MAX VON GRAFENSTEIN, FRANK PALLAS, JÖRG POHLE

Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1 DS-GVO

Methodische Überlegungen zur Feststellung und Durchsetzung des Wirksamkeits-Erfordernisses am Beispiel von Cookie-Bannern

HIIG DISCUSSION PAPER SERIES 2021-05

ABSTRACT

Mit dem Ansatz des Datenschutzes durch Technikgestaltung in Art. 25 Abs. 1 DS-GVO hat der EU-Gesetzgeber einen innovativen Ansatz, der lange eher ein Schattendasein führte, neu gefasst und signifikant gestärkt. Danach muss der Verantwortliche die rechtlichen Anforderungen der DS-GVO so in das technisch-organisatorische Design seiner Verarbeitungsprozesse implementieren, dass sie die Betroffenen wirksam vor den Risiken der Datenverarbeitung für ihre Grundrechtsausübung schützen. Damit stellt Art. 25 Abs. 1 DS-GVO eine Schlüsselnorm dar, die die Kluft zwischen rechtlichem Sollen und der organisatorisch-technisch-ökonomischen Realität überwinden helfen soll. In der Realität scheint die (Vollzugs-)Praxis jedoch einen weiten Bogen um die Norm zu machen, was an den methodischen Unklarheiten liegen mag. Das vorliegende Kurzpapier fasst daher den aktuellen Stand zur Prüfmethodik von Art. 25 Abs. 1 DS-GVO zusammen und versucht die Auswirkungen am Beispiel (wirksamer bzw. unwirksamer) Cookie-Banner zu veranschaulichen. Das Kurzpapier bildete damit die Grundlage für einen Praxisworkshop, in dessen Rahmen methodische Rückfragen sowie mögliche nächste Schritte zur Durchsetzung wirksamer Transparenz- und Interventionsmaßnahmen in der Praxis diskutieren wurden.

STICHWÖRTER

Datenschutz durch Technikgestaltung, Data Protection by Design, Privacy by Design, EU Datenschutz-Grundverordnung (DSGVO), Stand der Technik, State of the Art, Wirksamkeit, Transparenz, Betroffenenrechte, Cookie-Banner

ZITATION

Grafenstein, M. v., Pallas, F. & Pohle, J. (2021). Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1 DS-GVO. HIIG Discussion Paper Series 2021-05. 6 pages. https://doi.org/10.5281/zenodo.6325328.

LIZENZ

AUTORENINFO / INSTITUTION / FÖRDERUNG ETC.

Max von Grafenstein, Einstein Center Digital Future (Universität der Künste), Alexander von Humboldt Institute für Internet und Gesellschaft; Frank Pallas, Technische Universität Berlin; Jörg Pohle, Alexander von Humboldt Institute für Internet und Gesellschaft

Der Beitrag gibt einzig die persönliche Auffassung der Autoren wieder. Alle Autoren erklären, dass sie keine Interessenkonflikte haben.

CONTENTS/ INHALT

1 AUSGANGSLAGE: DIE ZURÜCKHALTENDE ANWENDUNG VON ART. 25 ABS. 1 DS-GVO IN DER (VOLLZUGS-)PRAXIS

Mit dem Ansatz des Datenschutzes durch Technikgestaltung in Art. 25 Abs. 1 DS-GVO hat der EU-Gesetzgeber einen innovativen Ansatz, der lange eher ein Schattendasein führte, neu gefasst und signifikant gestärkt.[1] Danach muss der Verantwortliche – kurz gesagt – die rechtlichen Anforderungen der DS-GVO so in das technisch-organisatorische Design seiner Verarbeitungsprozesse implementieren, dass sie die Betroffenen wirksam vor den Risiken der Datenverarbeitung für ihre Grundrechtsausübung schützen. Bei der Auswahl und Implementierung der Schutzmaßnahmen muss der Verantwortliche den sog. Stand der Technik sowie den Implementierungsaufwand berücksichtigen.[2] Insbesondere die Berücksichtigung des Stands der Technik verspricht, Marktdynamiken zur ständigen Fortentwicklung wirksamer Schutzmaßnahmen zu entfalten.[3]

Damit stellt Art. 25 Abs. 1 DS-GVO eine Schlüsselnorm dar, die die Kluft zwischen rechtlichem Sollen und der organisatorisch-technisch-ökonomischen Realität überwinden helfen soll. In der Realität scheint die (Vollzugs-)Praxis jedoch einen weiten Bogen um die Norm zu machen. Dies mag an den methodischen Unklarheiten liegen, die bisher mit der Normanwendung verbunden waren.[4] Das vorliegende Kurzpapier fasst daher den aktuellen Stand zur Prüfmethodik von Art. 25 Abs. 1 DS-GVO zusammen und versucht die Auswirkungen am Beispiel (wirksamer bzw. unwirksamer) Cookie-Banner zu veranschaulichen. Das Kurzpapier soll damit die Grundlage für einen Praxisworkshop bilden, in dessen Rahmen wir methodische Rückfragen sowie mögliche nächste Schritte zur Durchsetzung wirksamer Transparenz- und Interventionsmaßnahmen in der Praxis diskutieren möchten.

2 PRÜFMETHODIK VON ART. 25 ABS. 1 DS-GVO

Trotz der Komplexität von Art. 25 Abs. 1 DS-GVO sowohl in sprachlicher als auch in regulatorischer Hinsicht lässt sich zumindest folgende grundsätzliche Prüfstruktur aus dem Wortlaut und darauf aufbauenden Debatten in der Literatur ableiten. Danach verlangt die Vorschrift

(a) als Ergebnis einen wirksamen Schutz gegen die Risiken der Datenverarbeitung für die Grundrechte der betroffenen Person durch

(b) die Umsetzung der Verarbeitungsgrundsätze (Art. 5 DS-GVO) sowie weiterer konkretisierender Rechtsvorschriften (insb. Art. 6 bis 22 DS-GVO) in

(c) das technische und organisatorische Design der Datenverarbeitung,

---

[1] J. Pohle (2015), 'Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens', 2 FlfF-Kommunikation 32, pp. 41-44.
[2] F. Pallas (2018), Datenschutz in Zeiten alles durchdringender Vernetzung: Herausforderungen für das Zusammenspiel von Technik und Regulierung, in: Die Fortentwicklung des Datenschutzes (Hrsg. A. Roßnagel, M. Friedewald, M. Hansen), Springer Vieweg.
[3] Nachweise bei M. v. Grafenstein (in publishing, expected in 2022). Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design. In González-Fuster, G., van Brakel, R., & P. De Hert, Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, 1st Ed.. Cheltenham: Edward Elgar Publishing, preprint online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990.
[4] Siehe etwa L. A. Bygrave, 'Data protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 OLR 105.

(d) unter Berücksichtigung des Stand der Technik und des Aufwands.

Dabei ist mittlerweile insbesondere geklärt, wie die Risiken methodisch zu evaluieren sind.[5] Methodisch unbeantwortet bleibt jedoch die Frage, wie die Wirksamkeit des implementierten Schutzes gemessen und damit in der (Vollzugs-)Praxis gewährleistet werden kann.[6]

3 WIE KANN DIE WIRKSAMKEIT DER SCHUTZMAßNAHMEN METHODISCH FESTGESTELLT WERDEN?

Nach unserer Einschätzung stellt das Wirksamkeitserfordernis die größte Herausforderung für den Vollzug von Art. 25 Abs. 1 DS-GVO in der Praxis dar, da sich die Wirksamkeit von Schutzmaßnahmen oftmals nur mit nicht-rechtlichen Methoden aus anderen (nicht-rechtlichen) Disziplinen überprüfen lässt. Das ist eine Herausforderung für die Prüfpraxis zumindest insoweit, als diese meist von Jurist*innen angeleitet wird. Gleichzeitig lassen sich die Datenschutzjurist*innen auch nicht durch Vertreter*innen der jeweils anderen Disziplin ersetzen. Denn ob eine zum Beispiel mit mathematisch-statistischen oder empirischen Methoden festgestellte Wirksamkeit einer Schutzmaßnahme das erforderliche Soll der DS-GVO erfüllt, ist letztlich eine rechtliche und damit von Jurist*innen zu beantwortende Frage: Während beispielsweise Informatiker*innen unter Anwendung des Differential Privacy Modells für ein konkretes Anonymisierungsverfahren rechnerisch den Epsilon-Wert bestimmen können, müssen die Jurist*innen entscheiden, ob die Daten mit diesem Epsilon-Wert dem konkreten Fall angemessen sind und damit rechtlich als anonymisiert gelten können oder nicht. Ähnliches gilt auch für andere Anonymisierungsverfahren, etwa die k-Anonymisierung, oder für unterschiedliche Ausgestaltungen des Hashings.[7] Das Wirksamkeitserfordernis zwingt Datenschutzjurist*innen bei der Anwendung von Art. 25 Abs. 1 DS-GVO, sich konzeptionell-methodisch mit Vertreter*Innen anderer Disziplinen auszutauschen und abzustimmen.

Dieser interdisziplinäre Austausch stellt unseres Erachtens eine der wesentlichen Herausforderungen für die Anwendung von Art. 25 Abs. 1 DS-GVO in der (Vollzugs-)Praxis dar. Nichtsdestotrotz wird eine solche interdisziplinäre Zusammenarbeit nicht nur offiziell längst eingefordert, sondern in bestimmten Bereichen auch mit Selbstverständlichkeit gelebt. Ein Beispiel für den ersten Fall sind die „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“, in denen der EDSA feststellt, dass der Verantwortliche Schlüsselindikatoren festlegen muss, um die Wirksamkeit der von ihm eingesetzten Mittel zu messen und nachzuweisen. Dazu gehören unter anderem quantitative Metriken und qualitative Methoden wie etwa durch die Hinzuziehung entsprechender Sachverständiger.[8] Die quantitative und qualitative Messung von Leistungsindikatoren zum Nachweis der Wirksamkeit von bestimmten Maßnahmen erfordert Methoden und Konzepte, die üblicherweise von anderen Disziplinen erbracht wird als der Rechtsauslegung.[9] In Bezug auf die Mensch-Computer-Schnittstelle weist die Art. 29-Gruppe in ihren „Leitlinien für Transparenz gemäß der Verordnung 2016/679“ darauf hin, dass

[5] DSK, Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen.
[6] Siehe hierzu sowie den weiteren Ausführungen bei M. v. Grafenstein (under review), Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centered UX-design methods, CLSR; auch die Frage, wie der „angemessene Aufwand“ gemessen werden soll, ist noch weitgehend ungeklärt, siehe etwa F. Pallas in Fn. 2.
[7] M. Finck und F. Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, IDPL 2020, Vol. 10, No. 1, S. 11 ff.
[8] EDSA, ‘Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, 20. Oktober 2020, Rn. 16.
[9] Siehe allerdings die Disziplinen der Rechtswirkungsforschung und der Regulierungswissenschaft, die bereits im Ansatz interdisziplinär verfasst sind, die in der klassischen Ausbildung jedoch ein Nischendasein führen.

geeignete Transparenzmaßnahmen im Lichte der User Experience getestet werden und die Verantwortlichen im Rahmen der Anwendertests verschiedene Modalitäten ausprobieren sollten (z.B. Auditoriumtests oder andere Standardtests).[10] Auch in tatsächlicher Hinsicht rekurrieren Jurist*innen etwa in Debatten darüber, wie wirksam bestimmte Verschlüsselungs- oder Anonymisierungsverfahren das Vertraulichkeits- oder Datenminimierungsprinzips umsetzen, wie selbstverständlich auf Ergebnisse der technischen Diskussionen (auch wenn die rechtliche Einordnung dieser außer-rechtlichen Ergebnisse nicht immer leicht fällt).[11] Dass für die Feststellung der Wirksamkeit der Schutzmaßnahmen ein entsprechender interdisziplinärer Austausch nötig ist, wird zumindest in diesen Bereichen kaum angezweifelt. Uns ist kein Grund ersichtlich, wieso dies nicht auch für andere Verarbeitungsgrundsätze bzw. für weitere Methoden aus anderen Disziplinen gelten soll. Dies werden wir im übernächsten Punkt mit Blick auf die Umsetzung des Transparenzprinzips und der Betroffenenrechte durch User-Experience-Design-Methoden veranschaulichen. Zunächst soll aber kurz auf die Implikationen für den sog. Stand der Technik i.S.v. Art. 25 Abs. 1 DS-GVO eingegangen werden.

4 SCHLUSSFOLGERUNGEN FÜR DEN STAND DER TECHNIK

Sobald man die Wirksamkeit bestimmter Schutzmaßnahmen verlässlich prüfen kann, lassen sich diese in ihrer Wirksamkeit vergleichen. Ein solcher Vergleich ist unerlässlich für die Berücksichtigung des Stands der Technik, der die wirksamste, auf dem Markt verfügbare Technik fordert.[12] Eine solche sog. dynamische Verweisung hat zur Folge, dass das rechtlich zu berücksichtigende Schutzniveau sich an dem jeweiligen Schutzniveau ausrichtet, das auf dem Markt verfügbar ist. Erfahrungen aus dem Umweltrecht zeigen, dass eine solche Regelung eine für die Erreichung der gesetzgeberischen Ziele sehr positive Marktdynamik erzeugen kann. Das ist der Fall, sobald sich einzelne Akteure die Fortentwicklung des Stands der Technik zu ihrem Ziel setzen. Das können Forschungsinstitute, aber auch private Unternehmen sein, die die Fortentwicklung des Stands der Technik zu einem Element ihres Geschäftsmodells machen.[13] Voraussetzung hierfür ist jedoch zweierlei: erstens, dass die Methoden zur Feststellung der Wirksamkeit der Schutzmaßnahmen geklärt sind; und zweitens, dass die Methoden in der (Vollzugs-)Praxis auch angewendet werden.

5 WIRKSAME TRANSPARENZ UND BETROFFENENRECHTE AM BEISPIEL DES COOKIE-BANNERS

Unter Anwendung dieses methodischen Ansatzes lassen sich zum Beispiel Ausgestaltungen von Cookie-Bannern, die eine Kontrolle der Cookie-Einstellungen (und der mit ihnen verbundenen Risiken) für die Betroffenen leichter und damit wirksamer als andere Ausgestaltungen machen, relativ leicht feststellen und in der Praxis durchsetzen. Hängt die Wirksamkeit von Schutzmaßnahmen – wie bei der Transparenz und Betroffenenrechten – von der Nutzerfreundlichkeit dieser Maßnahmen ab, liegt eine Zusammenarbeit mit User-Experience-Design- bzw. Human-Computer-Interaction-Methoden nahe. Diese Disziplinen befassen sich seit einigen Jahrzehnten mit der Frage, wie man digitale Schnittstellen

[10] Art. 29-Gruppe, 'Leitlinien für Transparenz gemäß der Verordnung 2016/679', 11. April 2018, insb. Rn. 24 und 25.
[11] J. Hölzel, 'Differential Privacy and the GDPR' (2019) 5 European Data Protection Law Review, S. 184-196.
[12] Ob bzw. wieweit der Verantwortliche die wirksamste Technik dann tatsächlich implementieren muss, hängt u.a. von den Kosten ab, siehe bereits oben F. Pallas in Fn. 2 und M. v. Grafenstein in Fn. 6.
[13] Weitere Nachweise bei M. v. Grafenstein (in publishing, expected in 2022). Co-Regulation and the Competitive Advantage in the GDPR, siehe Fn. 2.

gestalten muss, damit Nutzer*innen in ihrer Interaktion mit den Maschinen bestimmte Ziele besonders leicht erreichen. Mit diesen empirischen Methoden lässt sich etwa messen, mit welcher Gestaltungsoption eines Banners Nutzer das Ziel einer selbstbestimmten Risikokontrolle wirksamer erreichen. Anhand der mit einem Cookie-Banner typischerweise erhobenen Daten und verfolgten Zwecke lassen sich die Risiken eines solchen Banners evaluieren und verschiedene grafische Ausgestaltungen des Banners in ihrer Wirksamkeit vergleichen. Die wirksamste Ausgestaltung stellt den Stand der Technik dar, den alle Verwender eines solchen Banners nun berücksichtigen müssen.[14] Dieses Ergebnis gilt, bis eine wirksamere Ausgestaltung nachgewiesen ist. Unserer Meinung nach lässt sich die zu erwartende Dynamik auf der Grundlage von Art. 25 Abs. 1 DS-GVO anstoßen. Hierfür braucht es aber nicht nur eines geklärten Prüfansatzes, sondern idealerweise auch eines abgestimmten Vorgehens der Datenschutzaufsichtsbehörden (idealerweise auf europäischer Ebene). In der Tat bräuchte man ein neues Gesetz dagegen nicht.[15]

6 REFERENCES

Artikel-29-Datenschutzgruppe (2018): Leitlinien für Transparenz gemäß der Verordnung 2016/679. 11. April 2018.

Bygrave, L. A. (2017): Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. In: *Oslo Law Review*, 1 (02), 105-120. DOI: https://doi.org/10.18261/issn.2387-3299-2017-02-03.

Datenschutzkonferenz (2018): Kurzpapier Nr. 18. Risiko für die Rechte und Freiheiten natürlicher Personen. Abgerufen am 11. November 2021, von https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

Europäischer Datenschutzausschuss (2020): Leitlinien 4/2019 zu Artikel 25. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. 20. Oktober 2020.

Finck, M. & Pallas, F. (2020): They who must not be identified - distinguishing personal from non-personal data under the GDPR. In: *International Data Privacy Law*, 10 (1), 11-36, DOI: https://doi.org/10.1093/idpl/ipz026.

Gerber, T. (2021): Zeitung: Justizministerium will Cookie-Banner umgestalten. Heise Online. Abgerufen am 11. November 2021, von https://www.heise.de/news/Zeitung-Justizministerium-will-Cookie-Banner-umgestalten-5026576.html.

Grafenstein, M. v. (im Erscheinen): Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design. In: González-Fuster, G., van Brakel, R. & P. De Hert (Hrsg.): *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*.

Grafenstein, M. v., Heumüller, J., Belgacom, E., Jakobi, T., Smieskol, P. & Wunderlich, L. (2021): Effective regulation through design - Aligning the ePrivacy regulation with the EU General Data Protection Regulation (GDPR): tracking technologies in personalised internet content and the data protection by design approach. In: OpenAIRE. DOI: 10.5281/zenodo.5575447

Hölzel, J. (2019): Differential Privacy and the GDPR. In: *European Data Protection Law Review*, 5 (2), 184-196. DOI: https://doi.org/10.21552/edpl/2019/2/8.

Pallas, F. (2018): Datenschutz in Zeiten alles durchdringender Vernetzung: Herausforderungen für das Zusammenspiel von Technik und Regulierung. In: Roßnagel, A., Friedewald, M. & Hansen, M. (Hrsg.): *Die Fortentwicklung des Datenschutzes. DuD-Fachbeiträge*. DOI: https://doi.org/10.1007/978-3-658-23727-1_2.

Pohle, J. (2015): Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. In: *FIfF-Kommunikation*, 32 (2), 41-44.

[14] Da die Kosten für die verschiedenen Gestaltungsoptionen bei einer Erstimplementierung neutral sind, steht hier der wirksamsten Gestaltungsoption zumindest kein Kostenargument entgegen.

[15] Siehe den Beitrag „Justizministerium will Cookie-Banner umgestalten" auf Heise.de verfügbar unter https://www.heise.de/news/Zeitung-Justizministerium-will-Cookie-Banner-umgestalten-5026576.html.