TUM THINK TANK

Vereinfachung der B2B-Compliance

Christoph Bausewein & Michael Will
Arbeitsgruppe DSGVO am TUM Think Tank

1. Kontext

Obwohl sich das Institut der Auftragsverarbeitung (Art. 28 und 29 DSGVO) in der Praxis bewährt hat und das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern sowie gegenüber Betroffenen und Dritten stimmig ordnet, führt es regelmäßig zu erheblichen administrativen und rechtlichen Aufwänden, die zusammen mit Problemen der praktischen Rechtsdurchsetzung zu einer grundlegenden Überprüfung Anlass geben:

Vor Beginn einer Verarbeitung müssen Verantwortliche sicherstellen, dass Auftragsverarbeiter

- die Anforderungen der DSGVO – insbesondere die Datenschutzgrundsätze nach Art. 5 DSGVO – erfüllen,
- im EU-Binnenmarkt zuverlässig und im Sinne des Gesetzgebers agieren,
- die Verarbeitung rechtmäßig erbringen,
- personenbezogene Daten sicher verarbeiten und angemessen gegen unbefugten Zugriff, Verlust etc. schützen,
- alle relevanten Informationen zur Verarbeitung bereitstellen können sowie
- bei Übermittlungen in Drittländer geeignete Garantien nach Art. 44 ff. DSGVO nachweisen, sodass ein ortsunabhängig im Wesentlichen gleichwertiges Schutzniveau gewährleistet ist.

In der Praxis ist der Verantwortliche hierfür regelmäßig auf die Kooperation des Auftragsverarbeiters angewiesen. Bei Ungleichgewichten – insbesondere bei marktmächtigen Auftragsverarbeitern – kann dies dazu führen, dass Verantwortliche ihre Pflichten nur mit erheblichem Aufwand oder gar nicht erfüllen können und sich in monopolähnlichen Situationen Bedingungen beugen müssen, die im Einzelfall nicht zwingend rechtskonform sind.

Zudem müssen für jede Einzelbeziehung wiederholt Nachweise erbracht und umfangreiche Auftragsverarbeitungsverträge geschlossen werden; bei internationalen Übermittlungen kommen, sofern kein Angemessenheitsbeschluss (Art. 45 DSGVO) oder andere geeignete Garantien (Art. 46 DSGVO) bestehen, Standardvertragsklauseln (SCCs) hinzu. Das verursacht hohe Transaktionskosten auf beiden Seiten, ohne dass – bei ökonomischer Analyse des Rechts – stets ein proportionaler Mehrwert für den individuellen Datenschutz erkennbar ist. Teilweise läuft dies sogar den Binnenmarktzielen der DSGVO (Art. 1 i. V. m. Art. 16 AEUV) zuwider und begünstigt die Wahrnehmung von Datenschutz-Compliance als bürokratische Last statt als Voraussetzung fairen Wettbewerbs und rechtskonformen Marktzugangs.

Bislang fehlt es an einer unionsweit einheitlichen und systematisch überprüfbaren Alternative, die Rechtsklarheit und Praktikabilität miteinander verbindet. Die Vielzahl individueller Vertragswerke, Standardklauseln und Auditverfahren führt nicht nur zu erheblichem Verwaltungsaufwand, son-

dern auch zu Rechtsunsicherheiten hinsichtlich Zuständigkeiten, Prüfmaßstäben und Haftungsverteilung. In der Folge entsteht ein Fragmentierungsproblem, das insbesondere für kleine und mittlere Unternehmen (KMU) die Teilnahme am europäischen Datenbinnenmarkt erschwert. Während große, global agierende Anbieter aufgrund ihrer Ressourcen und Marktstellung eigene Standardverträge und Compliance-Rahmen etablieren können, fehlt kleineren Marktteilnehmern oftmals die Verhandlungsmacht, um faire Bedingungen durchzusetzen. Dies führt zu einem Ungleichgewicht zwischen Verantwortlichen und Auftragsverarbeitern, das dem Gedanken gleicher Wettbewerbsbedingungen im Binnenmarkt zuwiderläuft.

Um Abhilfe zu schaffen, zugleich aber Grundrechte effektiv zu wahren sowie Kontrolle und Rechtsdurchsetzung sicherzustellen wird folgender Reformvorschlag unterbreitet, der das Ziel verfolgt, ein vereinfachtes, systemisch tragfähiges B2B-Compliance-Regime zu entwickeln, das

- Datenschutzkonformität als Marktzutrittsvoraussetzung für Auftragsverarbeiter definiert,
- Verantwortliche von Einzelfallprüfungen befreit, indem es Vertragsprüfungen ersetzt,
- zentralisierte Kontrolle von Selbstverpflichtungen durch Schlichtungsstellen und Aufsichtsbehörden statt einzelvertraglicher Selbsthilfe nutzt, und
- zugleich ein alternatives System zu Standardvertragsklauseln zur Absicherung von Datenübermittlungen in Drittländer schafft, das auf einmaligen, transparenten Verpflichtungen von Auftragsverarbeitern beruht,
- sowie im Übrigen – für Auftragsverarbeiter, die sich keiner Selbstverpflichtung unterwerfen – ihr Verhältnis zum Verantwortlichen als klar definiertes gesetzliches Schuldverhältnis ausgestaltet.

2. Reformvorschlag

Vor diesem Hintergrund hat die Arbeitsgruppe den folgenden Vorschlag zur Vorprüfung und Vertragspflicht zur Selbstverpflichtung mit gesetzlicher Vermutung erarbeitet.

Zur Wahrung und Förderung eines wirksamen Grundrechtsschutzes, zur Reduktion von Transaktionskosten und zur Stärkung von KMU in asymmetrischen Marktverhältnissen sollte die heutige Pflicht des Verantwortlichen zur Vorprüfung und zum Vertragsschluss weitmöglich zu rechtsverbindlichen Selbstverpflichtungen des Auftragsverarbeiters verlagert werden. Diese gelten allgemeinverbindlich (nicht nur im Einzelfall) und werden gegenüber einer zentralen europäischen Stelle abgegeben. Der Auftragsverarbeiter erklärt, dass er

- die Anforderungen der DSGVO – insbesondere die Grundsätze des Art. 5 – einhält,
- im Binnenmarkt rechtmäßig, transparent und verantwortungsvoll handelt und Datenschutz als integralen Bestandteil der Geschäftstätigkeit begreift,
- Rechenschaft über seine Verarbeitungstätigkeiten ablegen kann,
- durch angemessene Sicherheitsmaßnahmen (TOM) schützt,
- standardisierte, leicht zugängliche Informationen zu Art, Zweck, Umfang und Empfängern der Verarbeitung bereitstellt und
- bei Drittlandübermittlungen eigenständig geeignete Garantien gemäß den SCCs implementiert, die ein der DSGVO gleichwertiges Schutzniveau gewährleisten – unabhängig vom Speicher- oder Verarbeitungsort.

Publizität und Vermutung

Die Selbstverpflichtung wird in ein öffentliches Register aufgenommen; ab Veröffentlichung begründet sie eine gesetzliche Vermutung für die DSGVO-Konformität des Auftragsverarbeiters.

Sorgfaltspflicht des Verantwortlichen (geteilte Rechenschaft)

Verantwortliche dürfen auf diese Vermutung vertrauen; sie bleiben jedoch im Rahmen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO verpflichtet, bei konkreten Hinweisen eine plausibilisierende Prüfung vorzunehmen (keine „Blindverlass"-Freistellung).

Ergänzendes Haftungsregime

Mit Abgabe der Selbstverpflichtung unterwirft sich der Auftragsverarbeiter einem besonderen Haftungsregime, das das DSGVO-Haftungsgefüge (insb. Art. 82 DSGVO) ergänzt. Insbesondere Falschangaben und selbstverpflichtungswidriges Verhalten begründen eigene Haftungstatbestände.

Beschwerde- und Aufsichtsmechanismus: Kooperative Überwachung der Selbstverpflichteten

Ein plattformgestütztes, selbständiges Beschwerdesystem ermöglicht Verantwortlichen und Betroffenen substantiierte Beschwerden. Zum Missbrauchsschutz sollten Darlegungspflichten vorgesehen werden, die - neben bestehenden strafrechtlichen Grenzen, z. B. Verleumdung – Risiken einer exzessiven Rechtsausübung vorbeugen.

Selbständige Beschwerdestelle und Datenschutzaufsichtsbehörden werden zu enger Kooperation und regelmäßigem Austausch verpflichtet. Verstöße von Auftragsverarbeitern gegen ihre Selbstverpflichtungserklärungen sollen von den Datenschutzaufsichtsbehörden mit Priorität aufgegriffen werden.

Nachprüfungsmechanismus

Die Aktualität und Richtigkeit der Angaben des Auftragsverarbeiters sollen durch ein regelmäßig wiederkehrenden Nachprüfungsmechanismus gefördert werden:

- Jährliche Bestätigung der Angaben und unverzügliche Meldung wesentlicher Änderungen,
- qualifizierte aufsichtsrechtliche Verfolgung von Verstößen; bei schwerwiegenden/wiederholten Verstößen Löschung aus dem Register bzw. Marktausschluss,
- niedrigschwellige Beschwerden auch durch Mitbewerber, die standardisierte Ermittlungen auslösen können.

Wettbewerbsschutz

Als zusätzliches Korrektiv gegen Marktverzerrungen wird ein wettbewerbsrechtliches Element verankert: Falsche oder irreführende Selbstverpflichtungen können durch Mitbewerber zivilrechtlich angegriffen werden (unlauterer Wettbewerb). Das könnte Glaubwürdigkeit und Marktintegrität stärken.

„Take-it-or-leave-it" Prinzip

Nur Auftragsverarbeiter, die sich der Selbstverpflichtung mit allen Pflichten (inkl. Haftungs- und Aufsichtsregime) unterwerfen, dürfen umfassende, auch Verarbeitungen mit hohen Risken für Rechte und Freiheiten der Betroffenen umfassende Leistungen der Auftragsverarbeitung im EU-Binnenmarkt anbieten. Wer dies ablehnt, erhält insoweit keinen Marktzugang. Auftragsverarbeiter, deren Leistungen keine Verarbeitungen mit hohen Risiken umfassen erhalten Marktzugang schon im Rahmen eines gesetzlich definierten Auftragsverarbeitungsverhältnisses, das in Haftung und Aufsicht Abstufungen gegenüber Auftragsverarbeitern mit Selbstverpflichtungserklärungen vorsieht.

Förderung von Privacy-, Resilience- und Security-by-Design

Der Selbstverpflichtungsmechanismus verankert die Gedanken von Privacy-, Resilience- und Security-by-Design als Voraussetzung des Markteintritts. Er wahrt Gestaltungsfreiheit und Eigenverantwortung, koppelt diese aber an klare Rechenschaft und wirksame Aufsicht – ein Anreizsystem zugunsten sicherer, daten-

schutzgerechter Services.

Rechenschaft und Datentransparenz

Tragendes Element ist die Bringschuld des Auftragsverarbeiters zur Nachweiserbringung gegenüber Verantwortlichen. Ein standardisiertes Datenblatt (Schlüsselangaben i. S. v. Art. 28 DSGVO) könnte

- zur Überprüfbarkeit im B2B-Verhältnis beitragen,
- die Vertrauensbasis stärken und
- Mehrfachaufwand vermeiden, da es mehrfach nutzbar ist.

Zugleich kann es die Dokumentation des Verantwortlichen (Art. 30 DSGVO) erleichtern, indem es als Referenz in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden könnte. Die Zweckbestimmung der Auftragsverarbeitung bleibt dabei Aufgabe des Verantwortlichen.

Förderung von Privacy-, Resilience- und Security-by-Design

Der Selbstverpflichtungsmechanismus verankert die Gedanken von Privacy-, Resilience- und Security-by-Design als Voraussetzung des Markteintritts. Er wahrt Gestaltungsfreiheit und Eigenverantwortung, koppelt diese aber an klare Rechenschaft und wirksame Aufsicht – ein Anreizsystem zugunsten sicherer, datenschutzgerechter Services.

Seine Implementierung wird per Durchführungsrechtsakt der EU-Kommission übertragen, so dass Einzelheiten seiner Ausgestaltung und Fortentwicklung unter Beteiligung der Expertise der Datenschutzaufsichtsbehörden und des Europäischen Datenschutzausschusses sowie der betroffenen Kreise in einem transparenten und dynamischen Verfahren gewährleitet werden. Flankierend sind jedenfalls in Art. 24 und 25 ergänzend Pflichten des Auftragsverarbeiters zu begründen und notwendige Folgeanpassungen bei Individualrechtsschutz und Haftungsregeln zu berücksichtigen.

Regelungsvorschlag: Art. 28 DSGVO als gesetzliches Schuldverhältnis –Compliance by Default

Ergänzend werden die bisher in Art. 28 DSGVO durch Einzelverträge festzulegenden Grundpflichten von Auftragsverarbeitern und Verantwortlichen in ein gesetzliches Schuldverhältnis umgestaltet, das als Rechtsfolge bei Begründung eines Vertragsverhältnisses über Leistungen der Auftragsverwaltung weitgehend „automatisch“ zustande kommt. Gerade kleinere Auftragsverarbeiter, für die der Mechanismus der Selbstverpflichtungen zu hohe Komplexität mit sich bringen könnte, erfahren insoweit zusammen mit ihren Vertragspartnern Entlastungen von datenschutzrechtlichen Aufwendungen durch die oft als unproduktiv empfundene Abarbeitung von Standardvertragsklauseln. Der Regelungsvorschlag lässt freilich im Einzelfall zusätzlich zu berücksichtigende Anforderungen an Datenübermittlungen an Drittländer unberührt.

3. Einordnung

Nachfolgend findet sich eine zusammenfassende Übersicht der Vor- und Nachteile des Vorschlags zur weiterführenden Diskussion.

Vorteile

- **Systemische Entlastung des Binnenmarkts:** Einheitliche Selbsterklärung eliminiert individuelle Prüfpflichten der Verantwortlichen und reduziert Transaktionskosten bei gleichzeitig hoher Rechtssicherheit.
- **Regulatorische Effizienz:** Zentrale Kontrolle anstelle von Millionen bilateraler Verträge; fokussierte Aufsicht ermöglicht präzisere Intervention bei Verstößen.
- **Marktbasiertes Anreizsystem:** Auftragsverarbeiter haben ein Eigeninteresse, die Selbsterklärung einzuhalten – bei Täuschung drohen Sanktionen und Reputationsverluste. Dadurch wird Datenschutz vom Pflichterfordernis zum Wettbewerbsfaktor.
- **Bürokratieentlastung:** Verzicht auf individuelle Vereinbarungen zur Auftragsverarbeitung mindert Compliance-Aufwand und schafft Spielraum für datenschutzrechtliche Kernaufgaben.

Nachteile

- **Gefahr einer „Papier-Compliance“:** Ohne externe Überprüfung besteht das Risiko, dass Selbstverpflichtungen formal erfüllt werden, ohne tatsächliche Gewähr für die Einhaltung der Datenschutzgrundsätze zu bieten. Dies könnte zu einem bloßen „Vertrauensversprechen auf dem Papier“ führen, das Verantwortlichen keine zusätzliche materielle Sicherheit verschafft.
- **Unklarheiten zur Reichweite der Vermutungswirkung und zum Prüfmaßstab:** Ohne klare Vorgaben (z. B. Checklisten oder standardisierte Bewertungskriterien) drohen Inkonsistenzen zwischen Mitgliedstaaten und ein erhöhtes Risiko unterschiedlicher Aufsichts- oder Gerichtspraxis.
- **Herausforderung Qualitätssicherung:** Externe Prüfmechanismen – etwa durch anerkannte Zertifizierungs- oder Prüfinstitutionen – könnten trotzdem nur begrenzt ein höheres Maß an Verlässlichkeit und Vertrauen schaffen. Die Wirksamkeit solcher unabhängigen Kontrollen ist Grundbedingung für die Glaubwürdigkeit des Systems, das nur bei Gewährleistung einer engen Kooperation mit der Datenschutzaufsicht tragfähiges Vertrauen bei der Auswahl von Auftragsverarbeitern vermitteln wird.
- **Gefahr falscher Signalwirkung:** der Verzicht auf die Warnfunktion gesonderter vertraglicher Regelungen zur Auftragsverarbeitung kann die Rechtssicherheit über die im Einzelfall zu beachtenden Anforderungen und Verpflichtungen schmälern.

ARBEITSGRUPPE DSGVO

Die Arbeitsgruppe DSGVO am TUM Think Tank bringt Expertinnen und Experten aus Wissenschaft, Praxis, Aufsicht und Zivilgesellschaft zur Weiterentwicklung der DSGVO zusammen. Dies ist einer von vier konkreten, rechtlich anschlussfähigen Reformbausteinen, die sowohl Datenschutz wirksamer machen als auch verantwortliche Datennutzung für Wirtschaft und Gesellschaft erleichtern.

Der TUM Think Tank bietet die organisatorische Plattform. Initiiert wurde die Arbeitsgruppe von Kai Zenner, Max Schrems, Boris Paal und Markus Siewert.

INSTITUTION

TUM Think Tank | Hochschule für Politik München |
Technische Universität München

DISCLAIMER

Der vorliegende Reformvorschlag (Version 1.0) wird von einer Mehrheit der Arbeitsgruppe mitgetragen, auch wenn nicht alle Mitglieder allen Teilen gleichermaßen zustimmen und durchaus auch abweichende Meinungen existieren.

Die Vorschläge verstehen sich nicht als Endpunkt, sondern als Ausgangspunkt für weiterführende Diskussionen. In den kommenden Wochen und Monaten wird die Arbeitsgruppe diese Vorschläge – insbesondere vor dem Hintergrund der derzeit teilweise kontrovers geführten Debatten zum Digital Omnibus – weiterentwickeln und zusätzliche Reformbausteine ausarbeiten.

Die in diesem Bericht geäußerten Inhalte und Ansichten geben ausschließlich die Meinung der Autoren wieder und sind nicht dem TUM Think Tank als Institution oder seinen Mitgliedern zuzuschreiben.

KONTAKT

tumthinktank@hfp.tum.de
https://tumthinktank.de

Mitglieder der Arbeitsgruppe DSGVO

Christoph Bausewein | Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Linda Bienemann | Persönliche Referentin Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Franziska Boehm | FIZ-Karlsruhe & Karlsruher Institut für Technologie (KIT)

Stefan Brink | Wissenschaftliches Institut für die Digitalisierung der Arbeitswelt (WIDA) / Berlin

Thomas Fuchs | Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (HmbBfDI)

Niko Härting | HÄRTING & Deutscher Anwaltverein

Peter Hense | Spirit Legal Rechtsanwaltsgesellschaft mbH

Boris Paal | Technische Universität München

Frederick Richter | Stiftung Datenschutz

Max Schrems | noyb

Louisa Specht-Riemenschneider | Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Christiane Wendehorst | Universität Wien

Michael Will | Bayerisches Landesamt für Datenschutz (BayLDA)

Kai Zenner | MEP Axel Voss, Europäisches Parlament & TUM Think Tank