Datenschutz durch Technikgestaltung und unternehmerische Strategie in der Digitalwirtschaft

Verhaltenssteuernde Elemente der DSGVO im Licht einer spieltheoretischen Analyse am Beispiel von Art. 25 Abs. 1

Mona Winau [1], Florian Klaus Kaiser [2], Marcus Wiens [3], Frank Schultmann [4], Indra Spiecker gen. Döhmann [5]

Abstract: Der Beitrag beleuchtet das Konzept des Datenschutzes durch Technikgestaltung nach Art. 25 Abs.1 DSGVO im Spannungsfeld zwischen einer notwendigerweise abstrakten Risikoregulierung und den Gefahren der daraus folgenden Konkretisierungverantwortung datenverarbeitender Wirtschaftsunternehmen. Anhand einer spieltheoretischen Analyse wird nachvollzogen, wie sich Negativanreize der DSGVO aus Bußgeld- und Haftungsrisiken proaktiv nutzen lassen, um die Motivation datenschutzkonformer Firmen zu stärken, die tendenziell ein höheres Eigeninteresse an der Implementierung geeigneter technischer und organisatorischer Maßnahmen haben. Ökonomische Anreize einer Zertifizierung könnten eine datenschutzfreundliche Technikgestaltung für Unternehmen profitabel machen, wenn sich ein entsprechender Markt etabliert. Für die Unterscheidbarkeit datenschutzfreundlich gestalteter Produkte von Angeboten mit geringem Datenschutzniveau können Zertifikate als Signal gegenüber dem Verbraucher dienen und so eine Grundlage für einen innovationsfördernden Wettbewerb für den Datenschutz durch Technikgestaltung schaffen.

Keywords: Rechtsanalyse; Spieltheorie; Regulierung durch Anreize

[1] Karlsruher Institut für Technologie, Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL), Am Fasanengarten 5, 76131 Karlsruhe, Deutschland & Institut für Informations- und Wirtschaftsrecht (IIWR), Vincenz-Preißnitz-Straße 3, 76131 Karlsruhe, Deutschland, mona.winau@kit.edu

[2] Karlsruher Institut für Technologie, Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL), Am Fasanengarten 5, 76131 Karlsruhe, Deutschland & Institut für Industrielehre und Industrielle Produktion (IIP), Hertzstraße 16, 76187 Karlsruhe, Deutschland, florian-klaus.kaiser@kit.edu

[3] Karlsruher Institut für Technologie, Institut für Industrielehre und Industrielle Produktion, Hertzstraße 16, 76187 Karlsruhe, Deutschland, marcus.wiens@kit.edu

[4] Karlsruher Institut für Technologie, Institut für Industrielehre und Industrielle Produktion, Hertzstraße 16, 76187 Karlsruhe, Deutschland & Adelaide Business School, University of Adelaide, frank.schultmann@kit.edu

[5] Goethe-Universität Frankfurt am Main, Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaft, Institut für Öffentliches Recht, Theodor-W.-Adorno-Platz 4, 60629 Frankfurt am Main, Deutschland, spiecker@jur.uni-frankfurt.de

1 Risikobasierte Datenschutzregulierung und Risiken des unternehmerischen Umsetzungsspielraum

Unternehmen, die personenbezogene Daten verarbeiten, müssen gem. Art. 25 Abs. 1 DSGVO[6] dem konkreten Risiko angemessene Datenschutzmaßnahmen bereits in die technische und organisatorische Gestaltung des Verarbeitungsprozesses integrieren. Die technikneutral formulierte und an den abstrakten Begriff des Risikos gekoppelte Pflicht soll einen effektiven Schutz für die Rechte und Freiheiten natürlicher Personen gewährleisten und zugleich eine verhältnismäßige Anpassung der Pflichten an den jeweiligen Verarbeitungskontext beim Verantwortlichen sicherstellen.[7] Allerdings begründen die Regelungsunschärfe und der erhebliche Spielraum des Verantwortlichen bei der Auswahl geeigneter Maßnahmen Rechtsunsicherheit und bergen die Gefahr, dass das Pflichtenprogramm zugunsten der wirtschaftlichen Vorteile einer unangemessenen Datennutzung in der Praxis ausgehöhlt wird.[8] Die Datenschutz-Grundverordnung enthält wiederum diverse rechtliche und ökonomische Anreize, die eine datenschutzkonforme, oder sogar eine datenschutzfreundliche,[9] Verarbeitung attraktiv machen sollen. Aus ihnen ergeben sich Parallelen zu einer Regulierung strategischen Firmenverhaltens, wie sie etwa in Modellen der Wettbewerbsregulierung und im öffentlichen Wirtschaftsrecht vorkommen.[10]

1.1 Kontextabhängigkeit der Datenverarbeitung und ihre abstrakte Regulierung

Informationen sind kontextabhängig. Eine einzelne Information kann zu vorhandenem Wissen hinzutreten und den Schlüssel zu einer Erkenntnis bilden oder eine einzelne Information kann ohne weiteren Nutzen bleiben. Ihr kann in diversen Kontexten verschiedene Bedeutung zukommen und sie kann zu unterschiedlichen Schlussfolgerungen führen. Wegen der Abhängigkeit des Nutzens einer Information von ihrer Art, ihrem Zustand, Kontext und Verarbeitungsmöglichkeiten ist die Bestimmung eines objektiven wirtschaftlichen Wertes für Daten mit erheblichen Schwierigkeiten verbunden.[11] Ebenso ist das Risiko, das mit der Preisgabe eines personenbezogenen Datums für die betreffende Person verbunden ist - etwa die Gefahr weitreichender oder falscher Schlüsse über dieselbe - von den genannten Faktoren abhängig und nicht abstrakt feststellbar.[12] Allgemein lässt sich aber feststellen, dass sowohl der ökonomische Nutzen von personenbezogenen Daten als auch das Risiko

[6] Folgende Artikel ohne Kennzeichnung beziehen sich auf die DSGVO.

[7] Art. 29-Gruppe,[Ar14], 2; CIPL, [Ce], 4.

[8] Vgl. [Qu17], 14 ff; [Sc19], 505; [RG20], 40 ff; [By17], 117; [BTH14] formulieren in diesem Kontext "PbD expects [...] that the cat guards the milk", 71, und argumentieren, dass der Abstraktionsgrad von Privacy by Design-Regelungen wegen divergierender rechtlicher und technischer Privacy-Konzepte problematisch ist, 88 ff.

[9] Im Sinne einer über vorgegebene Mindeststandards hinausgehenden datenschutzfreundlichen Verarbeitung.

[10] M.w.N. zu Konzepten des funktionsfähigen Wettbewerbs, [Br10], 11 ff und zur Einbeziehung von Strategie für eine wirksmame Anreizregulierung im öffentlichen Wirtschaftsrecht, 233 ff; zur Rolle des Wettbewerbs in der datenschutzrechtlichen Regulierung, [Po17], 220 ff.

[11] Vgl.[K6b], 305 f; [Hä16], 735 f.

[12] Vgl. EG 75, 76.

ihrer Verarbeitung mit der immens gesteigerten und zukünftig weiter steigenden Menge an Daten[13] und den gigantischen, schnellen und automatisierten Möglichkeiten ihrer Speicherung, Kombination und Auswertung sehr hoch ist.[14] Wie das Bundesverfassungsgericht bereits 1983 erkannte, ist das Recht auf informationelle Selbstbestimmung, in den Grenzen des Gemeinschaftsbezugs von Informationen, eine Voraussetzung für die freie Grundrechtsausübung des Einzelnen und gilt unter den Bedingungen automatisierter Verarbeitung für jedes beliebig inhaltsarme Datum, solange es einen Bezug zur Person zulässt.[15] Je weiter die technischen Möglichkeiten fortschreiten und sich aus vorhandenen Informationen immer mehr und aussagekräftigere neue Informationen erschließen lassen, desto größer ist das Risiko, dass die Verarbeitung auch nur weniger und scheinbar trivialer Informationen über eine Person birgt. Wenn es bereits 1983 unter den Bedingungen automatisierter Verarbeitungstechniken keine „belanglosen“[16], oder ökonomisch ausgedrückt, wertlosen Daten zu einer Person gab,[17] gilt dies heute erst recht.[18]

1.2 Abstrakte Regulierung, Strategie und Anreizsteuerung

Die Technikneutralität und der risikobasierte Ansatz der Datenschutz-Grundverordnung begegnen dem sich fortlaufend erhöhenden, aber nicht allgemeingültig bestimmbaren, Risiko der Verarbeitung personenbezogener Daten.[19] Technikneutralität bedeutet, dass die Verordnungsregelungen für jede Verarbeitungstechnik (manuell oder automatisiert) gleichermaßen gelten.[20] Risikobasiert sind Pflichten der Verantwortlichen insoweit, wie ihre Geltung, ihr Umfang oder ihre Intensität vom Risiko der jeweiligen Verarbeitung abhängt.[21] Eine Datenschutz-Folgeabschätzung etwa muss gem. Art. 35 Abs. 1 nur für solche Verarbeitungen durchgeführt werden, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bergen. Und auch der Umfang und die Intensität von technischen oder organisatorischen Maßnahmen, die Verantwortliche gem. Art. 24 Abs. 1 zur Gewährleistung einer verordnungskonformen Verarbeitung und deren Nachweis treffen müssen, sind an das Risiko der Verarbeitung gekoppelt. Eine konkretere Ausgestaltung dieser Pflicht zu technischen und organisatorischen Schutzmaßnahmen

[13] Vgl. [RGR18].

[14] Dies wird anhand der rege geführten Debatten über Eigentums-, Besitz oder Nutzungsrechte an Daten und die wettbewerbsrechtliche Relevanz von Datenschutzrechtsverstößen deutlich, m.w.N. zu Eigentums-, Besitz- oder Nutzungsrechte an Daten, [K0]; [Ho19a];[Ad20]; zur kartellrechtlichen Debatte, [K6b]; [K6a]; [Ke16]; zur BGH-Entscheidung im Eilverfahren (Beschl. V. 23.6.2020 – KVR 69/19), [Po20], 1275. Nach der EU-Richtlinie über Verträge über digitale Inhalte und Dienstleistungen (RL (EU) 2019/770) wird die Bereitstellung personenbezogener Daten von Nutzern als Entgelt angesehen, [SS19], 418; kritisch [Hä16].

[15] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 = NJW 1984, 421 f.

[16] BVerfG, Urt. V. 15.12.1983 – 1 BvR 209/83 = NJW 1984, 419 (422).

[17] Dies drückt sich insbesondere auch in der "formal indifference"[Zu15] der Extraktion von Daten aus.

[18] Siehe auch [Sc17], 124.

[19] Vgl.[BTH14], 65, 68;[Qu17], 4; Art. 29-Gruppe, [Ar14], 2; CIPL, [Ce], 3 f; zu Art. 25, [By17], 106.

[20] Vgl. EG 15; näher zum Prinzip der Technikneutralität, [Ve18], 73 ff; [BTH14] argumentieren, dass auch der europäische Datenschutzregulierung dennoch eine gewisse Technikausrichtung innewohnt, 77 ff.

[21] Vgl. [Sc19], 503.

ist die hier betrachtete Pflicht zum Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1,[22] oft auch - begrifflich unpräzise - als „Privacy by Design“ oder treffender „Data Protection by Design“ bezeichnet.[23] Die Bestimmung des Risikos und die Spezifizierung des Pflichtenprogramms für die konkrete Verarbeitung obliegt dem Verantwortlichen selbst.[24] Sie lässt in besonderem Maße Raum für eine strategische unternehmerische Entscheidung.

Aus ökonomischer Perspektive stehen die Potentiale neuer technischer Möglichkeiten und ihr gewinnbringender Einsatz im Vordergrund. Die meisten privaten Wirtschaftsunternehmen haben längst die automatisierte Informationsverarbeitung in ihre Prozesse integriert und stützen hierauf teilweise sogar die Finanzierung ihrer Produkte.[25] In diesem Zusammenhang wird vielfach von Daten als „Rohstoff des 21. Jahrhunderts“ gesprochen.[26] Diesen wertvollen Rohstoff in möglichst großem Umfang zu erwerben, um ihn gewinnbringend weiterzuverarbeiten oder verkaufen zu können, entspricht auf den ersten Blick einer auf Ertrag fokussierten, d.h. ökonomischen, Handlungsweise, während eine datensparsame, zweckgebundene, speicherbegrenzte und transparente Verarbeitung entsprechend den Grundsätzen aus Art. 5 Abs. 1 in Gegensatz zu ihr tritt.[27] Technische und organisatorische Datenschutzmaßnahmen sind außerdem mit zusätzlichen Kosten verbunden.[28] Damit sich eine solche Investition aus ökonomischer Sicht lohnt, muss sich aus ihnen ein Nutzen ergeben, der die Investitionskosten einschließlich des Verzichts auf einen möglichen Gewinn aus einer weitreichenden Verarbeitung personenbezogener Daten übersteigt.[29] Um den Nutzen zu erhöhen, hat der europäische Gesetzgeber die Implementierung von technischen und organisatorischen Gestaltungsmaßnahmen mit rechtlichen und ökonomischen Anreizen verknüpft.[30]

2 Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1

Die Grundidee der Pflicht zum Datenschutz durch Technikgestaltung ist, dass Maßnahmen zum Schutz der Betroffenen unmittelbar in die verwendete Hard- und Software eingebaut und in organisatorische Abläufe der Verarbeitung personenbezogener Daten, über ihren gesamten Lebenszyklus hinweg, integriert werden.[31] Es handelt sich also um eine Pflicht zur datenschutzrechtlichen Gestaltung von Verarbeitungsprozessen allgemein und nicht

[22] Hartung, [KB20], Art. 24 Rn 9; Martini, [Pa21b], Art. 24 Rn 1; [By17], 114.
[23] Hartung,[KB20], Art. 25 Rn 1; Hansen, [SHSgD19], Art. 25 Rn 23; [By17], 115 f.
[24] [Sc19], 503 f;[Qu17], 7, 9 ff; [Qu18].
[25] Solche Geschäftsmodelle werden unter dem Begriff der „Datenwirtschaft“ diskutiert, [Ze15]; [Dr17].
[26] „Personal data is the new oil of the internet and the new currency of the digital world.“ Meglena Kuneva, ehemalige EU-Kommissarin für Verbraucherschutz nach [HG16], m.w.N. [Po19], 321; [K0], 24; eine Formulierung, die auch von der deutschen Bundeskanzlerin verwendet wird, FAZ, [Fr]; Bulletin der Bundesregierung, [Bu], 5.
[27] Zum Spannungsverhältnis zwischen der Ökonomisierung der Datenverarbeitung und Grundlagen der Datenschutzregulierung, [Hä16], 738 f; zwischen Big Data und Grundprinzipen der DSGVO, [SgD17a];[Za17].
[28] Siehe auch [BTH14], 75.
[29] Vgl. auch [RG20], 39.
[30] Mantz, [Sy18], Art. 25 Rn 78; [Th16], 715 f; als unzureichend bewertend [RG20], 52 ff, 56; [By17], 116 f, 119.
[31] Petri, [SHSgD19], Art. 24 Rn 2 ff; [By17], 106.

nur der Technikgestaltung.[32] Verantwortliche haben gem. Art. 25 Abs. 1 den Stand der Technik und die Implementierungskosten, aber auch Art, Umfang, Umstände und Zwecke der Verarbeitung, sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten des Betroffenen bei der Entscheidung über geeignete Maßnahmen zur Gewährleistung einer datenschutzkonformen Verarbeitung einzubeziehen. Insbesondere die Grundsätze aus Art. 5 Abs. 1 sollen durch eine datenschutzkonforme Technikgestaltung unmittelbar bei der Verarbeitung personenbezogener Daten umgesetzt werden.[33] Die Risiken der jeweiligen Verarbeitung für die Rechte und Freiheiten der betroffenen Person sollen dadurch von den Verantwortlichen selbst begrenzt werden.[34]

3 Konkretisierungsverantwortung und unternehmerische Strategie

Die Beurteilung des Risikos und die Auswahl geeigneter Maßnahmen obliegen in erster Linie den Verantwortlichen selbst. Eine Konkretisierung oder gar Definition des Risikobegriffs, über die genannten Faktoren der Eintrittswahrscheinlichkeit und der Schwere und die Beispiele in EG 75 hinaus, enthält die Verordnung nicht.[35] Die Datenschutz-Folgeabschätzung kann zumindest Anhaltspunkte zur Methodik der Risikobestimmung geben, ist aber nur für Verarbeitungen mit voraussichtlich hohen Risiken verpflichtend (Art. 35 Abs. 1). [36] Bei der Risikobewertung können sich die Verantwortlichen an konkretisierenden Leitlinien, Kurzpapieren und Empfehlungen von Datenschutzaufsichtsbehörden oder aus entsprechender Fachliteratur orientieren,[37] müssen den konkreten Fall letztlich aber eigenverantwortlich beurteilen. Dabei bleibt das Risiko der Verarbeitung allerdings nur einer, wenn auch ein zentraler, von mehreren Faktoren, die bei der Entscheidung über geeignete technische und organisatorische Maßnahmen gem. Art. 25 Abs. 1 zu berücksichtigen sind. Bei der konkreten Maßnahmenauswahl und der Beurteilung ihrer Geeignetheit anhand der genannten abstrakten Kriterien können Verantwortliche die Beispiele in EG 78 S. 3 sowie ebenfalls Maßnahmenvorschläge und Empfehlungen aus Öffentlichkeitsarbeit und Literatur heranziehen.[38] Für die Entscheidung verbleibt ihnen letztlich ein erheblicher Spielraum.[39] Trotz dieses Entscheidungsspielraums bei der Maßnahmenauswahl ist das Kriterium der Geeignetheit binär (geeignet - ungeeignet) und vollständig gerichtlich überprüfbar.[40] Aus den in Art.

[32] Martini/Hansen,[SHSgD19], Art. 25 Rn 16.

[33] EDSA, [Eub], 7; Hartung, [KB20], Art. 25 Rn 10; [By17], 115.

[34] [Qu18], 503. Auch wenn die geforderten Maßnahmen sich klar auf die Umsetzung der Verordnungsregelungen beschränken und auch bei besonders hohen Risiken für andere Grundrechte, etwa durch Diskrimnierungsgefahren oder Beeinträchtigungen der Meinungsfreiheit, keine darüberhinausgehenden Schutzvorkehrungen einschließen, kann die Kopplung von Umfang und Intensität der Datenschutzmaßnahmen an das jeweilige Verarbeitungsrisiko mittelbar auch einen Schutz für andere Rechte und Freiheiten entfalten. Das maßgebliche Risiko der Verarbeitung bezieht sich ausdrücklich nicht nur auf Datenschutz- und Privatheitsrechte (Art. 7 und 8), sondern allgemein auf Rechte und Freiheiten natürlicher Personen, EG 75;[Qu17]; DSK, [Un].

[35] [Sc19], 504.

[36] Vgl. auch [Sc19], 504 f; Martini,[Pa21b], Art. 25 Rn 37c.

[37] Z.B. Art. 29-Gruppe, [Ar]; DSK, [Un]; EDSA, [Eub], 11.

[38] Z.B. das Standard-Datenschutzmodell, DSK, [DS]; kritisch zur unspezifischen Regelung [RG20], 42 f.

[39] Hansen, [SHSgD19], Art. 25 Rn 36.

[40] Vgl. Martini, [Pa21b], Art. 25 Rn 36; zu grundrechtlichen Aspekten für eine Grenzziehung, [By17], 105 (109 ff).

25 Abs. 1 genannten Kriterien ergibt sich ein verhältnismäßiges Mindestpflichtenprogramm des Verantwortlichen als justiziable Untergrenze für den konkreten Fall.[41] Darüber hinaus lässt der unternehmerische Entscheidungsspielraum bei der Auswahl der Maßnahmen eine graduelle Abstufung der Datenschutz-Technikgestaltung zu. Der Verantwortliche kann selbst strategisch entscheiden, ob er Schutzmaßnahmen integriert, die er in Anbetracht des ermittelten Risikos für gerade noch geeignet hält, oder solche, die darüber hinausgehen.[42] So kann etwa der Transparenzgrundsatz (Art. 5 Abs. 1 lit. a) für Online-Dienste umgesetzt werden, indem lediglich eine Datenschutzerklärung zur Verfügung gestellt wird oder der Nutzer mithilfe eines Datenschutz-Dashboards die konkret zu seiner Person verarbeiteten Daten selbst überblicken und bestenfalls, zur Umsetzung weiterer Datenschutzgrundsätze, auch selbst berichtigen und löschen oder über ihre Verwendung entscheiden.[43]

Entscheiden sich mehrere Unternehmen für eine datenschutzfreundliche Technikgestaltung,[44] könnten sich neue Märkte für datenschutzfreundliche Angebote etablieren, deren Wettbewerb die Innovation bei der Technikgestaltung fördern kann und die einen gewissen Anpassungsdruck auf Anbieter in bestehenden Märkten ausüben könnten.[45] Geht man davon aus, dass datenverarbeitende Unternehmen sich überwiegend fremdhergestellter technischer Systeme bedienen,[46] betrifft dies auch die Sphäre der Hersteller von Hard- und Softwareprodukten. Obwohl die Hersteller nicht Verantwortliche und damit nicht von der Regelung des Art. 25 Abs. 1 erfasst sind, könnten sie mit Produkten, die hinter den nachgefragten datenschutzrechtlichen Standards zurückbleiben, nicht mehr am Markt bestehen.[47] Da das datenschutzrechtliche Pflichtenprogramm aus Art. 25 Abs. 1 nicht statisch ist, sondern wiederum vom Stand der Technik[48] und den Implementierungskosten abhängt, kann sich auch die rechtliche Grenze für das Mindestmaß an geeigneten Schutzmaßnahmen verschieben. Eine Anpassung der eigenen Technikgestaltung an verfügbare datenschutzfreundliche Technologie-Standards kann demnach aus unternehmerischer Perspektive nicht nur für die eigene Wettbewerbsfähigkeit interessant sein, sondern auch datenschutzrechtlich für Art. 25 Abs. 1 relevant. Allerdings können neue technische Entwicklungen das Mindestmaß geeigneter Maßnahmen nicht linear steigern. Es ergibt sich unter Verhältnismäßigkeitsgesichtspunkten anhand der genannten Kriterien, von denen der Stand der Technik nur eines

[41] Hansen, [SHSgD19], Art. 25 Rn 37.

[42] Zur Differenzierung zwischen „hard PETs“ und „soft PETs“ [RG20], 49 ff. "Privacy Enhancing Technology"wird hierbei nicht von Privacy by Design-Maßanahmen unterschieden. Zur Differenzierung der Begriffe [BTH14], 69 ff. Allgemeiner zur Skalierbarkeit risikobasierter Pflichten, [Qu17], 9 ff.

[43] Martini, [Pa21b], Art. 25 Rn 29a.

[44] Die EU-Kommission geht zumindest davon aus, dass bislang einige Unternehmen solche Marktvorteile erkannt und genutzt haben, KOM, [EUa], 3; Bewertung des Kommissionsbericht, [Ro21], 661.

[45] Vgl.[By17], 118 f, die Schwierigkeiten eines Markt datenschutzfreundlich gestalteter Produkte betonend.

[46] Vgl. auch [RG20], 40; [Bu20], 1.

[47] [Kl21] zu Auswirkungen auf die schuldrechtlichen Verhältnisse zwischen Herstellern und Verwendern. Mit Verweis auf EG 78 S.4, wonach die Hersteller ërmutigt"werden sollten, ihre Produkte anzupassen, Hartung, [KB20], Art. 25 Rn 13; Hansen, [SHSgD19], Art. 25 Rn 21. Tatsächliche Auswirkungen auf die Sphäre der Hersteller über die Marktentwicklung bezweifeln, [RG20], 43; [By17], 118 f. Auch die Datenethikkommission rät zu einer Inpflichtnahme der Hersteller, [St20]; DEK, [Da19], 74, 119.

[48] Darunter sind am Markt hinreichend verfügbare technische Standards; nicht der Stand der Wissenschaft, aber auch nicht der Stand der Praxis zu verstehen, Hartung,[KB20], Art. 25 Rn 21; Mantz, [Sy18], Art. 25 Rn 37 ff.

ist.[49] Mindestens muss der Verantwortliche aber die technischen Entwicklungen beobachten und fortlaufend in seine Entscheidung einbeziehen.[50]

Entscheidet sich die überwiegende Zahl der datenverarbeitenden Wirtschaftsunternehmen hingegen für eine möglichst weitreichende Datenverarbeitung und treffen sie unzureichende oder nur solche Schutzmaßnahmen, die sie gerade noch für geeignet halten,[51] ist die Wirksamkeit des risikobasierten Pflichtenprogramms stark eingeschränkt. Lediglich das obligatorische Mindestmaß, das aus Art. 25 Abs. 1 folgt, kann dann zwangsweise durch Aufsichtsbehörden im Rahmen ihrer begrenzten Kapazitäten durchgesetzt werden.[52]

4 Anreize für eine datenschutzfreundliche Technikgestaltung

4.1 Verhaltenlenkung durch Anreize in der DSGVO

Das Prinzip der Verhaltenssteuerung durch Anreize ist einfach. Durch externe Einflüsse können positive oder negative Konsequenzen (Anreize) gesetzt werden und die Bewertung des damit verknüpften Verhaltens beeinflussen. Wird infolge des gewünschten Verhaltens eine Belohnung entrichtet oder werden Nachteile eingeschränkt, wird das gewünschte Verhalten im Bewusstsein der Person aufgewertet. Genauso kann durch den Umkehrfall negativer Konsequenzen (Strafe, Minderung von Vorteilen) ein nicht erwünschtes Verhalten für den Adressaten abgewertet werden. Der Einfluss solcher Anreize auf eine Entscheidung nach dem Kosten-Nutzen-Prinzip hängt unter anderem davon ab, inwieweit sich die gesetzten Anreize gegenüber anderen positiven oder negativen Effekten durchsetzen können.[53]

Die folgende Darstellung ist auf die, für die anschließende ökonomische Analyse relevanten, Anreize aus möglichen monetären Einbußen (Bußgelder, Schadensersatz) und aus einem etwaigen ökonomischen Nutzen von Zertifikaten beschränkt.

4.2 Vollzugsmaßnahmen und Haftungsrisiko als Negativanreize

Die Überprüfung und gegebenenfalls die Durchsetzung der Pflicht aus Art. 25 Abs. 1 obliegt den Datenschutzaufsichtsaufsichtsbehörden (Art. 57 Abs. 1 lit. a). Bereits die Möglichkeit behördlicher Vollzugsmaßnahmen entfaltet eine abschreckende Wirkung, solange und soweit sie eine ernstzunehmende Gefahr für Unternehmen darstellt.[54] Sie ist Bestandteil der Anreizstruktur, die eine selbstständige Umsetzung der Verordnungsregelungen sicherstellen

[49] Hansen, [SHSgD19], Art. 25 Rn 27.
[50] [RG20], 37 (42); Mantz, [Sy18], Art. 25 Rn. 39 f; Ansätze für die Bewertung neuer Technikentwicklungen ergeben sich etwa aus einer Analyse zu Technikreife der ENISA, [Eu15].
[51] Nur prozedurale und keine Maßnahmen der Technikarchitektur sind nach [RG20], 50 zu erwarten.
[52] Zu strukturellen Defiziten des behördlichen Vollzugs im Datenschutzrecht, [Po17], 216 f; [SgD17b].
[53] [La20], 5 ff.
[54] [Gr19], 112, zitiert [WDH16], 4; vgl. auch [Gr16], 299.

soll.[55] Die Aufsichtsbehörden sind nach Art. 58 Abs. 2 lit. i, Art. 83 Abs. 4 lit. a verpflichtet, Verstöße gegen Art. 25 Abs. 1 mit einer Geldbuße bis zu einer Höhe von 10 000 000€ oder zwei Prozent des weltweit erzielten Jahresumsatzes zu ahnden.[56] Die Bußgelder sind gem. Art. 83 Abs. 1 im Einzelfall wirksam, verhältnismäßig, abschreckend und anhand der Kriterien des Abs. 2 zu bemessen. Letzterer umfasst wiederum einen Positivanreiz für die datenschutzfreundliche Implementierung technisch-organisatorischer Maßnahmen, indem der „Grad der Verantwortung" für den Verstoß unter Berücksichtigung der getroffenen Maßnahmen einzubeziehen ist. Wurden geeignete Schutzmaßnahmen getroffen, wirkt sich dies positiv auf die Bußgeldbemessung aus.[57] Die Formulierung legt darüber hinaus nahe, dass eine besonders sorgfältige Vorsorge durch technisch-organisatorische Maßnahmen auch entsprechend mildernd zu berücksichtigen ist.[58] Aus den Kriterien der Bußgeldbemessung ergibt sich außerdem noch ein zusätzlicher Negativanreiz für eine Priorisierung kommerzieller Interessen zulasten geeigneter Datenschutzmaßnahmen. Denn sonstige erschwerende Umstände, vor allem finanzielle Vorteile aus der rechtswidrigen Verarbeitung sind gem. Art. 83 Abs. 2 lit. k ebenfalls bei der Bußgeldbemessung zu berücksichtigen.[59]

Der Negativanreiz möglicher Schadensersatzpflichten ergibt sich aus der Haftung für materielle und immaterielle Schäden, die sich als voraussehbare Folge einer verordnungswidrigen Verarbeitung,[60] d.h. im hier betrachteten Fall einer Verarbeitung personenbezogener Daten trotz unzureichender Maßnahmen nach Art. 25 Abs. 1,[61] ergeben (Art. 82 Abs. 1). Die Bemessung immaterieller Schäden ist bislang noch mit erheblicher Unsicherheit verbunden. Zwar formuliert EG 146 S. 3, dass der Schadensbegriff weit und den Zielen der Verordnung entsprechend auszulegen ist, woraus einhellig eine Abschreckungsfunktion des Schadensersatzes hergeleitet wird.[62] Uneinigkeit besteht aber über die Folgen dieser Abschreckungswirkung für die konkrete Bemessung immaterieller Schäden.[63] In der Literatur wird vorgeschlagen die kommerzielle Nutzbarkeit der rechtswidrig verarbeiteten Daten zu berücksichtigen, um die Wirksamkeit der präventiven Schadensfunktion abzusichern, und die Kriterien des Art. 83 Abs. 2 als Orientierung heranzuziehen.[64] Die Priorisierung kommerzieller Interessen zulasten der Umsetzung der Pflichten aus Art. 25 Abs. 1 würde sich dann auch auf die Schadensersatzhaftung zusätzlich negativ auswirken, wäre also mit einer weiteren Abschreckunsgwirkung verbunden. In der deutschen Rechtsprechungspraxis

[55] Allgemeiner zum verhaltenslenkenden Potential von Geldbußen, [Gr16], 290 ff.

[56] Aus dem Wortlaut des Art. 83 Abs. 4 „werden [...] verhängt" folgt eine gebundene Entscheidung, Boehm, [SHSgD19], Art. 83 Rn 15, Bergt, [KB20], Art. 83 Rn 30 ff.

[57] Hollaender, [WB20], Art. 83 Rn 36; zur Anreizwirkung siehe auch [RG20], 37 (56)

[58] Vgl. auch Boehm, [SHSgD19], Art. 83 Rn 28.

[59] Näher hierzu Bergt, [KB20], Art. 83 Rn 57.

[60] Näher hierzu Boehm, [SHSgD19], Art. 82 Rn 10, 14.

[61] Nach a.A. handelt es sich bei Art. 25 nur um eine Verfahrensregelung, deren Nichtbeachtung für die Rechtmäßigkeit der Verarbeitung unerheblich ist und keine Schadensersatzpflicht begründet, Nolte/Werkmeister, [Go18], Art. 25 DSGVO Rn 3, 34.

[62] M.w.N. Bergt,[KB20], Art. 82 Rn 17; [Ko21], 978 (979).

[63] Insbesondere über die Grenze zum „Strafschadensersatz", vgl. Boehm, [SHSgD19], Art. 82 Rn 27. Eine mögliche strafende Wirkung zu hoher Schadensersatzposten betonen [We19], 295 und [Wy19], 3266 f.

[64] Boehm, [SHSgD19], Art. 82 Rn 27; Quaas, [WB20], Art. 82 Rn 31.

wurde der immaterielle Schadensersatz bislang eher zurückhaltend bemessen.[65] Europaweit soll inzwischen eine steigende Tendenz zu beobachten sein. [66] Über die Auslegung von Art. 82, insbesondere über die Frage nach einer Erheblichkeitsschwelle, wird demnächst der EuGH entscheiden müssen.[67] Wie die erforderliche Konkretisierung der Grundsätze zur immateriellen Schadensbemessung auch ausfallen wird, die Schadensersatzhaftung ist eine mehr oder weniger gewichtige negative Konsequenz, die unmittelbar aus einer Datenverarbeitung ohne geeignete Schutzmaßnahmen gem. Art. 25 Abs. 1 folgen kann. Ob sie im konkreten Fall als Folge eines DSGVO-Verstoßes eintritt, hängt indessen auch von Faktoren aus der Betroffenensphäre, etwa der Kenntnis von und der Initiative zur Wahrnehmung von Schadensersatzansprüchen, der Beweislastverteilung und Beweismöglichkeiten sowie des zu erwartenden Kosten-Nutzen-Verhältnisses eines möglichen Prozesses ab. Während über Beweiserleichterungen oder sogar eine Beweislastumkehr zugunsten der Betroffenen Uneinigkeit besteht,[68] bezwecken die Erweiterungen der Vertretungs- und Verbandsklagerechte nach Art. 80 DSGVO zweifelsfrei eine Erleichterung der Klagemöglichkeiten für Betroffene[69] und werden zukünftig um die Möglichkeit kollektiver datenschutzrechtlicher Klagen aufgrund der kürzlich verabschiedeten EU-Verbandsklage-Richtlinie ergänzt werden.[70] Die praktische Relevanz der Schadensersatzhaftung für die Verantwortlichen könnte demnach durch erweiterte prozessuale Möglichkeiten datenschutzrechtlicher Massenverfahren und Sammelklagen weiter zunehmen.[71] Gerade eine datenschutzrechtlich unzureichende Technikgestaltung, die in der Regel größere Personengruppen, beispielsweise den gesamten Kundenstamm eines datenverarbeitenden Unternehmens, betreffen, eignen sich für die geschäftsmäßige Durchsetzung von Ersatzansprüchen sowie Massen- und Sammelverfahren.[72] Abseits der im Recht angelegten finanziellen Negativanreize treten zu erwartende Reputationsverluste, insbesondere bei öffentlichkeitswirksamen Prozessen, die eine Vielzahl an Personen betreffen, als zusätzlicher ökonomisch relevanter Kostenfaktor des DSGVO-Verstoßes hinzu.[73]

[65] [Kl20], 433; [Wy19], 3267 f; [Pa21a], 242 f, wobei die Arbeitsgerichtsbarkeit zur höheren Bußgeldbemessung tendiert, [Fu20], 565; [Ko21], 979 f; [Le21]; [Pa21a], 244.

[66] [Th20], 503; weniger deutlich bei der Rechtsprechungsauswertung anderer Mitgliedstaaten dagegen, [Pa21a], 244 f.

[67] Das BVerfG gab einer Verfassungsbeschwerde gegen das Urteil des AG Goslar, das einen Schadensersatzanspruch wegen Unerheblichkeit ablehnte, wegen einer Verletzung von Art. 101 Abs. 1 S.2 GG statt und verpflichtete das Gericht zur Vorlage beim EuGH, BVerfG Beschl. v. 14.01.2021 – 1 BvR 2853/19 = BeckRS 1962; dazu [Ko21], 978. Die Literatur spricht sich überwiegend gegen eine Bagatellgrenze aus, Quaas, [WB20], Art. 82 Rn 31; Bergt, [KB20], Art. 82 Rn 18a; Gola/Piltz, [Go18], Art. 82; Rn 13; a.A. Frenzel,[Pa21b], Art. 82 Rn 10; wohl auch [Wy19], 3265 (3266 ff); [Sp19], 476; differenzierend [Pa21a], 245 f.

[68] Jeweils m.w.N. für eine Beweislastumkehr, [Fu20], 565; dagegen [Wy19], 3268; [Wy21], 1191 f.

[69] Boehm,[SHSgD19], Art. 80 Rn.2.

[70] RL (EU) 2020/1828, `https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32020L1828&from=DE`; [Ue19], 702 f.

[71] Zu den Grenzen der Schadensersatzdurchsetzung über UwG und UKlaG, [Ue19], insbesondere bzgl. Art. 25 Abs.1, 694 (700); zur Konstellation einer datenschutzrechtlichen Musterfeststellungsklage, [GS19], a.A. [Sp19], 477; zur Verbandsklage-RL [Pa21a], 246 f.

[72] Vgl. zur Kommerzialisierung der Schadensersatzklagen in solchen Konstellationen, [Sp19]; [Wy21], 1190 f.

[73] vgl. [We19], 294; [GS19], 3417 f; bzgl. Bußgeldverfahren, [Gr16], 299 ff.

4.3 Zertifizierung als Positivanreiz

Eine wesentliche Erweiterung brachte die DSGVO für Möglichkeiten der sog. regulierten Selbstregulierung.[74] Neben der beschriebenen Konkretisierungsverantwortung der Verantwortlichen bezüglich ihrer eigenen Rechtspflichten, können sie sich freiwillig zur Einhaltung genehmigter Verhaltensregeln verpflichten (Art. 40 f) oder eine Zertifizierung (Art. 42 f) beantragen. Private Stellen werden dabei unter behördlicher Kontrolle in die Skalierung und Spezifizierung der Verordnungspflichten und in die Überprüfung ihrer Einhaltung eingebunden.[75] Für Unternehmen kann die Teilnahme an solchen Selbstregulierungsverfahren insbesondere vorteilhaft sein, um ein gewisses Maß an Rechtssicherheit zu erlangen,[76] und zumindest faktisch die Wahrscheinlichkeit einer behördlichen Überprüfung reduzieren.[77]

Aus Art. 25 Abs. 3 folgt ein unmittelbarer rechtlicher Vorteil der Zertifizierung, indem sie als Faktor zum Nachweis geeigneter Maßnahmen anerkannt wird.[78] Verarbeitungsvorgänge, nicht die Technikgestaltung als solche oder ein Produkt selbst,[79] müssen mindestens als „datenschutzkonform“ zertifiziert werden, während eine Zertifizierung als „datenschutzfreundlich“ im Sinne eines abgestuften Konzepts nach einheitlich festgelegten höheren Standards nicht vorgesehen ist.[80] Enthalten die Zertifizierungskriterien konkrete Anforderungen an Maßnahmen nach Art. 25 Abs. 1, kann die erfolgreiche Zertifizierung deren Geeignetheit implizieren. Sie darf allerdings nicht als "Freischein"missverstanden werden, die den Verantwortlichen von einer kontinuierlichen Prüfung des Risikos und der getroffenen Maßnahmen entbinden könnte oder vor einer Überprüfung durch die zuständige Aufsichtsbehörde schützen würde.[81] Der, wenn auch beschränkte, Anreiz der Nachweiserleichterung wird durch die Einbeziehung der Einhaltung von Zertifizierungskriterien bei der Bußgeldmessung gem. Art. 83 Abs. 2 lit. j ergänzt.

Von größerer Bedeutung für die unternehmerische Strategie dürften jedoch die potentiellen ökonomischen Vorteile einer Zertifizierung sein. Sie ermöglicht einen werbewirksamen Einsatz und damit eine Differenzierung datenschutzrechtlich geprüfter Angebote von solchen konkurrierender Markteilnehmer. Zertifikate und Gütesiegel können in einem entstehenden Wettbewerb datenschutzfreundlicher Technikgestaltung als vertrauenswürdiges Kommunikationsmittel gegenüber dem Verbraucher dienen und die Wettbewerbsfähigkeit

[74] [K6c], 448 (452); zum Konzept der regulierten Selbstregulierung,[Po17], 209 ff.
[75] Roßnagel, [SHSgD19], Art. 40 Rn 3; Art. 42 Rn 4; [Ka20], 1599 ff; bzgl. der Verhaltensregeln, [Re19], 305 f.
[76] EDSA, [ED], 8 ff; Scholz, [SHSgD19], Art. 42 Rn 5.
[77] Vgl. Scholz, [SHSgD19], Art. 42 Rn 33.
[78] Teilweise wird vertreten, dass dieser Vorteil auch für genehmigte Verhaltensregelungen gilt und es sich bei der ausschließlichen Nennung der Zertifizierung um ein Redaktionsversehen handelt,so Baumgartner, [Eh18], Art. 25 Rn 22; zurückhaltender, aber mit Verweis auf die zumindest praktische Nachweiserleichterung, Martini, [Pa21b], Art. 25 Rn 53a.
[79] Hansen, [SHSgD19], Art. 42 Rn 21 ff, 25 f.
[80] Solche höheren Standards können aber grundsätzlich im Rahmen der DSGVO-Zielvorgaben vorgesehen werden, [Ho19b], 219 ff.
[81] Hansen, [SHSgD19], Art. 25 Rn 58.

eines Unternehmens verbessern.[82] Ein ökonomischer Vorteil kann sich zudem bei der Vergabe öffentlicher Aufträge ergeben, für deren Ausschreibungen datenschutzfreundliche Technikgestaltung nach EG 78 S. 5 berücksichtigt werden sollten.[83]

5 Spieltheoretisches Modell

Die Wirksamkeit der rechtlichen Steuerungselemente Sanktionierung, Haftung und Zertifizierung bei deren Interaktion mit dem unternehmerischen Gewinnkalkül zur Umsetzung von Art. 25 Abs. 1 sollen durch nachfolgendes spieltheoretisches Modell beleuchtet werden. Grundsätzlich besteht jedoch eine Übertragbarkeit auf andere DSGVO-Verstöße. Die Spieltheorie ist eine formal mathematische Methodik zur Analyse von Entscheidungssituationen. Insbesondere eignen sich spieltheoretische Untersuchungen, um die Auswirkungen und Interdependenzen von Entscheidungen unterschiedlicher Akteure – also Entscheidungen mit strategischem Charakter - abzubilden.[84] Hierbei ist eine Entscheidung als eine bewusste Wahl zwischen unterschiedlichen Handlungsalternativen gemeint. Spieltheoretische Analysen befassen sich demnach mit interaktiven und strategischen Entscheidungssituationen, bei denen mindestens zwei Entscheider zwischen mindestens zwei möglichen Handlungsalternativen auswählen können.[85] Ein Entscheider muss aufgrund der Interdependenzen antizipieren, wie sich sein gegenüber verhalten wird, um zu einer optimalen Entscheidung zu finden.

Definition 1 (Spiel) *Gegeben sei eine Entscheidungssituation, in der n Spieler aufeinandertreffen. Jeder dieser Spieler sei durch die Menge S möglicher Strategien (als dem vollständigen Plan über alle Aktionen innerhalb einer Entscheidungssituation) sowie durch den Nutzen u des Entscheidungsträgers, welche abhängig von der getroffenen Strategie eine Auszahlung wiedergibt, beschreibbar. Auf diese Weise ist ein Spiel* $\Gamma(N, S, u)$ *durch die Spieler, ihre Strategien und ihre Nutzen eindeutig beschrieben.*

5.1 Basisspiel

Ein Unternehmen (F) ist im gegebenen Anwendungsfall in ein Simultanspiel[86] mit der Datenaufsichtsbehörde bzw. ihrem staatlichen Rechtsträger (Land, Bund) (S) involviert. Das Unternehmen kann dabei entscheiden wie es die Spielräume bei der Umsetzung technisch implementierten Datenschutzes nutzt. Die Datenschutzaufsichtsbehörde determiniert die Kontrollintensität (z.B. Häufigkeit der Kontrollen) im Rahmen der ihr im Bundes- oder

[82] Vgl. EG 100; Scholz, [SHSgD19], Art. 42 Rn 4; Bergt/Pesch, [KB20], Art. 42 Rn 1 ff; allgemeiner [Ho19b], 40 f; [Ri13], 250; [RBW16], 248 f.

[83] Siehe auch [RG20], 54.

[84] [BW20].

[85] [BW20].

[86] Vereinfacht gesagt, treffen die Spieler in einem Simultanspiel ihre Entscheidungen zeitgleich. Somit sind die Entscheidungen im Moment ihrer Entscheidung unbeobachtbar voneinander, [BW20].

Landeshaushalt zur Verfügung gestellten Ressourcen. Der Unternehmensgewinn setzt sich aus einem vom Datenschutzniveau unabhängigen Betriebsergebnis (g_0), einem Zusatzgewinn durch nicht legitimierte Datennutzung im Umfang von x ($a \cdot x$), Kosten für technisch wirksamen Datenschutz ($c_F \cdot (1 - x)$) sowie der zu erwartenden Strafe in Höhe von $q \cdot (S + H) \cdot x$ (Erwartungswert der Sanktionierung, Schadensersatzpflichten) zusammen. Die variable q beschreibt die Kontrollwahrscheinlichkeit, S die Sanktion sowie H den Erwartungswert der Schadensersatzpflichten. Letztere fallen dabei nur dann an, wenn eine Verletzung der DSGVO nachgewiesen wurde, d.h. diese können nur durch eine (erfolgreiche) Kontrolle entstehen. Aus der Nutzenfunktion lässt sich die optimale Datennutzungsstrategie x^* der Firma ableiten.

$$\Pi_F = g_0 + (a - q \cdot (S + H)) \cdot x - \frac{c_F \cdot (1 - x)^2}{2} \Rightarrow x^* = \frac{a + c_F - q \cdot (S + H)}{c_F} \tag{1}$$

Ein Unternehmen wird also weitreichender (personenbezogene) Daten verarbeiten, je höher der Nutzen daraus, je höher die Kosten der Implementierung datenschutzsteigernder Technologien und je kleiner die erwartete Strafe (Schadensersatzpflichten und Bußgelder). Die Behörde hat das Ziel sicherzustellen, dass sich das Unternehmen datenschutzkonform ($x = 0$) verhält. Es soll somit garantiert sein, dass vom Unternehmen geeignete Maßnahmen der Technikgestaltung getroffen wurden. Dabei spiegelt der Präferenzfaktor b wider, welchen Wert die Behörde einer wirksamen Durchsetzung des Datenschutzes durch Technikgestaltung beimisst. c_S seien die Kosten der Kontrolle. Es wird angenommen, dass die Kontrollkosten des Staates überproportional in der Kontrollintensität ansteigen, was in Opportunitätskosten der Behörde sowie ihrem begrenzten Budget begründet liegt. Deckt die Behörde einen Verstoß gegen Art. 25 Abs. 1 DSGVO auf, so entsteht ihr ein Nutzen in Höhe von V.

$$\Pi_S = b \cdot (1 - x) + x \cdot q \cdot V - \frac{c_A \cdot q^2}{2} \Rightarrow q^* = \frac{V \cdot x}{c_S} \tag{2}$$

Analog zum Unternehmen lässt sich für die Behörde die optimale Kontrollintensität q^* ableiten. Die Behörde wählt eine umso höhere Kontrollintensität, je höher der Nutzen eines entdeckten Regelverstoßes, je höher die (erwartete) Intensität des Datenmissbrauchs und je niedriger ihre Kontrollkosten sind. In einem Simultanspiel ergibt sich das sogenannte Nash-Gleichgewicht (NGG),[87] das die wechselseitig optimalen Strategien bestimmt, damit wie in Formel 3 dargestellt.

$$x^*_{NGG} = \frac{(a + c_F) \cdot cS}{c_F \cdot c_S + V \cdot (H + S)}; q^*_{NGG} = \frac{(a + c_F) \cdot V}{c_F \cdot c_S + V \cdot (H + S)} \tag{3}$$

Die Parameter a und c_F treiben sowohl x als auch q in die Höhe. Darüber hinaus gilt, je höher die Kontrollkosten, umso größer x. Der Zusammenhang mit der Höhe des Nutzens

[87] Zum Lösungskonzept des NGG siehe [BW20].

eines entdeckten Regelverstoßes kann je nach Parameterkonstellation sowohl positiv als auch negativ sein. Abbildung 1(a) stellt die sogenannten Reaktionskurven der beiden Parteien dar. Diese stellen die jeweils optimale Strategie eines Spielers in Abhängigkeit der Strategie des anderen Spielers grafisch dar. Der Schnittpunkt der Kurven entspricht somit dem NGG des Spiels. Wie gezeigt, steigt die Kontrollintensität q, je höher die rechtswidrige Datenverarbeitung und umgekehrt, d.h. je höher die Kontrollintensität desto niedriger die DSGVO-Verstöße.

5.2 Unvollkommene Information

Wir unterscheiden nun zwischen zwei Typen von Firmen: Eine (+)Firma, die einen geringen Nutzen aus intensiver (bzw. missbräuchlicher) Datenverarbeitung zieht (bspw. hohe Sensitivität der Kunden und/oder niedriger Informationswert, niedriger Wert für a), und eine (-)Firma, die einen hohen Gewinn durch Datenverarbeitung erzielt (bspw. niedrige Sensitivität der Kunden, hoher Informationswert, hoher Wert für a). Die (-)Firma wird somit einen höheren x-Wert wählen als die (+)Firma. Die Behörde kann vor der Kontrolle aber nicht zwischen den Firmen unterscheiden und wählt daher eine mittlere Kontrollintensität q. Die optimale Kontrollintensität ist nun auch abhängig von den Erwartungen der Behörde, bei einer zufälligen Kontrolle eine (+)Firma oder eine (-)Firma anzutreffen (abhängig von den Wahrscheinlichkeiten p respektive $1-p$).

Die generelle Struktur der Nutzenfunktion der Unternehmen bleibt unverändert, diese unterscheiden sich nur in der Höhe von a. Die Reaktionsfunktionen ergeben sich wie in Abbildung 1(b) dargestellt. Die Behörde orientiert sich an der mittleren Reaktionsfunktion der beiden Firmen-Typen und bestimmt so ihre optimale Kontrollintensität q. Die Firmen wiederum passen sich optimal an dieses mittlere Kontrollniveau an, woraus sich das NGG bei unvollkommener Information, das sog. Bayes-Nash-Gleichgewicht (BNGG),[88] ergibt.

$$q^* = \frac{(a_- + c_F - (a_- + a_+)p)S}{c_F c_S + S(H+S)}; x_+^* = \frac{c_F(a_+ + c_F)c_S + (a_- - a_+)(p-1)V(H+S)}{c_F(c_F c_S + V(H+S))}$$
$$x_-^* = \frac{c_F(a_- + c_F)c_S + (a_- - a_+)pV(H+S)}{c_F(c_F c_S + V(H+S))} \quad (4)$$

Im BNGG kontrolliert die Behörde also beide Firmen mit der Kontrollwahrscheinlichkeit q^*. Die (+)-Firma wählt das (niedrigere) Datenmissbrauchslevel x_+^* und die (-) Firma wählt das (höhere) Datenmissbrauchslevel x_-^*. Die beiden schwarzen Punkte in der Grafik geben das BNGG an (optimale Reaktion von jedem Firmentypen auf die durchschnittliche Erwartung der Behörde). Die beiden grünen Punkte zeigen, welche NGG zustande kämen, wenn die Behörde beide Firmen (perfekt) unterscheiden könnte. An der Grafik wird erkennbar, dass die fehlende Unterscheidbarkeit der beiden Firmentypen durch die Behörde zu einem

[88] Zum Lösungskonzept des BNGG siehe [BW20].

hohen Effizienzverlust führt: Da die Behörde eine mittlere Kontrollintensität wählt, wird die (+)Firma zu stark und die (-)Firma vergleichsweise zu wenig kontrolliert. Genau an diesem Problem setzt der Gedanke der Zertifizierung an.

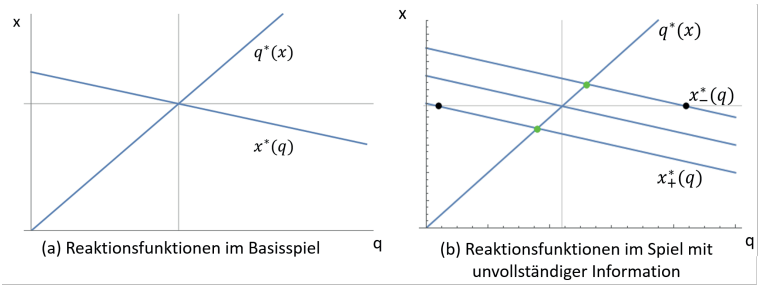

Abb. 1: Reaktionskurven der Behörde und des Unternehmens in beiden Spielen

5.3 Möglichkeiten der Zertifizierung und das Potential für die Herausbildung eines Marktes für datenschutzfreundliche Produkte

In der vorangegangenen spieltheoretischen Modellierung wurde aufgezeigt, dass allein die Wirkung der sanktionierenden Maßnahmen sowie die Haftungsansprüche dafür sorgen können, dass es für einige Unternehmen optimal ist geeignete technische Maßnahmen zum Schutz der Daten zu implementieren. Aufgrund der Intranzparenz kann die behördliche Kontrolle die Firmen jedoch nicht zielgerichtet adressieren, was zu Effizienzverlusten und einem niedrigeren Datenschutzniveau führt. Die Zertifizierung bietet nun eine potentielle Lösung dieses Problems: Da es der (+)Firma leichter fällt als der (-)Firma, die Anforderungen an die Zertifizierung zu erbringen, können die beiden Firmen-Typen für die Behörde unterscheidbar werden. Der Vorteil für die (+)Firma liegt auf der Hand: Als zertifizierte Firma hat sie fortan mit einer niedrigeren Kontrollintensität zu rechnen, da sich die Behörde vor allem auf (-)Firmen konzentrieren kann. Darüber hinaus bietet die Aussicht auf diese günstige Position der (+)Firma weitere Anreize, in datenschutzfreundliche Verarbeitungsvorgänge und Technologien zu investieren. Dies wiederum würde Herstellern datenschutzfreundlicher Produkte den Anreiz geben, ihr Angebot auszubauen. Gleichzeitig hätte die zertifizierte (+)Firma die Chance, einen Standard für datenschutzkonforme Technikgestaltung zu setzen. Um jedoch sicherzustellen, dass die Zertifizierung ein glaubwürdiges Signal für alle Marktteilnehmer darstellt, müssen mehrere Voraussetzungen erfüllt sein. Zunächst muss sich für die betreffenden Unternehmen ein klarer Vorteil durch die Zertifizierung ergeben. Neben der bereits angesprochenen niedrigeren Kontrolle durch die Behörde kann auch die Wirkung auf die Kunden von Relevanz sein. Eine zertifizierte (+)Firma kann die Zahlungsbereitschaft oder die Loyalität der Kunden erhöhen, wodurch sich ihre Position am Markt verbessert. Inwiefern diese Marktvorteile für datenschutzfreundliche Produkte

jedoch so ausgeprägt sind, ist dabei Thema teils kontrovers geführter Diskussionen.[89] Die aus spieltheoretischer Sicht größere Hürde liegt jedoch bei der (-)Firma. Je größer der Vorteil einer Zertifizierung, desto eher wird auch die (-)Firma bemüht sein, zumindest einmalig aus taktischen Erwägungen heraus die Anforderungen an die Zertifizierung zu erfüllen, um anschließend wieder der opportunistischen Datennutzungsstrategie zu folgen. Die (-)Firma muss also entweder durch zu große Hürden (etwa der Pflicht zur regelmäßigen Erneuerung des Zertifikats oder adäquat hohe Kontrollintensität des ausstellenden Instituts) davon abgehalten werden, die Zertifizierung aus rein taktischen Gründen anzustreben oder es gelingt, mithilfe der (+)Firmen eine Marktdynamik in Richtung eines neuen Datenschutz-Standards anzustoßen, den auch die (-)Firma mitgehen muss. Hierzu könnte eine vertiefte Kooperation der Behörde mit zertifizierten (+)Firmen der erste Schritt sein.

6 Fazit und Ausblick

Für die datenschutzrechtliche risikobasierte Regulierung im Bereich der Technikgestaltung sind klare abschreckende Wirkungen durch Bußgeld- und Haftungsrisiken als Negativanreize grundsätzlich geeignet das Verhalten datenverarbeitender Unternehmen innerhalb ihres Umsetzungsspielraums zu lenken. Die Lenkungswirkung hängt maßgeblich von der Aufdeckungswahrscheinlichkeit eines Verstoßes, d.h. mittelbar von der behördlichen Kontrollintensität, sowie der Höhe der Bußgelder und Schadensersatzposten ab. Die hinreichende Ausstattung der Aufsichtsbehörden ist demnach zentral für die Wirksamkeit der Negativanreize. Auch wenn Aufgaben und Kompetenzen der Aufsichtsbehörden unberührt bleiben, können sichere Zertifizierungsprogramme außerdem zu einer effizienten und ressourcenschonenden behördlichen Praxis beitragen. Ökonomische Anreize einer Zertifizierung können geeignet sein datenschutzfreundliche Technikgestaltung zu fördern, wenn die Zerifizierung ihrerseits eine sichere Erkennbarkeit datenschutzkonformer und datenschutzfreundlicher Technikgestaltung für den Verbraucher ermöglicht. Die Aussagekraft von Zertifikaten nach dem gegenwärtigen Konzept ist angesichts abstrakter Vorgaben, mangelnder dauerhafter Überprüfung und Anpassung[90] und der Heterogenität nebeneinander bestehender Zertifikate- und Zertifizierungsverfahren eingeschränkt.[91] Eine rechtssichere graduelle Abstufung von Zertifikaten nach der Datenschutzfreundlichkeit von Verarbeitungen böte eine optimale Entscheidungsgrundlage für Verbraucher und sollte für eine innovationsfördernde rechtliche Regulierung, die mit Marktanreizen arbeitet, bedacht werden. Hohe Standards, eine sichere Überprüfung der Zertifizierungsverfahren und Konzepte der "dynamischen Zertifzierung"[92] sollten zudem als zentrale Faktoren für die Vermeidung taktischer Zertifizierungen, die die Glaubwürdigkeit von Zertifikaten beeinträchtigen und damit ihre Anreizwirkung für datenschutzfreundliche Technikgestaltung konterkarieren würden, sichergestellt werden.

[89] [BKP12], [GA07], [AJL13].
[90] [Ho19b], 290 ff.
[91] [RBW16], 250 ff; [RG20], 53 f.
[92] [Ho19b]

Literaturverzeichnis

[Ad20] Adam, Simon: Daten als Rechtsobjekte. NJW, 73:2063–2068, 2020.

[AJL13] Acquisti, Alessandro; John, Leslie K; Loewenstein, George: What is privacy worth? The Journal of Legal Studies, 42(2):249–274, 2013.

[Ar] Guidelines in Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679 (WP 248 rev. 01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, Stand: 30.04.21.

[Ar14] Statement on the role of a risk-baed approach in data protection legal frameworks (WP 218). http://www.privacy-regulation.eu/privazyplan/materialien/eu-artikel-29-gruppe-workingpaper/wp218%20EN%20Role%20of%20risk-based%20approach%20in%20data%20protection%20legal%20frameworks.pdf, Stand: 30.04.21.

[BKP12] Beresford, Alastair R; Kübler, Dorothea; Preibusch, Sören: Unwillingness to pay for privacy: A field experiment. Economics letters, 117(1):25–27, 2012.

[Br10] Broemel, Roland: Strategisches Verhalten in der Regulierung. Mohr Siebeck, 2010.

[BTH14] Birnhack, Michael; Toch, Erin; Hadar, Irit: Privacy Mindset, Technology Mindset. Jurimetrics, 55:55–114, 2014.

[Bu] Rede der Bundeskanzlerin Dr. Angela Merkel beim Jahrestreffen des World Economics Forum am 24. Januar 2018 in Davos. https://www.bundesregierung.de/resource/blob/975954/775758/16212f149c37f3bf3641872d146533ae/10-1-bkin-davos-data.pdf?download=1, Stand: 30.04.21.

[Bu20] Buss, Sebastian: Privacy by Design und Software. Berücksichtigung datenschutzfreundlicher Anforderungen bei der Softwarebeschaffung. CR, 35:1–6, 2020.

[BW20] Bartholomae, Florian; Wiens, Marcus: Spieltheorie- Ein anwendungsorientiertes Lehrbuch. Springer Gabler, 2020.

[By17] Bygrave, Lee A.: Data Protection by Design and Default: Deciphering the EU's Legislative Requiremenrs. Oslo Law Review, 4:105–120, 2017.

[Ce] A Risk-based Approach to Privacy: Improving Effectiveness in Practice. https://www.huntonak.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf, Stand:30.04.21.

[Da19] Gutachten der Datenethikkommission der Bundesregierung. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, Stand:30.04.21.

[Dr17] Drexl, Josef: Neue Regeln für die Europäische Datenwirtschaft. NZKart, 5:339–344, 2017.

[DS] Standard-Datenschutzmodell, Version 2.0b. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html, Stand: 30.04.21.

[ED] Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Veordnung (EU)2016/679, Fassung 2.0. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_de.pdf, Stand: 30.04.21.

[Eh18] Ehmann, Eugen und Selmayr, Martin: DS-GVO. Datenschutz-Grundverordnung.Kommentar. C.H.Beck, 2. Auflage, 2018.

[EUa] Mitteilung der Kommission an das Europäische Parlament und den Rat, COM(2020) 264 final. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0264&from=EN, Stand: 30.04.21.

[Eub] Leitlinien 4/2019 zu Art. 25, Version 2. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf, Stand: 30.04.21.

[Eu15] Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. https://www.enisa.europa.eu/publications/pets/at_download/fullReport, Stand: 30.04.21.

[Fr] Merkel: Daten sind die Rohstoffe des 21. Jahrhunderts. https://www.faz.net/aktuell/wirtschaft/cebit/angela-merkel-fordert-mehr-modernisierte-digitale-technologien-14120493.html, Stand:30.04.21.

[Fu20] Fuhlrott, Michael und Oltmanns, Sönke: Immaterieller Schadensersatz wegen Datenschutzverstoß: Höhe und Bemessungsfaktoren. ArbAktuell, 12:565–567, 2020.

[GA07] Grossklags, Jens; Acquisti, Alessandro: When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In: WEIS. 2007.

[Go18] Gola, Peter: Datenschutz-Grundverordnung. VO (EU) 2016/679. Kommentar. C.H.Beck, 2. Auflage, 2018.

[Gr16] Grant, Hazel und Crowther, Hannah: How Effective are Fines in Enforcing Privacy? In (Wright, David und De Hert, Paul, Hrsg.): Enforcing Privacy. Regulatory, Legal and Technology Approaches. Springer International, S. 287–305, 2016.

[Gr19] Greze, Benjamin: The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives. International Data Privacy Law, 9:109–128, 2019.

[GS19] Geissler, Dennis; Stroebel, Lukas: Datenschutzrechtliche Schadensersatzansprüche im Musterfeststellungsverfahren. NJW, 72(47):3414–3418, 2019.

[Hä16] Härting, Niko: Digital Goods und Datenschutz-Daten sparen oder monetarisieren? CR, 32(11):735, 2016.

[HG16] Heuberger-Götsch, Olivier: Der Wert von Daten aus juristischer Sicht am Beispiel des Profiling. In: Big Data, S. 83–105. Springer, 2016.

[Ho19a] Hoeren, Thomas: Datenbesitz statt Dateneigentum. MMR, 22:5–8, 2019.

[Ho19b] Hofmann, Johanna M.: Dynamische Zertifzierung. Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computing. Nomos, 2019.

[K6a] Körber, Torsten: Ïst Wissen Marktmacht? Überlegungen zum Verhältnis von Datenschutz, "Datenmachtünd Kartellrecht - Teil 2. NZKart, 7:348–356, 2016.

[K6b] Körber, Torsten: „Ist Wissen Marktmacht?“ Ueberlegungen zum Verhaeltnis von Datenschutz, „Datenmacht“ und Kartellrecht – Teil 1. NZKart, 4:303–310, 2016.

[K6c] Kühling, Jürgen und Martini, Mario: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW, 27:448–454, 2016.

[K0] Kühling, Jürgen und Sackmann, Florian: Irrweg "Dateneigentum". ZD, 10:24–30, 2020.

[Ka20] Kaminski, Margot E.: Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability. California Law Review, 92:1529–1616, 2020.

[KB20] Kühling, Jürgen; Buchner, Benedikt: Datenschutz-Grundverordnung. BDSG. C.H.Beck, 2020.

[Ke16] Kerber, Wolfgang: Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection. GRUR Int., 65:639–647, 2016.

[Kl20] Klein, Susanne: Immaterieller Schadensersatz nach der DS-GVO. GRUR-Prax, 12:433–435, 2020.

[Kl21] Klingbeil, Thilo und Kohm, Simon: Datenschutzfreundliche Technikgestaltung und ihre vertraglichen Implikationen. MMR, 24:3–8, 2021.

[Ko21] Korch, Stefan: Schadensersatz für Datenschutzverstöße. NJW, 12:978–981, 2021.

[La20] Latzel, Clemens: Verhaltenssteuerung, Recht und Privatautonomie. Springer, 2020.

[Le21] Leibold, Kevin: Gerichtliche Entscheidungen zum Schadensersatz nach Art. 82 Abs.1 DSGVO - ein Fall für den EuGH. ZD-Aktuell, 11:05043, 2021.

[Pa21a] Paal, Boris und Aliprandi, Claudio: Immaterieller Schadensersatz bei Datenschutzverstößen. ZD, 11(5):241–247, 2021.

[Pa21b] Paal, Boris und Pauly, Daniel: Datenschutz-Grundveordnung. Bundesdatenschutzgesetz. C.H.Beck, 3. Auflage, 2021.

[Po17] Poll, Jens: Datenschutz in und durch Unternehmensgruppen im deutschen Datenschutzrecht. Nomos, 2017.

[Po19] Podszun, Rupprecht und Kersting, Christian: Modernisierung des Wettbewerbsrechts und Digitalisierung. NJOZ, 19:321–325, 2019.

[Po20] Podszun, Rupprecht: Der Verbraucher als Marktakteur:Kartellrecht und Datenschutz in der "FacebookEntscheidung des BGH. GRUR, 122:1268–1276, 2020.

[Qu17] Quelle, Claudia: The ‘risk revolution’ in EU data protection law: We can’t have our cake and eat it, too. In (Leenes, R.; van Brakel, R.; Gutwirth, S.; De Hert, P., Hrsg.): Data Protection and Privacy: The Age of Intelligent Machines. Tilburg Law School Legal Studies Research Paper Series, 2017.

[Qu18] Quelle, Claudia: Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach. European Journal of Risk Regulation, 9:502–526, 2018.

[RBW16] Rodrigues, Rowena; Barnand-Wills, Davis: The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. International Review of Law, Computers and Technology, 30:248–270, 2016.

[Re19] Reifert, Natascha: Codes of Conducts nach der DSGVO. ZD, 9:305–310, 2019.

[RG20] Rubinstein, Ira; Good, Nathaniel: The trouble with Article 25 (and how to fix it): The future of data protection by desgin and default. International Data Privacy Law, 10:37–54, 2020.

[RGR18] Reinsel, David; Gantz, John; Rydning, John: The Digitilazation af the World. From Edge to Core. IDC White Paper, 2018.

[Ri13] Richter, Frederik: Die Stiftung Datenschutz als chancenreiche Ergänzung. ZD, 3:249–250, 2013.

[Ro21] Roßnagel, Alexander: Die Evaluaition der Datenschutz-Grundverordnung. MMR, 24:657–661, 2021.

[Sc17] Schneider, Jens-Peter: Innovationsoffene Regulierung datenbasierter Dienste in der Informationsgesellschaft. Datenschutz, Regulierung, Wettbewerb. In (Körber, Torsten und Kühling, Juergen, Hrsg.): Regulierung - Wettbewerb - Innovation, S. 113–141. Nomos, 2017.

[Sc19] Schröder, Markus: Der risikobasierte Ansatz in der DS-GVO. ZD, 9:503–506, 2019.

[SgD17a] Spiecker gen. Döhmann, Indra: Big und Smart Data: Zweckbindung zwecklos? Spektrum der Wissenschaft, 1.17:56–62, 2017.

[SgD17b] Spiecker gen. Döhmann, Indra: Stichwort Datenschutz. In: Staatslexikon:Recht - Wirtschaft - Gesellschaft, Jgg. 1. Goerres-Gesellschaft zur Pflege der Wissenschaft, 2017.

[SHSgD19] Simitis, Spiros; Hornung, Gerrit; Spiecker gen. Doehmann, Indra: Datenschutzrecht. DSGVO mit BDSG. Nomos, 2019.

[Sp19] Spittka, Jan: Die Kommerzialisierung von Schadensersatz unter der DSGVO. GRUR-Prax, 11(21):475–477, 2019.

[SS19] Spindler, Gerald; Sein, Karin: Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen. MMR, 22:415–420, 2019.

[St20] Stromberg, Sabrina: Empfehlungen der Datenethikkommission: Datenschutz "by designünd "by default". ZD - Aktuell, 10:04397, 2020.

[Sy18] Sydow, Gernot: Europäische Datenschutz-Grundverordnung. Nomos, 2.auflage. Auflage, 2018.

[Th16] Thode, Jan-Christoph: Die neuen Compliance- Pflichten nach der Datenschutz-Grundveordnung. CR, 31:714–721, 2016.

[Th20] Thiel, Barabara und Wybitul, Tim: Bußgelder wegen Datenschutzverstößen - aus Sicht von Aufsichtsbehörden und Unternehmen. ZD, 10:3–7, 2020.

[Ue19] Uebele, Fabian: Datenschutz vor Zivilgerichten. GRUR, 121(7):694–703, 2019.

[Un] Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen. https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_18_Risiko.pdf, Stand: 30.04.21.

[Ve18] Veerpalu, Anne: Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De VoogD and Hedqvist. Baltic Jornal of Law and Politics, 11:63–94, 2018.

[WB20] Wolff, Amadeus; Brink, Stefan: BeckOK Datenschutzrecht. C.H.Beck, 35. Auflage, 2020.

[WDH16] Wright, David; De Hert, Paul: Introduction to Enforcing Privacy. In (Wright, David; De Hert, Paul, Hrsg.): Enforcing Privacy. Regulatory, Legal and Technological Approaches. Springer International, S. 1–5, 2016.

[We19] Wenzel, Michael und Wybitul, Tim: Vermeidung hoher DS-GVO-Bußgelder und Kooperation mit Datenschutzbehörden. ZD, 9:290–295, 2019.

[Wy19] Wybitul, Tim: Immaterieller Schadensersatz wegen Datenschutzverstößen – Erste Rechtsprechung der Instanzgerichte. NJW, 9:3265–3269, 2019.

[Wy21] Wybitul, Tim: Verteidigung gegen Schadensersatzklagen wegen Datenschutzverstößen. NJW, 74(17):1190–1194, 2021.

[Za17] Zarsky, Tal Z.: Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Review, 47:995–1018, 2017.

[Ze15] Zech, Herbert: ̈Industrie 4.0 Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. GRUR, 117:1151–1160, 2015.

[Zu15] Zuboff, Shoshana: Big other: surveillance capitalism and the prospects of an information civilization. JIT, 30(1):75–89, 2015.