Dennoch obliegt es dem für die Datenverarbeitung Verantwortlichen zu beurteilen, ob ein hohes Risiko vorliegt.
   - *Kriterium 2 – Eintrittswahrscheinlichkeit eines hohen Risikos (Aufzählung)*: Die Verordnung sieht drei Arten von Datenverarbeitungsvorgängen vor, für die eine DSFA erforderlich ist, da diese Vorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen. Mit anderen Worten, die folgenden Datenverarbeitungsvorgänge werden vom Gesetz her als sehr risikoreich eingestuft; diese Liste ist jedoch nicht erschöpfend:
     - „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 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten und
     - „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ (Artikel 35 Abs. 3).
   - *Kriterium 3 – Eintrittswahrscheinlichkeit eines hohen Risikos (positive Auflistung von Datenschutzbehörden)*: Eine nationale oder regionale Datenschutzbehörde (DSB) ist berechtigt, für ihren Zuständigkeitsbereich weitere Arten von Verarbeitungsvorgängen festzulegen, für die eine DSFA erforderlich ist (Artikel 35 Abs. 4).
   - *Kriterium 4 – Eintrittswahrscheinlichkeit eines hohen Risikos (negative Auflistung von DSBs)*: Dieselbe Behörde kann für ihren Zuständigkeitsbereich weitere Arten von Verarbeitungsvorgängen festlegen, für die *keine* DSFA erforderlich ist (Artikel 35 Abs. 5). Sollten beide Listen allgemein grenzüberschreitende Datenverarbeitungsvorgänge betreffen, sind diese nach Maßgabe des Kohärenzverfahrens dem Europäischen Datenschutzausschuss (EDSA) zur Stellungnahme zu übermitteln (Artikel 35 Abs. 4 – 6). Der EDSA gibt seit 2018 solche Stellungnahmen ab.
   - *Kriterium 5 – frühere Folgenabschätzung von Vorschriften*: Soweit die Mitgliedstaaten nicht anderweitig entscheiden, ist das DSFA-Verfahren für personenbezogene Daten, die zur Erfüllung einer rechtlichen Verpflichtung (Artikel 6 Abs. 1 Buchstabe c)) oder im öffentlichen Interesse (Artikel 6 Abs. 1 Buchstabe e)) nach Maßgabe des Unionsrechts oder des Rechts eines Mitgliedstaates verarbeitet werden und sofern die Verarbeitung bereits im Rahmen eines anderen Bewertungsverfahrens im Zusammenhang mit dem Erlass dieser Rechtsgrundlage erfolgte, nicht mehr erforderlich. Hierzu muss das andere Beurteilungsverfahren jedoch im Wesentlichen die Bedingungen der DSGVO beachten (Artikel 35 Abs. 10).

- *Kriterium 6 – Ausnahmen für bestimmte Berufe*: Betreffen die Datenverarbeitungsvorgänge „personenbezogene Daten von Patienten oder von Mandanten und erfolgen sie durch einen einzelnen Arzt, sonstige Angehörige eines Gesundheitsberufes oder Rechtsanwalt“, so gelten diese Vorgänge nicht als umfangreich (siehe z.B. Artikel 35 Abs. 3 Buchstabe b)). Daher ist die DSFA für solche Datenverarbeitungsvorgänge nicht erforderlich (Erwägungsgrund 91).

Wenn eines der ersten drei Kriterien erfüllt ist, ist ein DSFA-Verfahren zwingend vorgesehen. Ist dagegen eines der letzten drei Kriterien erfüllt, wird der für die Datenverarbeitung Verantwortliche von der Durchführung des Bewertungsverfahrens befreit.

2) *Beschreibung*: Nach der Verordnung hat die Folgenabschätzung mit einer „systematischen Beschreibung der geplanten Verarbeitungsvorgänge“ zu beginnen (Artikel 35 Abs. 7 Buchstabe a)). Diese Beschreibung umfasst insbesondere:

   a) eine *kontextbezogene Beschreibung* der geplanten Datenverarbeitungsvorgänge, insbesondere ihrer Art, ihres Umfangs, ihres Kontexts und ihrer Zwecke, des berechtigten Interesses des für die Verarbeitung Verantwortlichen (falls zutreffend) und der beteiligten Akteure (betroffene Personen, für die Verarbeitung Verantwortliche, Auftragsverarbeiter, Dritte und Behörden);

   b) eine *technische Beschreibung* der Übermittlung personenbezogener Daten und wenn möglich der diesbezüglichen visuellen Elemente.

   Die Beschreibung der geplanten Datenverarbeitungsvorgänge kann auf der Grundlage der Erstbeschreibung erfolgen, anhand derer festgestellt wurde, ob der Beurteilungsprozess gerechtfertigt war (siehe Etappe 1).

3) *Bewertung des geplanten Verarbeitungsvorgangs oder einer Reihe ähnlicher Vorgänge:* Die Verordnung schreibt die aufeinander folgende bzw. parallele Anwendung von mindestens zwei verschiedenen Bewertungstechniken (Methoden im engeren Sinne) vor, nämlich die Bewertung der Notwendigkeit und der Verhältnismäßigkeit sowie die Risikobewertung. Beide Techniken stellen weitgehende Neuerungen im Datenschutzrecht dar. Entsprechend dem „legal hook“-Ansatz (gesetzliche Verankerung) enthält die DSGVO allgemeine Regelungen zu diesen Techniken, d.h. sie enthält keine Angaben hinsichtlich ihrer konkreten Anwendung.

   a) Die Bewertung der „Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf [ihren] den Zweck“ (Artikel 35 Abs. 7 Buchstabe b)).

      Die Bewertung der Notwendigkeit und Verhältnismäßigkeit bezieht sich auf die Einhaltung der Grundsätze des Schutzes personenbezogener Daten (Artikel 5 Abs. 1). Insbesondere betrifft sie den Grundsatz der Zweckbindung – d.h. zunächst wird die Frage des Zwecks des Verarbeitungsvorgangs untersucht, d.h. ob die „Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann“ (Erwägungsgrund 39) und ob die personenbezogenen Daten für „festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“ (Artikel 5 Abs. 1 Buchstabe b)). Diese Bewertung betrifft ferner den Grundsatz der Rechtmäßigkeit der Verarbeitung (Artikel 6) sowie die Grundsätze der Datenminimierung, Richtigkeit und Speicherbegrenzung. Mit anderen Worten, es wird untersucht, ob die personenbezogenen Daten auf „rechtmäßige Weise, nach Treu und Glauben und auf nachvollziehbare Weise“ verarbeitet werden, „dem Zweck angemessen, erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sind, „sachlich richtig und erforderlichenfalls auf dem neuesten Stand“ sind und nicht länger als notwendig gespeichert werden (Artikel 5 Abs. 1 Buchstabe a) – e)).

      Diese Bewertung erfolgt auf der Grundlage einer faktenbasierten Analyse, die sich auf hinreichende, klar formulierte und überprüfbare Beweise stützt. Die Beurteilung der Notwendigkeit und Verhältnismäßigkeit unterscheidet sich inhaltlich im privaten und öffentlichen Sektor. Darüber hinaus ist beim öffentlichen Sektor zwischen Gesetzgebung und Gesetzesanwendung zu differenzieren.

   b) Die Bewertung der „Risiken für die Rechte und Freiheiten der betroffenen Personen“ (Artikel 35 Abs. 7 Buchstabe c)).

      Die Risikobewertung im Rahmen der DSFA beinhaltet typischerweise eine detaillierte Identifizierung, Analyse und Bewertung der möglichen künftigen negativen Folgen von Datenverarbeitungsvorgängen und konkret der durch solche Vorgänge verursachten Schäden. Deren Bewertung bezieht sich auf den „physischen, materiellen oder immateriellen Schaden“ und umfasst beispielsweise Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste oder Rufschädigung, Verlust der Vertraulichkeit, unbefugte Aufhebung der Pseudonymisierung, erhebliche wirtschaftliche oder gesellschaftliche Nachteile, Verlust der Kontrolle über personenbezogene Daten und die Verarbeitung unbefugter sensibler Daten oder Daten von schutzbedürftigen natürlichen Personen, insbesondere von Kindern (Erwägungsgrund 75 enthält eine längere Liste an Beispielen für solche Schäden; deren nähere Ermittlung erfolgt während des Bewertungsprozesses). Die Entscheidung darüber, ob eine Verarbeitung ein Risiko beinhaltet und – in der Folge – ob das Risiko hoch ist, trifft der für die Datenverarbeitung Verantwortliche „anhand einer objektiven Bewertung“ (Erwägungsgrund 76).

      Die im Rahmen der DSFA zu bewertenden Risiken beziehen sich auf natürliche Personen, einschließlich betroffener Personen und der Gesellschaft im Allgemeinen, nicht jedoch auf die für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeiter. Diese Risiken betreffen die Wahrnehmung von Rechten und Freiheiten durch Einzelpersonen und stellen daher nicht (nur) Compliance-Risiken dar. Angesichts des Ziels der Verordnung erstrecken sich diese Risiken auf einen weitaus größeren Bereich als das Recht auf den Schutz personenbezogener Daten und erfassen uneingeschränkt andere Rechte und Freiheiten. (Erwägungsgrund 4 nennt Rechte wie etwa Privatleben, Recht auf einen wirksamen Rechtsbehelf, ein faires Verfahren, Vielfalt der Kulturen, Religionen und Sprachen, Freiheiten wie Gedankenfreiheit, Gewissens- und Religionsfreiheit, Freiheit der Meinungsäußerung, Informationsfreiheit und unternehmerische Freiheit.)

      Die Bewertung der Risiken hinsichtlich der Rechte und Freiheiten folgt weitgehend einem qualitativen Ansatz. Geprüft werden der Schweregrad (das Ausmaß des Risikos) und die Eintrittswahrscheinlichkeit (z.B. gering, mittel oder hoch) unter Berücksichtigung der „Ursache“, der „Besonderheit“ (Erwägungsgrund 84) sowie der „Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“ (Erwägungsgründe 75-76). Bestimmte Datenschutzrisiken, wie etwa Datensicherheitsrisiken, könnten quantitativ beurteilt werden (z.B. durch Berechnung des Schweregrads und der Wahrscheinlichkeit). Die Beschreibung der geplanten Datenverarbeitungsvorgänge kann auf der Grundlage der Erstbeschreibung erfolgen, anhand derer festgestellt wurde, ob der Beurteilungsprozess gerechtfertigt war (siehe Etappe 1).

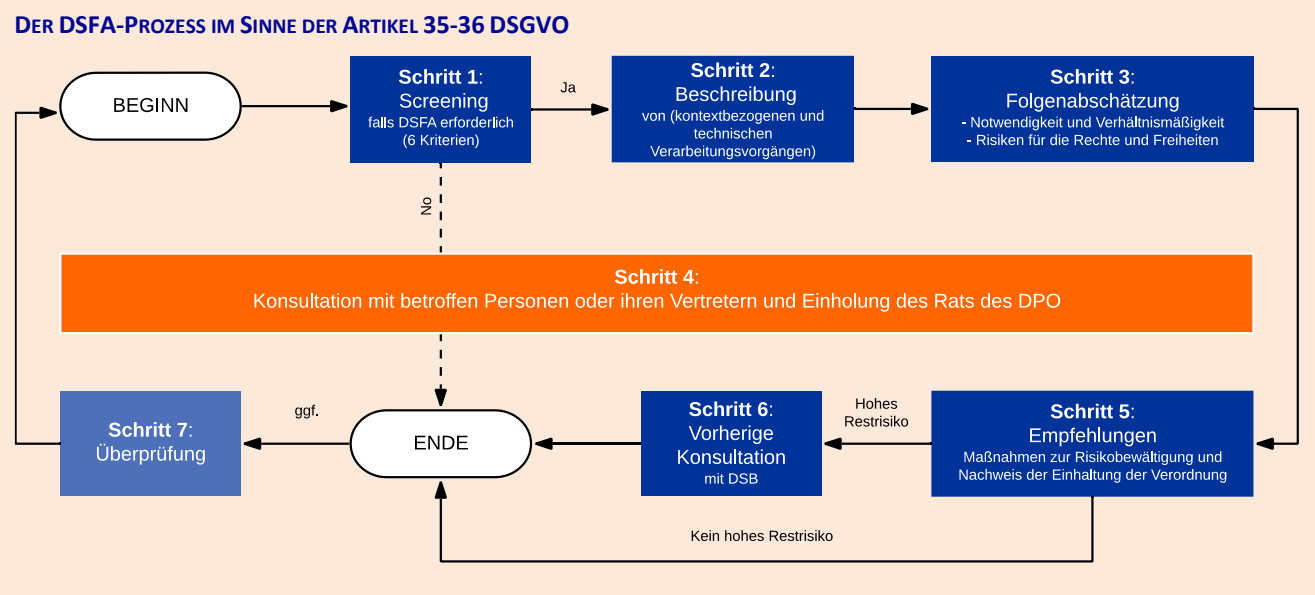
4) *Beteiligung von Interessenträgern (Beteiligung der Öffentlichkeit) bei der Entscheidungsfindung*: Die Verordnung sieht vor, dass „gegebenenfalls“ der Standpunkt der betroffenen Personen oder ihrer Vertreter unter gebührender Beachtung des berechtigten Interesses an Vertraulichkeit (d.h. der „Schutz gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge“) eingeholt wird (Artikel 35 Abs. 9). Die „Zweckmäßigkeit“ einer Konsultation ist nicht als „optional“ zu verstehen. Ausnahmen sind möglich, wenn beispielsweise keine neuen Erkenntnisse durch die Einbeziehung von Interessenträgern gewonnen werden konnten oder wenn dies mit einem, gemessen an den Ergebnissen, unverhältnismäßigen Aufwand verbunden wäre.

Entscheidungen hinsichtlich der Nichteinbeziehung von Interessenträgern oder einer Abweichung einer solchen Konsultation sind zu begründen und zu dokumentieren. Gleichzeitig ist auf Anfrage der Rat eines Datenschutzbeauftragten (DPO) einzuholen, sofern ein solcher benannt wurde (Artikel 35 Abs. 2 und 39 Abs. 1 Buchstabe c)); nichtsdestotrotz *kann* der DPO den Bewertungsvorgang *nicht* durchführen.

5) *Empfehlungen*: Die Verordnung verlangt den Abschluss des Bewertungsprozesses anhand einer Liste empfohlener Maßnahmen zur:
   a) Bewältigung der Risiken einschließlich „Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird“ und
   b) Gewährleistung der Einhaltung der Verordnung, wobei „den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird“ (Artikel 35 Abs. 7 Buchstabe d)).

   Die Ergebnisse der Abschätzung „sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit [der] Verordnung in Einklang steht“ (Erwägungsgrund 84).
6) *Vorherige Konsultation einer Aufsichtsbehörde:* Die Verordnung knüpft den DSFA-Prozess an eine vorherige Konsultation. Im Falle eines hohen Restrisikos, d.h. wenn der Beurteilungsprozess ein hohes Risiko aufzeigt, das auch nach der Umsetzung der Empfehlungen aus dem Beurteilungsprozess durch den für die Verarbeitung Verantwortlichen verbleibt, ist dieser verpflichtet, sich vor Beginn der Verarbeitung personenbezogener Daten und nach einem vorgeschriebenen Verfahren an eine Datenschutzbehörde zur Konsultation zu wenden (Artikel 36).
7) *Überprüfung*: „Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind“ (Artikel 35 Abs. 11). Erfolgen kann diese Überprüfung folglich erst nach einem bestimmten Zeitraum, und zwar zu Kontrollzwecken oder bei einer Änderung, aufgrund derer die vorherige Bewertung (teilweise oder ganz) überholt ist. Die Verordnung regelt jedoch nicht die Folgen einer solchen Überprüfung; da sich das Risiko ändern kann, muss der Bewertungsprozess unter Umständen (teilweise oder ganz) neu durchgeführt werden.

Die oben vorgeschlagene spezifische Methode für die DSFA legt den Grundstein für die Anpassung dieser Methode an einen bestimmten Anwendungskontext, z.B. im Bereich der Telekommunikation oder „intelligenter“ Energienetze. Dabei wird der „Schutz personenbezogener Daten“ gewährleistet und der Nachweis für die „Einhaltung der Verordnung“ erbracht (Artikel 35 Abs. 7 Buchstabe d)).



Nach dieser Auslegung deckt die DSGVO nicht alle zehn Etappen der generischen Methode ab. Manche Etappen erfordern nicht notwendigerweise eine gesetzliche Regelung; sie sind jedoch aus pragmatischen Gründen im Bewertungsprozess enthalten. Insbesondere regelt die Verordnung nicht das sog. *Scoping*. (In der Praxis würde im Rahmen des *Scoping* beispielsweise festgelegt, welche Teile des Rechts auf den Schutz personenbezogener Daten durch eine geplante Datenverarbeitung beeinträchtigt werden können und wer eine betroffene Person oder Vertreter einer betroffenen Person bei einer solchen Verarbeitung ist.) Andere Etappen der generischen Methode können größtenteils anhand sonstiger Bestimmungen der Verordnung ausgelegt werden. Hinsichtlich der *Planung und Vorbereitung* bestimmt die Verordnung lediglich, dass beispielsweise ein einzelner Bewertungsprozess mehrere ähnlich geartete Verarbeitungsvorgänge erfassen kann (Erwägungsgrund 92) oder dass ein Datenverarbeiter einen für Datenverarbeitung Verantwortlichen bei der Durchführung des Bewertungsprozesses zu unterstützen hat (Artikel 28 Abs. 3 Buchstabe f)). Bezüglich der *Dokumentation* ist der Verantwortliche beispielsweise verpflichtet, den Nachweis dafür zu erbringen, dass die Verarbeitung gemäß der Verordnung erfolgt (Artikel 24 Abs. 1). Bei der *Qualitätskontrolle* beispielsweise wird ein DPO mit der Kontrolle des Verarbeitungsvorgangs (Artikel 39 Buchstabe c)) und eine DSB mit der Durchführung von Datenschutzüberprüfungen betraut (Artikel 58 Abs. 1 Buchstabe b)). Im Vergleich zur generischen Methode sieht die DSGVO jedoch den zusätzlichen Schritt *Vorherige Konsultation einer Datenschutzbehörde* vor.

4 ABSCHLIEßENDE BEMERKUNGEN

Im vorliegenden Strategiepapier legt das d.pia.lab den Grundstein für zwei Folgenabschätzungsmethoden: zum einen eine generische Methode, die den Rahmenbedingungen seines letzten Strategiepapiers Rechnung trägt und eine Basis für auf spezifische Praxisbereiche und Anwendungskontexte zugeschnittene Bewertungsmethoden bilden soll; zum anderen eine auf der generischen Methode aufbauende Methode für die DSFA in der EU, die nach Maßgabe der DSGVO ausgelegt ist.

In der EU basiert der DSFA-Prozess auf einer Reihe neuer Kernkonzepte wie etwa dem Risiko für Rechte. Aufgrund des sog. „legal hook"-Ansatzes (gesetzliche Verankerung) ist der Prozess im Gesetz jedoch eher minimal geregelt und erfordert Auslegung und Anleitung. Vor diesem Hintergrund hat das d.pia.lab den Versuch unternommen, die DSFA-Methode nach Maßgabe der Artikel 35-36 der DSGVO abzuleiten, wobei der Schwerpunkt auf umstrittenen, unzureichend diskutierten Themen lag. (Da neben der DSGVO auch einige andere Rechtinstrumente der EU eine Verpflichtung zur Durchführung des DSFA-Prozesses normieren, könnten die vorliegenden Ausführungen analog gelten.) Fragen wie Techniken zur Beurteilung der Notwendigkeit und Verhältnismäßigkeit, zur Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen und zur Einbeziehung der Interessenträger, einschließlich der Öffentlichkeit, verdienen allerdings mehr Aufmerksamkeit seitens der Wissenschaft und der Fachwelt, an die sich das d.pia.lab in seinen künftigen Beiträgen wenden möchte.

Daneben bedarf es für die nach Maßgabe der DSGVO abgeleitete Methode für die DSFA nach wie vor einer eingehenden Anleitung, Klärung und Anpassung. Hierfür eignet sich insbesondere der EDSA, der in Abstimmung mit den nationalen und regionalen Datenschutzbehörden der EU agiert, um zu mehr Rechtssicherheit zu gelangen und sich und diese als „Referenzzentren" für sämtliche Arten der Folgenabschätzung zu etablieren. In diesem Zusammenhang sei vor allem auf die Muster für DSFA hingewiesen, die auf die Gegebenheiten des jeweiligen Mitgliedstaats und einen bestimmten Anwendungskontext (z.B. Industrie oder Governance-Sektor) zugeschnitten sind.

AUSGEWÄHLTE RELEVANTE QUELLEN

Arnstein, Sherry R. (1969) "A Ladder of Citizen Participation," *Journal of the American Institute of Planners*, 35(4), S. 216–224. doi: 10.1080/01944366908977225.

De Hert, Paul, Dariusz Kloza and David Wright (2012) "Recommendations for a Privacy Impact Assessment Framework for the European Union," Brussels – London. https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf.

Gellert, Raphaël (2018) "Understanding the notion of risk in the General Data Protection Regulation", *Computer Law & Security Review* 34(2), S. 279–288. doi: 10.1016/j.clsr.2017.12.003.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," *d.pia.lab Policy Brief* 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

van Dijk Niels, Raphaël Gellert and Kjetil Rommetveit (2016) "A risk to a right? Beyond data protection risk assessments", *Computer Law & Security Review*, 32(2), S. 286–306. doi: 10.1016/j.clsr.2015.12.017.

Duden Deutsches Universalwörterbuch; https://www.duden.de/woerterbuch.

LITERATURHINWEISE

Datenschutzgruppe nach Artikel 29 (2017) *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"*, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

International Organization for Standardization [ISO] (2018) *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

Jasanoff, Sheila (2012) *Science and Public Reason*. London: Routledge. doi: 10.4324/9780203113820.

European Data Protection Supervisor [EDPS] (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2017) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* [draft]. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

EDPS (2019) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf.

Grunwald, Armin (2018) *Technology Assessment in Practice and Theory*. Abingdon: Routledge. doi: 10.4324/9780429442643.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*. Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Noble, Bram F. (2015) *Introduction to Environmental Impact Assessment. A Guide to Principles and Practice*. Toronto: OUP Canada.

ÜBER DAS D.PIA.LAB

Das **Brussels Laboratory for Data Protection & Privacy Impact Assessments** bzw**. d.pia.lab** verbindet Grundlagen-, Methoden- und angewandte Forschung, bietet Schulungen an und leistet Politikberatung für Folgenabschätzungen in den Bereichen Innovation und Technologieentwicklung. Die rechtlichen Aspekte des Schutzes der Privatsphäre und personenbezogener Daten bilden den Kern seiner Tätigkeit. Das Labor befasst sich jedoch auch mit anderen Fachrichtungen wie Ethik, Philosophie, Anwendungsstudien und Naturwissenschaften und Wissenschaftsforschung (science and technology studies, STS). Das im November 2015 gegründete d.pia.lab ist Teil der Research Group on Law, Science, Technology & Society (LSTS) an der Vrije Universiteit Brussel (VUB), Belgien, und baut auf den Erfahrungen dieser Gruppe auf.

Das Fachwissen des Labors gründet sich auf Datenschutz-Folgenabschätzungen im Rahmen zahlreicher abgeschlossener und laufender Forschungsprojekte wie etwa PERSONA, HR-RECYCLER, SYSTEM (von der EU kofinanziert) and PARENT (von Innoviris kofinanziert). Die in diesem Strategiepapier zum Ausdruck gebrachten Meinungen geben nicht die Ansichten der Trägereinrichtungen wieder.

Wir danken – in alphabetischer Reihenfolge – Alexandra Aslanidou, Jonas Breuer, Alessandra Calvi, Roger Clarke, Katerina Demetzou, Catherine Jasserand-Breeman, Anna Johnston, Gianclaudio Malgieri, Anna Mościbroda, Kjetil Rommetveit, Julien Rossi, Juraj Sajfert, Laurens Vandercruysse, Heidi Waem, Ine van Zeeland und einem anonymen Prüfer für sein Feedback zur Vorversion des vorliegenden Strategiepapiers. Deutsche Übersetzung von Dipl.Üb. Sabine Schumann und Dipl.Dol. Janina Schmidt (Februar 2020).

dpialab.org | **dpialab@vub.ac.be**