Port7

hüneborn | it

Haftungsfalle eRechnung an Verbraucher:

Neuere Rechtsprechung zum ungeschützen eMailversand von Rechungen

Artikel von Jürgen Hüneborn | Fachanwalt für IT-Recht in Münster

25.04.2025

Seit dem 1. Januar 2025 gilt die sogenannte e-Rechungspflicht für alle inländischen Unternehmer in Deutschland, die keine Kleinunternehmer sind. Seit diesem Termin müssen sie zumindest passiv in der Lage sein, e-Rechnungen zu empfangen und zu verarbeiten. Die elektronische Rechnungsstellung ist seitdem nicht mehr an die Zustimmung des Empfängers geknüpft.

Es ist daher verständlich, dass seit diesem Datum der Rechnungsversand per eMail noch einmal zugenommen hat. Wie sollte man die e-Rechnung sonst auch sinnvoll versenden?

Zwei interessante OLG-Urteile aus 2023 und Ende 2024, von denen das zweite seit einiger Zeit nun auch rechtskräftig geworden ist, werfen jedoch **haftungstechnisch** einige Fragen auf, derer sich **Unternehmer** bewusst sein sollten.

Den meisten Unternehmern ist zwar klar, daß eMails grundsätzlich als "unsicheres Medium" für den Versand personenbezogener und auch sonstiger Daten gelten müssen, da sie aus sich heraus weder Aufschluss darüber geben, wer sie auf dem Transportweg gelesen hat, ob sie verändert wurden und ob sie überhaupt vom angeblichen Absender stammen. Welche und ob überhaupt Schlußfolgerungen daraus für den Versand elektronischer Rechnungen per eMail gezogen werden müssen, wurde bislang jedoch selten erörtert. Die meisten Unternehmer standen auf dem Standpunkt: Kommt die eMail mit der Rechnung nicht an, sende ich sie eben noch einmal.

Eine (grundsätzliche) Pflicht zur Durchführung technischer Schutzmaßnahmen beim eMailversand ergibt sich aus Art. 32 DSGVO und betrifft z.B. Anwälte und Ärzte in der Mandanten- und Patientenkommunikation. Der Art. 32 DSGVO wurde jedoch immer so verstanden, daß ich - wenn ich eMails zur Übersendung von Daten nutze - um so mehr technische "Zusatzmaßnahmen" treffen muß, je **intensiver und wichtiger** die kommunizierten personenbezogenen Daten sind.

Bei uns Anwälten war es z.B. so, daß wir Dinge wie eine Terminsbestätigung oder das Übersenden leerer Vollmachtsformulare problemlos per eMail machen durften, daß wir aber z.B. auch mit Einwilligung des Mandanten keine Daten wie Gesundheitsdaten, Mitarbeiterlisten oder ähnliches versenden durften. Alles andere war dann irgend wie so "dazwischen"; Rechnungen und "normale" Schriftstücke wurden entsprechend per eMail

versendet, wenn der Mandant das wünschte. Und meistens wünscht er das. Es gab und gibt aber keine gesetzliche Vorgabe die genau regelt, ab welchem Punkt der kommunizierte Inhalt so relevant ist, daß auf jeden Fall ein zusätzlicher Schutz benötigt wird.

Das OLG Schleswig Holstein sagt nun aber in der Entscheidung [12 U 9/24]:

> Nicht nur die Intensität und Wichtigkeit der kommunizierten personenbezogenen Daten sind ausschlaggebend, sondern auch die **Wahrscheinlichkeit und Höhe** eines Schadenseintritts. Also bei hoher Wahrscheinlichkeit des Eintritts eines erheblichen Schadens brauchen die kommunizierten Daten keine besondere Wichtigkeit gehabt haben.

Was war passiert?
Der vom OLG entschiedene Fall betraf den offenen Versand einer Rechnung im PDF-Format per eMail von einem Bauunternehmer an einen privaten Bauherren. Die Rechnung hatte einen Betrag von 15.000,- €.
Unter ungeklärten Umständen war die eMail des Unternehmers von Onlinebetrügern abgefangen und verändert worden; in dem PDF-Dokument, dass dem Bauherren schließlich vorlag, fand sich eine geänderte Kontoverbindung wieder. Ebenso waren bestimmte Attribute der Mail verändert worden, wie Schriftfarbe und Fontart.
Dem Bauherren kam dies jedoch nicht verdächtig vor; er nahm die geänderte Kontoverbindung zwar zur Kenntnis, überwies den Betrag jedoch ohne Rückfrage an die neue Kontoverbindung (…die in Wahrheit natürlich den Betrügern und nicht dem Bauunternehmer gehörte). Diese Art von Rechnungsscam kommt allein in Deutschland täglich hunderte Male vor.

Der Unternehmer verlangte nun erneute Zahlung an seine „richtige“ Kontoverbindung; der Bauherr meinte, schuldbefreiend bereits an Dritte geleistet zu haben. Das Ausgangsverfahren vor dem Landgericht gewann der Bauunternehmer.
In der Berufung vor dem OLG wurde die Entscheidung aufgehoben und die Klage abgewiesen. Hier trug der Anwalt des Bauherren vor, sein Mandant habe zwar nicht schuldbefreiend geleistet, er könne jedoch die sog. „dolo-agit“-Einrede erheben, da er einen Schadensersatzanspruch gegen den Bauunternehmer in gleicher Höhe habe.

Die Entscheidung
Das OLG stützt seine Entscheidung auf Art. 82 der DSGVO in Verbindung mit Art. 32 DSGVO und der dolo-agit-Einrede aus § 242 BGB (unzulässige Rechtsausübung).

Der elektronische Versand der Rechnung als eMail stellt nämlich neben der Übermittlung der eigentlichen Rechnungsdaten auch eine Übermittlung personenbezogener Daten (Name, Anschrift, Leistungsadresse, ggfs. nähere Umstände wie Zeiträume der Leistung etc.) dar. Dies um so mehr, als die Rechnung an einen Verbraucher gestellt wird, der in der Regel diese mit seinem bürgerlichen Namen + Anschrift empfängt.
Bei der Verarbeitung solcher Daten ist gem. Art. 32 DSGVO immer eine Abwägung hinsichtlich der Sicherheit der Verarbeitung zu treffen: Unter Berücksichtigung des Standes der Technik, Kosten, Umfang, Umstände, Zwecke der Verarbeitung und Verkehrserwartung muß der Verantwortliche „geeignete“ technische und

organisatorische Maßnahmen (allg. „TOMs“ genannt) treffen, um ein **dem Risiko angemessenes Schutzniveau** sicherzustellen.
Der Unternehmer konnte hier nicht beweisen, dass er überhaupt eine Risikoabwägung getroffen habe. So behauptete er zwar, die eMail sei aufgrund seines Providers mit einer Transportverschlüsselung (TLS) versehen gewesen. Dies konnte er allerdings nicht beweisen. Das OLG sah zudem eine reine Transportverschlüsselung als von vorn herein ungeeignete Maßnahme iSd. Art. 32 DSGVO an. So schützt die TLS-Verschlüsselung nur auf dem Transportweg zwischen zwei Knotenpunkten, nicht aber gegen Kenntnisnahme an diesem Knotenpunkt. Dies verhindert nur eine Ende-zu-Ende-Verschlüsselung.
Das Gericht führte zudem aus, dass es allgemeine Risiko des Abfangens einer eMail aufgrund der Vielzahl der bekannten Fälle durchaus mit „hoch“ bewertet. Ebenso sei der mögliche Schadenseintritt bei einem Rechnungsbetrag von 15.000,- € ebenfalls mit „hoch“ einzustufen.
Da von den beiden Faktoren "Wahrscheinlichkeit und Höhe" der erste praktisch immer gleich ist - also es ist mehr oder weniger immer gleich wahrscheinlich, daß eine konkrete eMail zufällig zum Ziel von Betrügern wird - dreht sich bei der Abschätzung letztlich alles um den zweiten Faktor: Mögliche Schadenshöhe. Diese wird man also in Anwendung der Logik des OLG ab einem Betrag von einigen tausend € ebenfalls immer mit „hoch“ bewerten müssen.
Schließlich lehnte das OLG noch eine Teilzahlung aufgrund von Mitverschulden gem. § 254 BGB ab. Zwar seien dem Beklagten Änderungen zu vorherigen Abschlagsrechnungen aufgefallen. Angesichts der Tatsache, dass sich Kontoverbindungen im Geschäftsleben aus diversen Gründen ändern könnten, könnte zumindest einem privaten Kunden nicht vorgeworfen werden, vor der Zahlung keine Rücksprache mit dem Unternehmer gehalten zu haben.

Aufgrund der somit fehlerhaften Verarbeitung personenbezogener Daten (Absenden der eMail ohne Risikoabschätzung und Einhaltung von TOMs) stehe dem Beklagten ein Schadensersatzanspruch aus Art. 82 DSGVO in gleicher Höhe zur Zahlungsforderung des Klägers zu. Diesen konnte er im Rahmen der dolo-agit-Einrede dem (nicht erloschenen) Zahlungsanspruch des Klägers entgegenhalten.

<u>Folgen</u>
Nach dem Ergebnis dieser Rechtsprechung sind bei größeren Rechnungsbeträgen somit praktisch immer zusätzliche Schutzmaßnahmen beim eMailversand erforderlich, um einer etwaigen Haftung zu entgehen. Denn: Das OLG "verbietet" ja nicht den Versand, sondern sagt lediglich: Man begibt sich in einer Schadensersatzhaftung gem. Art. 82 DSGVO, sofern man es einem nicht gelingt, die Einhaltung zusätzlicher, erforderlicher Schutzmaßnahmen nachzuweisen.
Auf Mitverschulden des Verbrauchers kann man kaum setzen; das OLG hat ja jetzt bereits klargestellt, daß allein eine abweichende Kontoverbindung kein solches Mitverschulden begründet. Der Kunde/Rechnungsempfänger muß also nicht alleine aufgrund der geänderten Kontoverbindung mißtrauisch werden, sondern nur, wenn noch weitere Aspekte hinzutreten. Solche Aspekte können etwa ungewöhnliche Formulierungen im Anschreiben, ungewöhnliche andere Zahlungsmethoden, Bankverbindungen im Ausland oder seltsame eMail-Adressen sein. Diese müßten dann allerdings auch vom Kläger bewiesen werden.

Schutzmaßnahmen / TOMs

Das OLG hat ebenfalls klargestellt, daß es nicht den Versand der Rechnung per eMail infrage stellt, sondern lediglich den Versand "ohne Risikoabschätzung und Zusatzmaßnahmen", die es im Bereich der datenschutzrechtlichen TOMs angesiedelt sieht. Zu solchen Maßnahmen zählen technische (wie Verschlüsselung) aber auch organisatorische Maßnahmen (etwa Abgleich auf einem zweiten Kommunikationsweg), die einen Schutz und die Integrität der Daten sicherstellen. Der einfachen Transportverschlüsselung (TLS) hat das OLG aber bereits eine Absage erteilt, die reicht also nicht.

Als technische und organisatorische Maßnahmen kämen – je nach Risikobewertung und -abschätzung somit generell infrage:

- PGP-Verschlüsselung der ganzen eMail
- S/MIME-Verschlüsselung der ganzen eMail – hier ist jedoch darauf zu achten, dass nicht versehentlich lediglich Transportverschlüsselung aktiviert wird.
- unverschlüsseltes Senden der Mail mit verschlüsseltem Anhang, etwa ZIP-Archiv
- unverschlüsseltes Senden der Mail ohne Anhang aber mit Rechnungslink, der auf eine gegen Veränderung gesicherte Cloud verweist (z.B. nextCloud-Dateien) – Problem: Der Link könnte gefälscht werden
- Verweis auf eine Online-Rechnungsplattform zum "runterladen" der Rechnung
- Fraglich: Versenden der eMail mit gegen Veränderung gesperrtem PDF-Anhang oder signiertem PDF, das widerspricht allerdings wiederum dem PDF/A-Format, was nach den GOBD zu nutzen wäre. Ebenso unklar, ob hier jede Software-Lösung mit dem „ZugFerd“-Format der eRechnung arbeitet
- Versenden der Rechnung per eMail *und* auf einem zweiten Kommunikationsweg, so daß vor Zahlung der Inhalt abgeglichen werden kann
- Letztlich wäre eine rein organisatorische Maßnahme, die zumindest die Integrität der Kontodaten sicherstellt, auch die Zahlung per ELV ("Lastschrift"), ggfs. mit anschließender Bestätigung.

Welche dieser Maßnahmen anzuwenden ist und ob z.B. durch eine bewußte Freizeichnung seitens des Kunden darauf verzichtet werden kann, ist einerseits umstritten, andererseits risikoabhängig.

Und was gilt für B2B, also zwischen Unternehmen gestellten Rechnungen?

Nun könnte man denken, dass diese Bedenken lediglich auf B2C-Verhältnisse anwendbar wären.

Hier kommt jedoch die ältere Entscheidung des OLG Karlsruhe vom 27. Juli 2023 (Az. 19 U 83/22) ins Spiel. Dort hatte das Gericht in einem Rechtsstreit, der zwei Unternehmer betraf, zwar ebenfalls darauf hingewiesen, daß es keine gesetzlichen Vorgaben für konkrete Sicherungsmaßnahmen gibt. Es kam dann aber zu dem Schluß, daß maßgeblich "die berechtigten Sicherheitserwartungen des jeweiligen Geschäftsverkehrs" seien. Hier wäre natürlich Raum für das Argument, daß der entsprechende Geschäftsverkehr z.B. keine Verschlüsselung erwartet.

Allerdings stellte auch das OLG Karlsruhe wie jetzt das OLG Schleswig Holstein fest:

> *"Verstößt der Gläubiger einer Geldforderung gegen von ihm geschuldete Sicherheitsvorkehrungen im Zusammenhang mit dem Versand einer geschäftlichen E-Mail und hat dieser Verstoß zur Folge, dass der Schuldner der Forderung den geschuldeten Geldbetrag auf das Konto eines deliktisch handelnden Dritten überweist, führt dies nicht zum Erlöschen der Forderung gemäß § 362 BGB, sondern begründet allenfalls einen Schadensersatzanspruch des Schuldners, den dieser gemäß § 242 BGB der Forderung entgegenhalten kann (dolo-agit-Einwendung)."*

Man ist damit also keineswegs "aus dem Schneider", sondern es kann durchaus passieren, daß ein Gericht auch im B2B-Bereich die konkret getroffenen Maßnahmen als für zu gering erachtet und auch dem gewerblichen Schuldner die "dolo-agit"-Einrede erlaubt, so daß er nicht ein zweites Mal zu zahlen braucht.
Das gilt um so mehr, als wir jetzt das "neue" Urteil des OLG Schleswig Holstein haben. Da könnten gewerbliche Schuldner auch im B2B-Verhältnis auf den Gedanken kommen zu sagen: "Meine berechtigte Sicherheitserwartung war allerdings das, was das OLG Schleswig entschieden hat!". Die Situation Rechnungsversand per ungesicherter eMail ist daher aus meiner Sicht auch für den B2B-Bereich mindestens mit erheblicher Unsicherheit behaftet. Theoretisch ausgenommen wären lediglich B2B-Rechnungen, die keinerlei personenbezogene Merkmale enthalten, da hier ein Anknüpfungspunkt an die DSGVO fehlt. Es besteht jedoch das Risiko, dass Gericht hier mit der Verletzung von vertraglichen Sorgfalts- und Nebenpflichten argumentieren, die das OLG Schleswig-Holstein zwar nicht geprüft, aber ausdrücklich offengelassen hat.

<u>Fazit</u>
Nach der aktuellen obergerichtlichen Rechtsprechung, die aufgrund zweier praktisch gleichlautender Entscheidungen als „ständige Rechtsprechung“ angesehen werden kann, besteht die Gefahr der Schadensersatzhaftung für betrügerisch veränderte e-Rechnungen, die ohne weitere Schutzmaßnahmen (TOMs) per einfacher eMail versandt wurden und vom Rechnungsempfänger fälschlich an eine fremde Kontoverbindung bezahlt wurden. Dabei wird im Rahmen des Mitverschuldens prozentual die ggfs. beiderseitige Fahrlässigkeit berücksichtigt.

Dabei ist v.a. die Höhe des potentiell zu erwartenden Schadens – also des Rechnungsbetrages – zu berücksichtigen: Je höher dieser ist, um so eher müssen Maßnahmen ergriffen werden.

In allen IT-rechtlichen und markenrechtlichen Fragestellungen berät Sie gerne:

Port7 Rechtsanwälte
Jürgen Hüneborn, Rechtsanwalt, Fachanwalt für IT-Recht
hueneborn@port7.de
Am Mittelhafen 16, 48155 Münster
0251 – 203 188 00

www.port7.de