DSFA
Datenschutz-Folgenabschätzung

Diskussionsvorlage

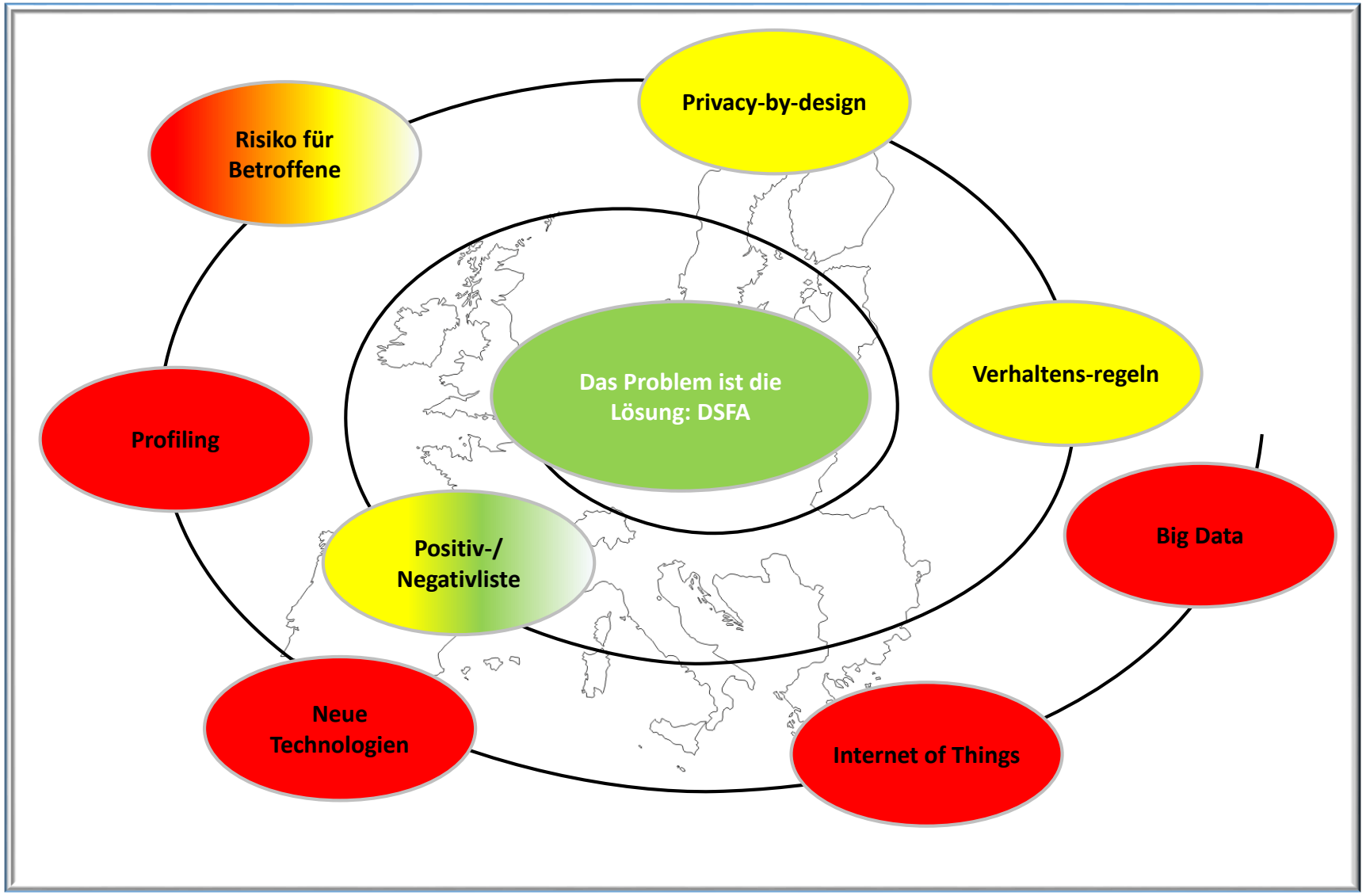
6. DialogCamp, München

17. 2. 2017

Anforderungen an eine DSFA	Überlegungen/Fragen	Folgen
Artikel 35 Absatz 1 DS-GVO „Riskante Datenverarbeitung“	Risikobegriff: • nicht in DS-GVO definiert • objektive Kriterien (EW 76) PIA oder DPIA?	Kein hohes Risiko => keine DSFA -> allgemeines PIA Art. 24, 25, 32) Hohes Risiko => zusätzlich zur PIA: DSFA (= DPIA)
Artikel 35 Absatz 3 DS-GVO „Muss-DSFA-Fälle“	• DSFA nur wenn Bewertung der Person auf automat. Verarbeitung (inkl. Profiling) gründet • keine DSFA bei Patienten- und Mandatendaten, wenn die Verarbeitung durch den Arzt oder Rechtsanwalt erfolgt • Was fällt alles unter optoelektronische Vorrichtung?	• “reines“ Profiling unterliegt nicht der DSFA • Was muss bei Großkanzleien/-praxen berücksichtigt werden?
Artikel 35 Absatz 4-6 DS-GVO „Positiv-/Negativ“-Liste der Aufsichtsbehörden	? Pflicht der Aufsichtsbehörde ➢ Negativ-Liste = keine DSFA ➢ Positiv-Liste = DSFA erforderlich ✓ bei cross border Verarbeitung oder Überwachung => Pflicht zum Kohärenzverfahren	DSFA immer durchführen, auch wenn keine Liste erstellt wurde oder Verarbeitung auf der Negativ-Liste steht?

Anforderungen an eine DSFA	Überlegungen/Fragen	Folgen
Artikel 35 Absatz 7 DS-GVO „Mindestprüfelemente“	• Bekannt aus der Vorabkontrolle • Kombination aus Art. 5 Abs. 1 a-f und Art. 35 Abs. 7	Risikoanalyse/-bewertung Können die identifizierten Risiken mit Garantien oder Sicherheitsvorkehrungen beherrscht werden? • Abhilfemaßnahmen • Sicherheitskonzept • Dokumentation der erbrachten Abhilfemaßnahmen
35 Absatz 9 DS-GVO „Einbeziehung betroffener Personen“	Beispiel Profiling: • iVm Art. 22 Abs. 3 und EW 71 Pflicht bei automatisierter Entscheidung inkl. Profiling ist die betroffenen Person einzubeziehen	• Ausnahme vom Profiling ist die Regel (Art. 22 Abs. 3 lit a-c) z.B. Vertragsabschluss, allerdings: Betroffene muss das Recht auf Einwirkung auf die Entscheidung haben In allen anderen Fällen: kann das Einholen der Standpunkte der betroffenen Personen eine risikominimierende Maßnahme darstellen
Artikel 36 Absatz 2 DS-GVO „Konsultationsverfahren“	• Was konkret prüft die Aufsichtsbehörde? • Gilt Schweigen der Aufsicht als „Genehmigung“? • Könnte „Überforderung“ der Aufsichtsbehörde „sicherheitshalber“ zu Verbot der Verarbeitung führen („Verantwortlicher geht ja selbst von hohem Risiko aus“)	

Weg ist das Ziel!



Artikel 35 Absatz 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 Verarbeitungs-vorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Artikel 35 Absatz 2

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

Artikel 35 Absatz 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 natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Artikel 35 Absatz 4/5

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.
(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss

Artikel 35 Absatz 6

Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten

Artikel 35 Absatz 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 gemäß Absatz 1 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.

Artikel 35 Absatz 8

Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

Artikel 35 Absatz 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 35 Absatz 10

Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

Artikel 35 Absatz 11

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 36 Absatz 2

Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen (….) entsprechende schriftliche Empfehlungen (…). Diese Frist kann (…) um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet (…) über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags (…). Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.