Schlussstrich

Die Regelungen zur Datenportabilität in der DSGVO, dem DMA und dem DA bieten umfassende und vielseitige Ansprüche, die sowohl natürliche als auch juristische Personen betreffen. Diese Rechte fördern die Kontrolle über personenbezogene und nicht-personenbezogene Daten und unterstützen den Wettbewerb im digitalen Binnenmarkt. Dennoch bestehen unterschiedliche Anforderungen und Einschränkungen hinsichtlich der Anspruchsberechtigten, -verpflichteten und der Art der herauszugebenden Daten. Auch der Schutz von Geschäftsgeheimnissen spielt eine zentrale Rolle. Sofern Unternehmen noch nicht mit der Implementierung von entsprechenden Prozessen begonnen haben, scheint es höchste Zeit zu sein.

Die aktualisierten Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung

Eine Untersuchung der Entwicklung und der Unterschiede in den AVB Cyber idF 2017 und 2024

BEITRAG. Die Relevanz von Cyberversicherungen hat angesichts der zunehmenden Bedrohungen durch Cyberrisiken an Bedeutung gewonnen. Dieser Beitrag führt eine konzise Analyse der vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) im Februar aktualisierten Musterbedingungen für die Cyberrisiko-Versicherung durch und beleuchtet die Änderungen im Vergleich zu den ursprünglichen Musterbedingungen aus dem Jahr 2017, die iW mit den österreichischen Musterbedingungen übereinstimmen. Ziel dieser kurzen Abhandlung ist das Aufzeigen der Weiterentwicklung und die Anpassung der Versicherungsbedingungen an die sich verändernde Bedrohungslage sowie die Rezeption der Anforderungen seitens der Versicherungswirtschaft.[1)] ecolex 2024/411

Mag.[a] **Lisa Katharina Promok** ist Leiterin des Forschungsinstituts für Privatversicherungsrecht an der Paris Lodron Universität Salzburg.

A. Vorbemerkungen

Im Kontext der voranschreitenden Digitalisierung und der damit einhergehenden zunehmenden Bedrohungen durch Cyberrisiken haben Cyberversicherungen an Relevanz gewonnen. Derartige Versicherungen können, je nach Ausgestaltung, Schutz vor finanziellen Schäden bieten, die durch Informationssicherheitsverletzungen, Datenverluste und andere mit Cyberangriffen einhergehende Schadensereignisse eintreten können. In den folgenden Ausführungen werden die vom GDV im Februar 2024 aktualisiert ausgegebenen Musterbedingungen für die Cyberrisiko-Versicherung einer kurzen Analyse unterzogen und die Änderungen im Vergleich zu den ursprünglichen Musterbedingungen aus dem Jahr 2017 beleuchtet. Ziel dieses Similes ist das Aufzeigen der inhaltlichen Unterschiede, um ein besseres Verständnis der jeweiligen Deckungsumfänge, Risikoausschlüsse und der spezifischen Bedingungen zu ermöglichen sowie daraus resultierende Implikationen einerseits für Versicherungsnehmer[2)] und andererseits für die Versicherungswirtschaft in ihrer Gesamtheit zu untersuchen.

Die in Österreich vom Verband der Versicherungsunternehmen Österreichs (VVO) herausgegebenen Musterbedingungen für die Cyberversicherung, die ABC 2018, orientieren sich stark an den AVB Cyber in der Fassung aus 2017 und wurden spezifisch für den österr Markt mit geringfügigen Anpassungen versehen. Da sich die österr Musterbedingungen aus dem Jahr 2018 somit nicht wesentlich von den deutschen Musterbedingungen aus dem Jahr 2017 unterscheiden, in Teilen gar wortgleich sind, weisen die folgenden Ausführungen auch für die österr Musterbedingungen hohe Relevanz auf. Nachdem der deutsche Verband nun wieder maßgeblich vorangegangen ist, werden geringfügige Adaptierungen der österr Musterbedingungen für die Cyberversicherung vermutlich innerhalb der nächsten zwölf Monate zu erwarten sein. Es kann allerdings auch sein, dass der VVO aufgrund der vom GDV so zögerlich erfolgten Adaptierungen an der Originalversion der ABC 2018 festhält. Sowohl die deutschen als auch die österr Musterbedingungen gehen an den Marktbedürfnissen vorbei. Die jüngsten Änderungen der deutschen Musterbedingungen verdeutlichen, dass die Erfahrungen der Praxis teilweise in die Aktualisierung eingeflossen sind. Es sei an dieser Stelle darauf hingewiesen, dass der Umfang dieses Kurzbeitrags lediglich eine überblicksartige Darstellung der wichtigsten Änderungen ermöglicht.

1. Struktur und Aufbau der beiden Fassungen

Beide Versionen sind ähnlich strukturiert und gliedern sich in zwei Teile (A und B), die beide in weitere Abschnitte unterteilt sind und die verschiedenen Aspekte der Cyberrisiko-Versicherung abdecken. Teil A enthält Regelungen zur Ausgestaltung

[1)] Die Grundlage und Literatur für diesen Beitrag bilden lediglich die Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung Stand: 2017 und Stand: 2024.

[2)] Im Folgenden kurz VN genannt.

des Versicherungsschutzes in der Cyberrisiko-Versicherung und umfasst die vier folgenden Bausteine:[3)]
- ➤ Abschnitt A1 – Basis-Baustein
- ➤ Abschnitt A2 – Service- und Kosten-Baustein
- ➤ Abschnitt A3 – Drittschaden-Baustein
- ➤ Abschnitt A4 – Eigenschaden-Baustein

In den einzelnen Abschnitten des Teil A werden allgemeine bausteinübergreifende Regelungen (A1), Kostenpositionen für den Zeitpunkt vor und nach Eintritt des Versicherungsfalls (A2), der Haftpflichtversicherungsschutz sowie der Versicherungsschutz für Eigenschäden (Betriebsunterbrechung und Datenwiederherstellung) geregelt. Teil B enthält Bestimmungen über allgemeine Rechte und Pflichten der Vertragsparteien und regelt den Beginn des Versicherungsschutzes und die Beitragszahlung (Abschnitt 1) sowie Dauer und Ende des Vertrags/die Kündigung. Die Abschnitte 3 und 4 enthalten Obliegenheiten des VN bei und nach Eintritt des Versicherungsfalls und weitere Vorschriften (statt Bestimmungen).

Was den Aufbau anbelangt, so sind daran keine Unterschiede festzumachen, lediglich der Umfang hat sich geringfügig ausgedehnt, was eher auf ausführlichere Formulierungen an mancher Stelle rückführbar ist, denn auf groß angelegte Erweiterungen.

B. Wesentliche Unterschiede der beiden Fassungen

1. Definition und Umfang der Informationssicherheitsverletzung

Sowohl die AVB Cyber[4)] idF 2017 und idF 2024 definieren eine *Informationssicherheitsverletzung* jeweils in Teil A Abschnitt A1–2.1 als eine Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit von elektronischen Daten oder informationsverarbeitenden Systemen. Der Unterschied liegt jedoch im Detail der Formulierung und den Bedingungen des Versicherungsschutzes. Es erfolgte eine Deckungserweiterung in A1–2.1 AVB Cyber auf Daten, die mittels *Fernzugriff* genutzt werden. Nachdem die ursprünglichen Bedingungen Homeoffice und mobiles Arbeiten vollständig ausklammerten, wird nun den Veränderungen der Arbeitswelt insb nach der COVID-19-Krise Rechnung getragen, wonach Homeoffice-Regelungen und mobiles Arbeiten an Relevanz gewonnen haben. So werden Daten, derer sich via Fernzugriff bedient wird, nun explizit vom Versicherungsschutz mitumfasst. Es werden an dieser Stelle allerdings keine weiteren Sicherheitsanforderungen an die Datenabfrage via Fernzugriff geknüpft, sodass sich für den Versicherer[5)] hier eine schwer kalkulierbare Deckungserweiterung ergäbe. Es gelangen jedoch die unter 3. ausgeführten Obliegenheiten vor Eintritt des Versicherungsfalls, wie bspw der zusätzliche Schutz gegen unberechtigten Zugriff, bei Geräten, die einem *erhöhtem Risiko* ausgesetzt sind, zur Anwendung.

2. Vorrangige Versicherung

Beide Versionen der AVB Cyber enthalten in A1–12 AVB Cyber eine *Spezialitätsklausel.* Demnach besteht Versicherungsschutz nach den Bedingungen des Cyberrisiko-Versicherungsvertrags vorrangig, auch wenn das Risiko in einem anderen Versicherungsvertrag mitabgedeckt ist. Im Gegensatz dazu ist in der D&O-Versicherung die *Subsidiaritätsklausel*[6)] als Standard zu erachten.[7)] Es sei an dieser Stelle darauf hingewiesen, dass es keine österr Musterbedingungen für die D&O-Versicherung gibt, man bedient sich hier ebenfalls des deutschen Bedingungswerks, wobei die Musterbedingungen der D&O-Versicherung (AVB D&O aus dem Jahr 2020) nicht als Klauselstandard angesehen werden können, sondern maßgeschneiderte Versicherungslösungen unterschiedlich ausfallen und stark voneinander abweichen können.[8)] A1–12 AVB Cyber spezifiziert darüber hinaus, dass ein Regressanspruch auch bei Vorliegen einer Mehrfachversicherung nach § 78 Abs 2[9)] VVG[10)] davon unberührt bleibt.[11)]

3. Obliegenheiten

Die Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit (A1–16 AVB Cyber) wurden verschwindend geringen Änderungen unterzogen. Die AVB Cyber sind nun etwas ausführlicher und geben spezifischere Anweisungen und Beispiele zu den einzelnen Erfordernissen, während die Ursprungsversion prägnanter formuliert ist. Die seitens der Praxis immer wieder geforderten Klarstellungen, was ua die sog *Stand-der-Technik-Klausel* anbelangt, blieben aus, wie in den weiteren Ausführungen dargestellt.

In den Anforderungen an informationsverarbeitende Systeme und der Unterscheidung der Nutzer und der Befugnisebenen wurde eine *detaillierte Anforderung an Passwörter* eingefügt, für diese gibt es nun bestimmte *Mindestanforderungen,* insb *die Anzahl der Zeichen* betreffend. Weitere Klarstellungen dazu wurden nicht getroffen. Es wurde in A1–16.1 lit b AVB Cyber optisch besser hervorgehoben, dass bei Geräten, die über das Internet erreichbar sind (Server), oder bei Mobilgeräten ein erhöhtes Risiko besteht und aufgrund dessen ein *zusätzlicher Schutz* der informationsverarbeitenden Systeme gegen unberechtigte Zugriffe zu erfolgen hat. Zudem wurden Bsp für Schutzmaßnahmen für mobile Geräte, wie Smartphones oder Laptops, in concreto die Verschlüsselung von Datenträgern mobiler Geräte, die Diebstahlsicherung oder ähnlich wirksame Maßnahmen erwähnt.

Darüber hinaus wurde in A1–16.1 lit d AVB Cyber das erhöhte Risiko bei informationsverarbeitenden Systemen, die einem Patch-Management-Verfahren unterliegen, etwas ausführlicher thematisiert. In diesem Fall wird in den AVB Cyber nun eine zeitnahe Installation von relevanten Sicherheitsupdates gefordert, in der die Reduktion des Risikos für die Sicherheit der informationsverarbeitenden Systeme des VN sichergestellt wird.

---

3) Für eine ausführliche Darstellung s *R. Koch,* in *Bruck/Möller*[10], Band 5, AVB Cyber, 8 ff.

4) Soferne im Folgenden die *AVB Cyber* erwähnt werden, ist die aktuell in Geltung stehende Ausgabe aus dem Jahr 2024 gemeint. Es wird an der jeweiligen Stelle konkret darauf hingewiesen, sofern auf die Version aus 2017 Bezug genommen wird.

5) Im Folgenden kurz VR genannt.

6) Zur Einordnung und Abgrenzung der Subsidiaritätsklausel von der Doppelversicherung s *Perner,* Privatversicherungsrecht (2021) 7.26 sowie zur Subsidiaritätsklausel allgemein *Ramharter,* D&O-Versicherung (2018) 133.

7) Siehe Abschnitt B4 Weitere Regelungen B4-1 AVB D&O.

8) *Perner,* Privatversicherungsrecht (2021) 7.105.

9) In Österreich regelt § 67 VersVG den Rückgriffsanspruch des VR.

10) Deutsches VersicherungsvertragsG.

11) Zum Regress des Cyberversicherers s *R. Koch,* in *Bruck/Möller*[10], Band 5, AVB Cyber, 18 ff.

Die Obliegenheiten zur IT-Sicherheit enthalten nun spezifischere Anweisungen, insb zu Passwortanforderungen und Schutzmaßnahmen für mobile Geräte.

Was den wöchentlichen Sicherungsprozess in A1–16.1 lit e AVB Cyber anbelangt, erfolgt hier eine detaillierte Anforderung an die physische Trennung des Backup-Mediums und den Schutz der Sicherungskopien. Hinsichtlich der Obliegenheiten legen die AVB Cyber idF 2024 insgesamt einen stärkeren Fokus auf präventive Maßnahmen und regelmäßige Überprüfungen.[12)]

4. Risikoausschlüsse

a) Allgemeines

In puncto Risikoausschlüsse gibt es Unterschiede in den spezifischen Ausschlüssen, wobei die tiefgreifendste Änderung der Bedingungsaktualisierung die *Kriegsklausel* betrifft, um auch den geopolitischen Entwicklungen Rechnung zu tragen.

Der in den AVB Cyber idF 2017 enthaltene Risikoausschluss *Fahrzeuge,* der ident auch in Art 2 3. ABC 2018 enthalten ist, wurde von den Risikoausschlüssen entfernt und findet sich weiter hinten bei den Besonderen Ausschlüssen unter A3–7.5 AVB Cyber. Der aktualisierte Ausschluss erweitert den Ausschluss auf spezifische Ansprüche aus Gebrauch, Planung, Konstruktion, Herstellung, Lieferung und Tätigkeiten an Fahrzeugen und Fahrzeugteilen sowie auf den Einsatz und die Entwicklung von Software für diese. Die adaptiere Variante enthält einen expliziten Ausschluss für Ansprüche iZm Softwareeinsatz und -entwicklung für Fahrzeuge und Fahrzeugteile. Ferner werden auch Ansprüche aufgrund von Verkehrsbeeinträchtigungen zu Land, Wasser und in der Luft ausgeschlossen.

Der in der Praxis oftmals wesentliche Grund für den Abschluss einer Cyberversicherung, nämlich die Abdeckung von *Lösegeldzahlungen,* ist auch weiterhin in den Allgemeinen Versicherungsbedingungen unter den Ausschlüssen aufgeführt (A1–17.7 AVB Cyber). Dies bedeutet, dass trotz der praktischen Relevanz und des zunehmenden Auftretens von Ransomware-Angriffen die Zahlung von Lösegeld an Cyberkriminelle nicht von der Versicherung abgedeckt wird. Diese Auffassung spiegelt sich lediglich in den Ausschlüssen der Musterbedingungen wider, während der Marktstandard hiervon abweicht und derartige Schäden bzw Erpressungsgelder per se regelmäßig unter spezifischen Auflagen vom Deckungsumfang mitumfasst.

b) Die Kriegsklausel

Die in A1–17.2 AVB Cyber enthaltene Kriegsklausel trägt nun den Titel *Krieg und staatliche Angriffe.* Vom Ausschluss A1–17.2 AVB Cyber umfasst sind gem lit a Versicherungsfälle oder Schäden aufgrund von Krieg, kriegsähnlichen Ereignissen, Bürgerkrieg, Revolution, Rebellion oder Aufstand, auch wenn diese Versicherungsfälle oder Schäden aufgrund einer Informationssicherheitsverletzung gem A1–2.1 AVB Cyber durch einen Staat im Auftrag oder unter Kontrolle eines Staats im Verlauf eines Kriegs entstanden sind. Die Einführung der Fälle, in denen Schäden auf Informationssicherheitsverletzungen staatlicher Akteure zurückzuführen sind, sollen den *Cyberwar* thematisieren. Neu hinzugekommen ist eben diese Spezifikation bei staatlich verursachten Cyberangriffen. Lit b thematisiert Versicherungsfälle oder Schäden aufgrund von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staats verursacht worden sind, wenn dadurch kritische Infrastrukturen im Umfang der Regelungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in diesem oder einem anderen Staat ausgefallen oder beeinträchtigt sind.

Neu sind detaillierte Anforderungen an die Beweislast und die Zuschreibung von Informationssicherheitsverletzungen zu einem Staat. Die Beweislast für die Zuschreibung einer Informationssicherheitsverletzung an einen Staat liegt beim VR. Es besteht die Möglichkeit der Berücksichtigung objektiv angemessener Beweismittel, einschließlich offizieller Zuschreibungen durch staatliche Stellen. Während die Ursprungsversion eine, wenn auch ungünstige Definition des Kriegs enthielt, wird eine solche im überarbeiteten Wording beiseitegelassen. Ebenso wenig wird auf die einzelnen Varianten des Kriegs (klassischer/konventioneller Krieg, hybrider Krieg und Cyberkrieg/Cyberwar) zufriedenstellend eingegangen. Die Änderungen, den Kriegsausschluss betreffend, sind insgesamt sehr viel zurückhaltender ausgefallen als erwartet.

Die Formulierung der Allgemeinen Ausschlüsse, *politische Gefahren* (A1–17.3 AVB Cyber) und *Terrorakte* (A1–17.4 AVB Cyber) betreffend, blieb wortgleich.

c) Vorsatz und wissentliche Pflichtverletzung

Die Risikoausschlüsse der AVB Cyber 2024 erweitern die Kriegsklausel und decken weiterhin keine Lösegeldzahlungen ab.

Schäden, die durch vorsätzliches oder wissentliches Fehlverhalten entstehen, sind nach den AVB Cyber nicht gedeckt. Die *grob fahrlässige Herbeiführung des Versicherungsfalls* (§ 81 Abs 2 VVG) ist nun in der adaptierten Version dezidiert abbedungen worden. Die AVB Cyber Stand 2024 enthalten einen Katalog an vertraglichen Obliegenheiten, die den erwarteten Stand der Technik mehr oder wenig konkret definieren. Ebenfalls hinzugekommen ist die vorvertragliche Risikoermittlung.

5. Drittschaden-Baustein

In den Erweiterten Deckungsbausteinen (A3–4 AVB Cyber) wird die *Verletzung von Datenschutzvorschriften* (A3.4.1 AVB Cyber) nun ausführlicher und konkreter geregelt. Die Neuauflage spezifiziert den Deckungsbaustein und eröffnet konkrete Ausführungen auch zu E-Payment (A3–4.2 AVB Cyber) und bietet zusätzliche Optionen für vertragliche Schadenersatzansprüche (A3–4.3 AVB Cyber). Immaterielle Schäden sind im Haftpflichtbaustein explizit eingeschlossen, insb im Hinblick auf potenzielle Klagen aus Datenschutzverletzungen nach Cyberangriffen.[13)]

6. Eigenschaden-Baustein

In den Besonderen Ausschlüssen (A4–1.2 AVB Cyber) werden Unterbrechungsschäden unter bestimmten Fällen vom Versicherungsschutz ausgeschlossen. Die Neuerung bezieht sich auf

[12)] Die ersten beiden Urteile zur Cyberversicherung beschäftigen sich mit den vorvertraglichen Anzeigepflichten und thematisieren insb die Risikofragen des Cyberversicherers. Siehe dazu LG Tübingen 26. 5. 2023, 4 O 193/21 und LG Kiel 23. 5. 2024, 5 O 128/21.

[13)] Siehe Art 82 DSGVO.

Schäden während einer *geplanten Abschaltung* von IT-Maßnahmen. Diese sind gem A4–1.2 lit a AVB Cyber ausgeschlossen, es sei denn, die Maßnahmen stehen iZm präventiven Aufwendungen vor Eintritt des Versicherungsfalls gem A2–3 AVB Cyber. Ähnlich verhält es sich auch mit geplanten Löschungen oder der Veränderung elektronischer Daten (A4–1.2 lit b AVB Cyber), der Einführung neuer informationsverarbeitender Systeme oder Software (A4–1.2 lit c AVB Cyber) oder den Einsatz ungetesteter Software (A4–1.2 lit d AVB Cyber). Schäden, die daraus resultieren, sind ausgeschlossen, es sei denn, es handelt sich um relevante Sicherheitsupdates oder Präventionsmaßnahmen.

7. Weitere Neuerungen

Die neue Version der Allgemeinen Versicherungsbedingungen weist detailliertere und spezifischere Ausschlüsse, bzgl der Verletzung von Immaterialgüterrechten (A1–17.11 AVB Cyber) und Diskriminierung (A1–17.13 AVB Cyber), auf. Seit der Aktualisierung ermöglichen die AVB Cyber flexiblere Vertragslaufzeiten und bieten Optionen für kürzere oder längere Vertragszeiträume (B1–1 AVB Cyber). Zudem werden detaillierte Regelungen für Zahlungsausfälle getroffen und die damit verbundenen Rechte und Pflichten der VN und des VR (B1–3 AVB Cyber).

Schlussstrich

Die Änderungen sind weitaus zögerlicher ausgefallen, als dies seitens der Wissenschaft und Praxis gewünscht bzw gefordert wurde, es sind allerdings einige Klarstellungen getroffen worden. Die Obliegenheiten und Risikoausschlüsse in beiden Versionen fallen weitestgehend ähnlich bzw gleichlautend aus. Lediglich die Kriegsklausel wurde einer eher kosmetischen als inhaltlichen Umgestaltung unterzogen. Das neue Bedingungswerk erhebt den Anspruch, detaillierter und spezifischer in seinen Bestimmungen zu sein, und enthält an mancher Stelle zusätzliche Regelungen, die im älteren Bedingungswerk weniger stark ausgeprägt sind.

RECHTSPRECHUNG

Bearbeitet von Alexander Höller

Örtliche Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet

ecolex 2024/412

§ 92b JN; Art 7 Z 2 EuGVVO

OGH 26. 4. 2024, 6 Ob 30/24s

Persönlichkeitsrechtsverletzung; Zuständigkeit; Gerichtsstand; Erfolgsort; Handlungsort; Ubiquitätstheorie; Mosaiktheorie; Löschung; Facebook; Meta; TikTok; Google; Twitter; X; kununu; DocFinder

1. § 92b JN ist eine innerstaatliche Parallelnorm zu Art 7 Z 2 EuGVVO für jene Fälle, die nicht in den Anwendungsbereich der EuGVVO (oder des LGVÜ) fallen.

2. Eine Person kann eine Klage wegen behaupteter Persönlichkeitsrechtsverletzungen im Internet auf Ersatz des gesamten entstandenen Schadens sowie auf Widerruf unwahrer und beleidigender Äußerungen einschließlich deren Veröffentlichung entweder vor dem (sachlich zuständigen) Gericht des Orts, an dem der Urheber dieser Inhalte seinen Wohnsitz oder Sitz hat, oder vor dem (sachlich zuständigen) Gericht des Orts, an dem sich der Mittelpunkt ihrer Interessen befindet, erheben.

Sachverhalt:

Der Bekl [ist] Inhaber eines Facebookprofils. Er [hat] dort als Teilnehmer eines „Shitstorms" gegen den Kl eine bei der besagten Demonstration ohne dessen Zustimmung von ihm angefertigte Bildaufnahme mitsamt einem rufschädigenden und ehrenbeleidigenden Begleittext veröffentlicht.

Der Bekl schulde ihm daher den begehrten immateriellen Schadenersatz, habe die unwahren und beleidigenden Behauptungen zu widerrufen und diesen Widerruf zu veröffentlichen.

Die örtliche Zuständigkeit ergebe sich aus § 92b JN. Alle Berufskollegen des Kl, die mit ihm im Einsatz standen und in Tirol wohnen, könnten ihn auf dem Bild erkennen, die Veröffentlichungen abrufen und einen unwahren, jedoch schlechten Eindruck vom Kl bekommen.

Der Bekl erhob die Einrede der örtlichen Unzuständigkeit. Der Kl habe seinen Lebensmittelpunkt in Kärnten, daher liege der Ort des schädigenden Ereignisses iSv § 92b JN dort.

Entscheidungsgründe:

Im RevRekVerfahren ist ausschließlich strittig, ob das angerufene ErstG aufgrund von § 92b JN örtlich zuständig ist.

Gem § 92b JN idF der ZVN 2022 (BGBl I 2022/61) können Streitigkeiten wegen Verletzung eines Persönlichkeitsrechts in einem elektronischen Kommunikationsnetz auch bei dem Gericht angebracht werden, in dessen Sprengel das schädigende Ereignis eingetreten ist oder einzutreten droht.

Nicht strittig ist, dass die geltend gemachten Ansprüche von § 92b JN umfasst sind und sich der Rechtsstreit auf die Verletzung von Persönlichkeitsrechten in einem elektronischen Kommunikationsnetz bezieht (vgl dazu auch *Kustor/Prossinger* in *Kodek/Oberhammer,* ZPO-ON § 92b JN Rz 4, 5).

Das angerufene Gericht ist gem § 92b JN aber nur dann örtlich zuständig, wenn in dessen Sprengel die behauptete Persönlichkeitsrechtsverletzung eingetreten ist oder einzutreten droht.

Nach den Mat war Art 7 Nr 2 […] EuGVVO 2012 Vorbild für § 92b JN. Der Gesetzgeber wollte eine innerstaatliche Parallelnorm für jene Fälle schaffen, die nicht in den Anwendungsbereich der EuGVVO 2012 fallen (vgl ErlRV 1291 BlgNR 27. GP 5).

Gem Art 7 Nr 2 EuGVVO 2012 besteht bei Ansprüchen aus unerlaubten Handlungen ein Wahlgerichtsstand vor dem Gericht des Orts, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht.

Mit der Wendung „Ort, an dem das schädigende Ereignis eingetreten ist" ist nach der Rsp des EuGH sowie des OGH sowohl der Ort der Verwirklichung des Schadenserfolgs (Erfolgsort) als auch der