Kommunikation & Recht

K&R
4 April 2025
28. Jahrgang
Seiten 217 -288

Chefredakteur
RA Torsten Kutschke

Stellvertretende Chefredakteurin
RAin Dr. Anja Keller

Redakteur
Dr. Maximilian Leicht

Redaktionsassistentin
Stefanie Lichtenberg

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

Anhang III KI-VO spezifisch sind. Dieser Maßstab gilt nach ErwG 128 KI-VO explizit für den Fall einer wesentlichen Veränderung eines Hochrisiko-KI-Systems i. S. v. Art. 25 Abs. 1 lit. b KI-VO und kann hier entsprechend übertragen werden.

2. Beispiel: Unternehmenseigenes HR-Tool auf Basis eines LLMs

Geht es beispielsweise bei der Verwendung eines LLMs im Kern nicht mehr um die Ein- und Ausgabe von Text in natürlicher Sprache, sondern um die Vorfilterung von Bewerbungen (Anhang III Nr. 4 lit. a KI-VO), liegt typischerweise eine relevante Zweckänderung vor, selbst wenn dabei weiterhin Text verarbeitet wird. Denn die reine „Textverarbeitung" mithilfe eines LLMs trägt im Ausgangspunkt nicht das Diskriminierungs- und Schadenspotenzial in sich, das mit dem Einsatz von KI im Beschäftigungskontext verbunden ist. Es handelt sich wertungsmäßig daher um ein neues (Hochrisiko-)KI-System.

Timo Bosman
Jahrgang 1993; Studium an der Universität Heidelberg, Referendariat in Hamburg und Brüssel; seit 2022 RA bei Osborne Clarke in Hamburg; Schwerpunktbereiche: Daten- und KI-Recht.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

E-Rechnung: Verschlüsseln oder Signieren?

Kurz und Knapp

Das OLG Schleswig-Holstein hat entschieden, dass E-Mails, die eine Rechnung an Verbraucher übermitteln, Ende-zu-Ende zu verschlüsseln sind. Das schütze die Rechnung vor Manipulationen und den Kunden vor Fehlüberweisungen. Die Autoren prüfen, ob diese Aussage technisch korrekt ist. Zudem wirft das Urteil im Kontext der E-Rechnung erhebliche Fragen auf, zumal die derzeit verfügbaren Formate XRechnung und ZUGFeRD gravierende Sicherheitslücken aufweisen.

I. Entscheidung des OLG Schleswig-Holstein

Das Urteil des OLG Schleswig-Holstein vom 18. 12. 2024[1] fordert Ende-zu-Ende-Verschlüsselung für den Rechnungsversand per E-Mail jedenfalls gegenüber natürlichen Personen bzw. Verbrauchern. Welche Konsequenzen hat das Urteil für die E-Mail-Kommunikation im Allgemeinen und im Besonderen für den Versand verpflichtender „E-Rechnungen", die § 14 Abs. 2 UStG zum 1. 1. 2025 eingeführt hat?

Dieser Abschnitt stellt die OLG-Entscheidung dar, darauf aufbauend untersucht Abschnitt II, ob die technischen Annahmen des OLG dessen rechtliche Beurteilung tragen.

Abschnitt III stellt dar, wie sich das Urteil zu einer Entscheidung des OLG Karlsruhe aus dem Jahr 2023 verhält, das keine Pflicht zur Ende-zu-Ende-Verschlüsselung einer PDF-Rechnung sah, weil dies die „Sicherheitserwartungen des Verkehrs" nicht erfordern würden.[2]

Abschnitt IV untersucht die Relevanz der Entscheidung für die E-Rechnung mit den Formaten „XRechnung" und „ZUGFeRD" und zeigt dabei zwei Sicherheitslücken in diesen Formaten.

Das OLG hat die Klage eines Unternehmers gegen einen Verbraucher auf Zahlung von Werklohn abgewiesen. In der Rechnung über € 15 385,78, die dem Verbraucher als PDF-Datei per E-Mail zuging, hatte ein Unbekannter die Bankverbindung verändert. Der Beklagte hat daher auf das Konto eines Dritten überwiesen.

Die Vorinstanz hatte den Beklagten zur erneuten Zahlung verurteilt. Auf das Konto aus der manipulierten Rechnung zu überweisen, habe die Zahlungspflicht nicht erfüllt. Durch „Transportverschlüsselung" sei die E-Mail im Sinne der Artt. 5 Abs. 1 lit. f, 32 DSGVO ausreichend gegen unbefugte Dritte geschützt.

Diese Auffassung lehnte das OLG unter Berufung auf die Orientierungshilfe der Datenschutzkonferenz vom 27. 5. 2021[3] und die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ab:[4]

Der Beklagte habe durch die Überweisung seine Zahlungspflicht zwar nicht erfüllt; er könne die Zahlung jedoch nach dem „Dolo-agit-Einwand" verweigern, weil er aus Art. 82 DSGVO einen Schadensersatzanspruch gegen den Kläger in gleicher Höhe habe. Die vom Kläger genutzte „Transportverschlüsselung" beim E-Mail-Versand der Rechnung sei ungeeignet, um die personenbezogenen Daten des Beklagten gemäß Art. 32 DSGVO zu schützen. Dies gelte jedenfalls dann, wenn dem Empfänger als „Privatkunde" wie hier hohe finanzielle Risiken durch eine Modifikation der Rechnung drohen. Vielmehr sei die Ende-zu-Ende-Verschlüsselung das Mittel der Wahl. Sei das nicht möglich, bleibe der Versand der Papierrechnung per Post.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 1. 3. 2025.

1 OLG Schleswig-Holstein, 18. 12. 2024 – 12 U 9/24, K&R 2025, 272 ff. (in diesem Heft).

2 OLG Karlsruhe, 27. 7. 2023 – 19 U 83/22, K&R 2023, 607, 610; kritisch dazu *Deusch/Eggendorfer*, K&R 2024, 242, 244.

3 https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf. Unter der „Datenschutzkonferenz" (DSK) treffen die Datenschutzbehörden in Deutschland Beschlüsse zur einheitlichen Anwendung der gesetzlichen Datenschutzvorgaben (https://www.datenschutzkonferenz-online.de/dsk.html).

4 Abschnitt II der Urteilsgründe, insbesondere Ziffer 2., a), bb), (1), (cc), (ccc), sowie die BSI-Empfehlungen: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationenund-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html.

Trotz Zulassung der Revision ist das Urteil gemäß Auskunft des OLG gegenüber den Verfassern zwischenzeitlich rechtskräftig.

II. Technische Fragen: Vorgehen der Täter und Gegenmaßnahmen

Manipulierte elektronische Rechnungen, meist per E-Mail im PDF-Format versendet, treten jüngst vermehrt auf.[5] Die Täter tauschen die Bankverbindung des Rechnungsstellers aus, so dass die Überweisung dort eingeht. Wo genau diese Angriffe passieren, bleibt wie auch im vorliegenden Fall regelmäßig ungeklärt. Es gibt mehrere mögliche Angriffsvektoren:

- Mitarbeiter des Auftragnehmers könnten als Insider die Rechnung vor dem Versand ändern.
- Dritte könnten die E-Mail mit der Rechnung während des Zwischenspeicherns beim Versand auf dem Server des Providers des Absenders verändern.
- Ebenso könnten Dritte die E-Mail während der Speicherung auf dem Mailserver des Providers des Rechnungsempfängers manipulieren. Dieser Angriff bietet technisch den Vorteil, dass die E-Mails dort meist länger lagern.
- Auch beim Scan auf Schadsoftware könnten Angreifer die Rechnung sowohl beim Versender als auch Empfänger manipulieren.
- Außerdem könnte Schadsoftware die Rechnung beim Rechnungsempfänger manipulieren.[6]

Der hohe technische Aufwand (unten IV) scheint sich vorliegend bei erbeuteten ca. € 15 000 zu lohnen.

1. Gegenmaßnahmen

Laut OLG Schleswig-Holstein hätte der Absender durch Ende-zu-Ende-Verschlüsselung den Schaden verhindern können.[7] Wenngleich die Autoren dem Senat beim Wunsch nach Verschlüsselung im rechtlichen Ergebnis folgen (unten Abschnitt III), sind die verschiedenen IT-Sicherheitsziele bei der Datenübertragung zu unterscheiden: Vertraulichkeit, Integrität und Authentizität.[8]

a) Vertraulichkeit

Unabhängig von den Zielen Integrität und Authentizität steht die Vertraulichkeit. Sie stellt sicher, dass kein Unberechtigter vom Inhalt der Kommunikation Kenntnis erlangt. Das erreicht Verschlüsselung – schon Cäsar nutzte sie. Er ersetzte jeden Buchstaben durch den ihm z. B. drei Stellen weiter im Alphabet folgenden.[9] An diesem einfachen Verfahren lässt sich gut Algorithmus und Schlüssel unterscheiden: Das Alphabet zu verschieben ist der Algorithmus, drei – die Verschiebung – der Schlüssel.

Das Verfahren ist symmetrisch: Zum Ver- und Entschlüsseln dient derselbe Schlüssel. Das schafft das Problem des Schlüsselaustauschs zwischen Sender und Empfänger, kann den ein Dritter abgreifen, ist der Schutz der Verschlüsselung dahin.

Asymmetrische Verfahren nutzen zwei verschiedene, mathematisch voneinander abhängige Schlüssel: Den öffentlichen und den privaten. Der Absender verschlüsselt mit dem öffentlichen Schlüssel des Empfängers die Nachricht, der (und nur der) sie mit seinem privaten Schlüssel entschlüsseln kann. Der private Schlüssel ist schützenswert, der öffentliche dagegen darf z. B. auf der Webseite stehen.[10]

b) Integrität

Integrität bedeutet, dass eine Nachricht den Empfänger unverändert erreicht.[11] Dabei gibt es verschiedene Fehlermöglichkeiten: Zufällige Übertragungsfehler, bildlich das Rauschen im Radio. Dagegen helfen einfache Prüfsummen wie z. B. in der IBAN: Die ersten beiden Ziffern hinter der Länderkennung errechnen sich aus den einzelnen Ziffern der restlichen IBAN. Zufällige Tipp- oder Übertragungsfehler lassen sich so detektieren, sie schützt aber nicht vor Manipulationen wie im Fall des OLG Schleswig-Holstein. Jeder, der den Algorithmus kennt, kann zu einer Prüfsumme eine gültige IBAN konstruieren.

Daher sind Prüfsummen nötig, die auch gegen böswillige Angreifer robust sind: kryptographisch sichere Hash-Verfahren.[12] Deren erzeugte Prüfsumme ist wesentlich länger als die beiden Ziffern in der IBAN. Bei gängigen Verfahren sind die Prüfsummen zwischen 128 und 512 Bit lang, als Dezimalzahlen ca. 38 bis 154 Stellen. Sie sind zudem kollisionsresistent: Für ein Datum mit einem gegebenen Hashwert ist es praktisch unmöglich, ein Zweites mit demselben Hashwert zu finden.

Möchte also A an B Daten so senden, dass B sicher sein kann, dieselben Daten zu erhalten, würde A die Daten und den darüber berechneten Hashwert an B schicken. B berechnet selbst nochmal einen Hashwert mit demselben Algorithmus. Sind die beiden Hashwerte identisch, sind die Daten unverändert. Soweit unterwegs niemand den Hashwert manipulieren konnte – ihn müsste der Absender daher wenig praktikabel auf einem gesonderten Weg übertragen.

Ein kleiner Trick hilft: Um den Hashwert beim Übertragen zu schützen, bietet es sich an, asymmetrische Verschlüsselung in abgewandelter Form zu nutzen. Der Absender verschlüsselt nur den Hashwert mit seinem privaten Schlüssel. Dann kann jeder, also auch der Empfänger, mit dem öffentlichen Schlüssel des Absenders den Hashwert wieder entschlüsseln und mit dem selbst errechneten vergleichen. Hätte wer anders als der Absender den Hashwert verschlüsselt, lässt er sich mit dessen

5 Siehe z. B. die Warnung der IHK Ulm https://www.ihk.de/ulm/online-magazin/vermehrt-manipulierte-digitale-rechnungen-im-umlauf-6199380 und den Bericht des NDR 1: https://www.ndr.de/nachrichten/schleswig-holstein/Cyber-Betrug-Perfide-Masche-mit-falschen-Rechnungen-in-SH,betrug524.html.

6 Unabhängig vom Angriffsweg deuten die Tatkomplexe auf arbeitsteilige Kriminalität hin.

7 Abschnitt II Ziffer 2., a), bb), (1), (cc), (ccc) der Urteilsgründe: „End-to-End-Verschlüsselung zurzeit das Mittel der Wahl“, um personenbezogene Daten bei dem „hier bestehenden Risiko durch Verfälschung der angehängten Rechnung“ zu schützen.

8 Vertraulichkeit, Integrität und Authentizität sind grundlegende Konzepte der IT-Sicherheit, wer sich damit en detail beschäftigen möchte, kann neben den Quellen in den Fußnoten dieses Beitrags auch nachlesen in Werken wie z. B. *Friedrich Ludwig Bauer*, Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie, 2000, *Albrecht Beutelspacher*, *Jörg Schwenk*, *Klaus-Dieter Wolfenstetter*, Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge und darüber hinaus, 2022, sowie auch die Ausführungen in *Deusch/Eggendorfer*, Beauftragte für Informationssicherheit und IT-Sicherheit, 2024, Ziffer 2.2 (S. 14 ff.) sowie *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 39. Ergänzung, 2024, Kap. 50.1 Rn. 6 und 16 - 30.

9 Online lässt sich das mit https://www.cryptool.org/en/cto/caesar/ nachvollziehen.

10 Zum Schutzziel der Vertraulichkeit und zur Verschlüsselung siehe *Deusch/Eggendorfer* (Fn. 8), Ziffer 2.2.1 und 2.3.1.

11 *Deusch/Eggendorfer* (Fn. 8), Ziffer 2.2.2, S. 14; *dieselben*, in: Taeger/Pohle, Computerrechts-Handbuch (Fn. 8), Kap. 50.1 Rn. 18.

12 *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch (Fn. 8), Rn. 19; *dieselben*, Beauftragte für Informationssicherheit und IT-Sicherheit (Fn. 8), Ziffer 2.2.2; *Eggendorfer*, Hashes, Salz und Pfeffer, Linux Magazin 10/2015, https://www.linux-magazin.de/ausgaben/2015/10/hashfunktionen/.

öffentlichen Schlüssel nicht mehr korrekt entschlüsseln, die Manipulation ist offensichtlich.

Wichtig ist der Unterschied zu oben lit. a: Geht es beim Verschlüsseln um Vertraulichkeit, nutzt der Absender den öffentlichen Schlüssel des Empfängers und dieser seinen privaten Schlüssel zum Entschlüsseln.

Diese geschützte Prüfsumme nennt die Informatik „digitale Signatur". Sie stellt ausschließlich die Integrität der Nachricht sicher, nicht die Vertraulichkeit.

Die juristische Sicht auf digitale Signaturen bildet die eIDAS-VO[13] in drei Stufen ab: Die erste Stufe ist ein E-Mail-„Abbinder", der den Absender angibt („Elektronische Signatur" gemäß Art. 3 Nr. 10 eIDAS-VO). Technisch erreicht das weder Authentizität noch Integrität und ist insofern zum „Unterzeichnen" völlig ungeeignet, darüber hinaus leicht zu fälschen; der Terminus „Signatur" ist irreführend. In der zweiten Stufe wird eine Signatur nach dem hier beschriebenen Verfahren berechnet („Fortgeschrittene elektronische Signatur" gemäß Art. 3 Nr. 11 eIDAS-VO), die dritte Stufe („Qualifizierte elektronische Signatur" gemäß Art. 3 Nr. 12 eIDAS-VO) ergänzt dieses Verfahren um die Identitätsprüfung des Absenders durch einen Vertrauensdiensteanbieter. Dieser vergibt z. B. Chipkarten („Qualifizierte elektronische Signaturerstellungseinheit" gemäß Art. 3 Nr. 23 eIDAS-VO), die sicherstellen sollen, dass nur berechtigte Personen die Signatur erstellen können.

c) Authentizität

Weil der Absender den Hashwert mit seinem privaten Schlüssel verschlüsselt hat, auf den nur er Zugriff hat, ist auf den ersten Blick klar, wer der Absender sein muss. Doch dafür ist ein System nötig, das die Schlüsselpaare aus öffentlichen und privaten Schlüsseln eindeutig einem Nutzer zuordnet.[14]

Damit wird der Schlüssel eine Art „digitaler Ausweis". Der Schlüsselinhaber gewinnt Vertrauen, weil eine vertrauenswürdige Stelle den Ausweis fälschungssicher herausgegeben hat.

Im Kern gibt es in der digitalen Welt als „vertrauenswürdige Stelle" zwei Varianten: Das von PGP bzw. GnuPG/GPG[15] propagierte Web-of-Trust,[16] bei dem Nutzer gegenseitig die Echtheit verifizieren. Interessant ist dabei das Angebot von Governikus,[17] das den elektronischen Personalausweis zum Verifizieren nutzt. Alternativ ist eine zentrale Ausgabestelle, wie zum Beispiel im Bereich der Hochschulen das Deutsche Forschungsnetz (DFN). Diesen Ansatz nutzt z. B. S/MIME.

Das unabhängige Web-of-Trust steht jedermann kostenlos zur Verfügung, wohingegen S/MIME-Zertifikate üblicherweise gebührenpflichtig sind.[18] Eine ähnliche Idee verfolgen Chip-Karten oder vergleichbare Systeme zur Signaturerstellung, die eine vertrauenswürdige, zentrale Stelle ausgibt, wie z. B. die Bundesnotarkammer bei der „beA-Karte".

d) Zusammenfassung

Eine digitale Signatur („fortgeschrittene elektronische Signatur" im Sinne des Art. 3 Nr. 11 eIDAS-VO) stellt die Integrität von Daten sicher: Ein Angreifer kann diese nicht mehr verändern (im OLG-Fall: die Rechnung mit Bankverbindung).

Nutzt der Absender einen z. B. durch das GPG-Web-of-Trust gesicherten Key, lässt sich auch nachprüfen, dass die Rechnung tatsächlich von ihm stammt.

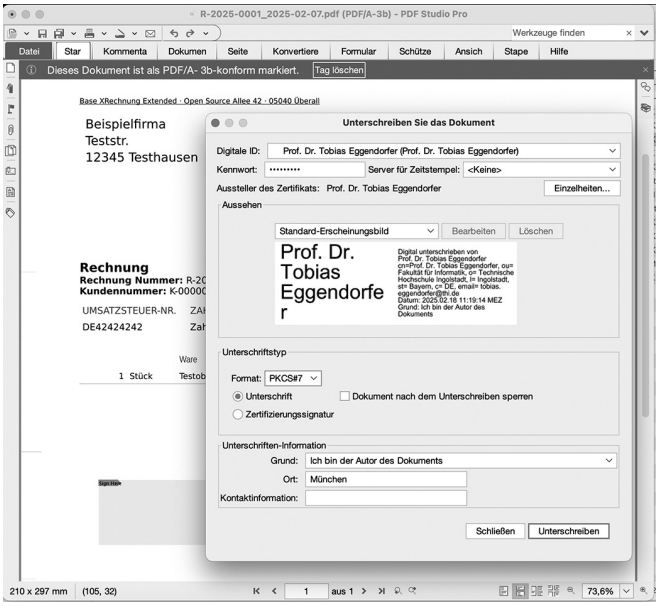
Zusätzlich wäre Vertraulichkeit durch Verschlüsselung wünschenswert. Der Mehraufwand hierfür beschränkt sich auf einen Mausklick, wenn beide Kommunikationspartner digitale Signaturen nutzen, da diese dieselbe technische Infrastruktur benötigen. Im Unternehmen lässt sich die Verwaltung der Schlüssel zentralisieren und automatisieren.[19]

2. Umsetzbarkeit der Gegenmaßnahmen

In der Praxis verweigern Versender häufig Verschlüsselung und Signatur, angeblich sei der Mehraufwand gigantisch. Dabei ist in (fast) allen gängigen E-Mail-Programmen nur ein Klick nötig. Der Irrglaube an die Komplexität hält sich trotzdem hartnäckig, vermutlich, weil die Mathematik dahinter nicht trivial ist.

Ebenso falsch ist die Aussage, habe der Empfänger keinen Schlüssel, könne er die Mail nicht lesen. Doch ohne Schlüssel keine Verschlüsselung,[20] daher bekommt er einfach eine unverschlüsselte Mail. Damit liegt die Entscheidung über Verschlüsselung aus technischer Sicht beim Empfänger.

Eine Signatur erfordert nur ein eigenes Schlüsselpaar, und ist so ohne Zutun des Empfängers möglich. Ob er die Signatur prüft, bleibt seine Entscheidung und sein Risiko. Interessant, insbesondere für Rechnungen, ist dabei, dass jeder auch PDF-Dateien mit einer digitalen Signatur versehen kann.



Erforderlich ist lediglich ein Zertifikat; dieses enthält das Schlüsselpaar zum Signieren. Das kann sich jeder Nutzer selbst erstellen oder von einem Vertrauensdiensteanbieter erwerben.[21] Zum Signieren einer PDF-Datei bieten die gängigen Programme nutzerfreundliche Funktionen.[22] Damit ist der

13 VO (EU) 910/2024, zuletzt geändert durch VO (EU) 2024/1183.
14 *Deusch/Eggendorfer* (Fn. 8), Ziffer 2.2.3 sowie auch generell Fn. 8.
15 https://gnupg.org/.
16 Web-of-Trust – Netz des Vertrauens. Die Idee ist, dass rechnerisch jeder Mensch über nur wenige Personen die ganze Welt kennt. Dadurch sind gegenseitige Bestätigungen der Echtheit und der Zuordnung des Keys über ein Vertrauensnetz für alle nutzbar.
17 https://pgp.governikus.de/?lang=DE.
18 *Deusch/Eggendorfer* (Fn. 8), Ziffer 2.3.1.6.3.
19 *Eggendorfer*, PGP-Keyserver im Unternehmen einsetzen, Linux-Magazin 11/20219, https://www.linux-magazin.de/ausgaben/2019/11/pgp-pki/.
20 Verfahren wie WebKey-Discovery können die Suche nach Schlüsseln auch weiter automatisieren. Dazu auch Fn. 19.
21 Siehe oben lit. a.
22 Das Benutzerhandbuch des Adobe-Readers beschreibt das Signieren bzw. Einfügen des Zertifikats z. B. unter https://helpx.adobe.com/de/acrobat/using/securing-pdfs-certificates.html

Inhalt der PDF-Datei geschützt. Ob die Signatur gültig ist, zeigt das PDF-Programm unmittelbar an.[23]

Der einfache Arbeitsschritt „PDF unterschreiben" schützt also vor Rechnungsmanipulationen wie im Fall des OLG Schleswig-Holstein.

3. Fazit Technik

Zusammenfassend lässt sich feststellen: Eine digitale Signatur, sei es in der PDF-Datei der Rechnung oder der E-Mail mit der Rechnung, hätte Manipulationen nach dem Erstellen auf die Rechnung erfolgreich verhindert. Denn durch die Signatur hätte der Rechnungsempfänger erkennen können (und müssen), dass die Daten geändert wurden.

Verschlüsselung schützt dagegen, anders als vom OLG Schleswig-Holstein postuliert, nicht vor Manipulation. Das kann jeder leicht mit einem Cäsar-Chiffre selbst probieren: Wird mit dem Key 3 aus „K&R" „N&U", lässt sich das auf dem Transportweg immer noch blind manipulieren zu „G&H", was sich dann zu „D&E" entschlüsselt.[24] Der Angreifer kann allerdings in der Regel nicht vorhersagen, was beim Entschlüsseln herauskommt.

Die nötige Software ist seit Jahrzehnten verfügbar, es scheitert allein an der Nutzung.

III. Rechtliche Würdigung und Relevanz des Urteils

1. OLG Schleswig-Holstein vs. OLG Karlsruhe

Das OLG Schleswig-Holstein spricht dem Rechnungsempfänger einen Schadensersatzanspruch aus Art. 82 DSGVO zu. Denn eine „Transportverschlüsselung" der E-Mail sei kein geeigneter Schutz, um die Daten des Rechnungsempfängers vor unberechtigten Dritten zu schützen. Diese Auffassung entspricht dem Stand der Technik. Die Autoren haben hierauf bereits an anderer Stelle hingewiesen.[25]

Die Annahme des OLG, Ende-zu-Ende-Verschlüsselung sei „das Mittel der Wahl", um Rechnungsmanipulationen zu verhindern, kann das Urteil allerdings nur eingeschränkt tragen. Wie Abschnitt II zeigt, stellt die digitale Signatur als geeignete technische Maßnahme die Integrität einer Nachricht, mithin die Unveränderbarkeit der elektronischen Rechnung, sicher. Das rechtliche Ergebnis bleibt trotzdem dasselbe. Denn Art. 32 Abs. 1 lit. b DSGVO erfordert auch die Sicherstellung der Integrität einer Nachricht. Dies schließt die Bankverbindung des Rechnungsstellers ein, selbst wenn es sich um das Bankkonto einer GmbH handelt, deren Daten nicht von der DSGVO geschützt sind. Denn die Rechnung enthält den Zahlungsbefehl an den Empfänger und ist somit insgesamt für ihn als Betroffenen ein personenbezogenes Datum.[26]

Art. 32 DSGVO verpflichtet allerdings den Rechnungsaussteller nicht nur zum Schutz der Integrität, sondern auch der Vertraulichkeit. Für die Vertraulichkeit ist die Ende-zu-Ende-Verschlüsselung in der Tat das Mittel der Wahl.[27] Die so gewährleistete Vertraulichkeit mag zwar Angriffe auf Rechnungen erschweren, weil der Täter möglicherweise nicht weiß, ob die Mail eine Rechnung enthält. Doch das ist aus Sicht der IT-Sicherheit ein schwaches Argument: Er könnte jederzeit die verschlüsselte Mail abfangen und durch eine eigene ersetzen. Zum Verschlüsseln reicht der öffentliche Schlüssel des Empfängers aus.

Interessanterweise schließt sich das OLG Schleswig-Holstein in Abschnitt II, Ziffer 1 der Urteilsgründe dem OLG Karlsruhe[28] an, wonach die Zahlung an die falsche Bankverbindung keine Erfüllung gemäß § 362 BGB herbeiführt. Beide OLGs zitieren weiter die identischen Quellen der DSK und des BSI zur „Ende-zu-Ende-Verschlüsselung",[29] kommen aber zu entgegengesetzten Ergebnissen, wobei das OLG Schleswig-Holstein einen offenen Widerspruch zum OLG Karlsruhe vermeidet. Dies liegt auch daran, dass dem OLG Karlsruhe eine Rechnungsmanipulation im „B2B"-Verhältnis zugrunde lag; geschädigt war eine juristische Person. Deshalb hat der Karlsruher Senat eine Pflicht zur Ende-zu-Ende-Verschlüsselung und einen Datenschutzverstoß verneint.[30] Vor dem OLG Schleswig-Holstein war ein Verbraucher der Rechnungsadressat.[31] Der Verstoß des Rechnungsausstellers gegen Art. 32 DSGVO betraf damit unmittelbar den fehlenden Schutz der personenbezogenen Beklagtendaten und verursachte bei diesem einen Schaden in Höhe der Fehlüberweisung. Es bestand für das OLG Schleswig-Holstein somit keine Notwendigkeit, sich mit dem Postulat der „Sicherheitserwartungen des Verkehrs" aus Karlsruhe auseinanderzusetzen, wonach „transportverschlüsselte E-Mails" ausreichend seien.[32]

2. Praxisrelevanz der unterschiedlichen OLG-Urteile

Da sich der BGH mangels Revision zu den Sorgfaltspflichten in der E-Mail-Kommunikation bis auf Weiteres nicht äußern wird, bleibt für die Praxis folgender Befund:

- Unternehmer, die Rechnungen per E-Mail an natürliche Personen versenden, sollten die Mail oder Rechnung signieren und Ende-zu-Ende-verschlüsselt versenden. Falls dies nicht möglich ist, bleibt die Papierrechnung. Dies gilt auch nach Einführung der E-Rechnung, jedenfalls, wenn der Rechnungsempfänger ein Verbraucher ist (siehe unten Abschnitt IV). Andernfalls besteht wegen der Entscheidung des OLG Schleswig-Holstein das Risiko des Rechnungsausfalls bzw. Schadensersatzes. Obgleich hier der Beklagte „Privatkunde" war, gilt das auch gegenüber Unternehmern, sofern sie natürliche Personen sind (z. B. „e. K." oder Freiberufler). Denn auch diese können aus einem DSGVO-

23 Eine Ausnahme ist ausgerechnet der unten in Abschnitt 7 vorgestellte Quba-Viewer.

24 Wer nicht von Hand zwei Alphabete übereinanderlegen möchte, kann sich online Unterstützung holen: https://www.cryptool.org/en/cto/caesar/ bietet hervorragende Erklärung, Darstellung und Experimentiermöglichkeiten zu einer Vielzahl von Verschlüsselungsverfahren.

25 *Deusch/Eggendorfer*, K&R 2015, 11 ff.; *dies.* K&R 2022, 577 (Transportverschlüsselung keine angemessene Geheimhaltungsmaßnahmen gemäß § 2 Nr. 1 b) GeschGehG), K&R 2024, 242, 244 (kritisch zum Urteil des OLG Karlsruhe, 27. 7. 2023 – 19 U 83/22, K&R 2023, 607).

26 Gemäß Abschnitt II Ziffer 2., a), bb), (1), (cc), (ccc) der Urteilsgründe ist auch die aus der Rechnung stammende Information, dass ein Werkvertrag mit dem Beklagten besteht, ein personenbezogenes Datum.

27 *Deusch/Eggendorfer*, K&R 2015, 11, 14, 16; *dies.*, K&R 2022, 577; *Eggendorfer*, Fn. 19 mit jeweils weiteren Quellen, siehe auch Fn. 8.

28 OLG Karlsruhe, 27. 7. 2023 – 19 U 83/22, K&R 2023, 607 ff.

29 Siehe oben Fn. 3 und Fn. 4.

30 Richtigerweise werden auch bei Rechnungen gegenüber juristischen Personen personenbezogene Daten verarbeitet, zum Beispiel die Namen von Geschäftsführern bzw. Mitarbeitern der GmbH, die die Rechnung empfangen hat. Geschädigt bleibt allerdings die juristische Person als Rechnungsempfänger. Diese kann sich nicht auf den DSGVO-Verstoß berufen, siehe *Deusch/Eggendorfer*, K&R 2024, 242, 244; ähnlich *Wiedemann/Sorge*, K&R 2023, 612, die wie die Autoren (K&R 2024, 242, 244) zum OLG Karlsruhe die fehlende Signatur als Schadensursache identifizieren.

31 Der Senat bezeichnet die Beklagtenseite in Abschnitt II, Ziffer 2 a) bb) mehrfach als „Privatkundin".

32 Was die Autoren kritisch sehen, siehe *Deusch/Eggendorfer*, K&R 2024, 242, 244.

Verstoß Schadensersatzansprüche gemäß Art. 82 DSGVO ableiten. Natürliche Personen, die keine Verbraucher sind, müssen aber jedenfalls nach dem 31. 12. 2027 eine „E-Rechnung" erhalten; für diese Fälle bestehen die Probleme in Abschnitt IV.

- Durch eine Manipulation geschädigte Rechnungsempfänger können eine nochmalige Zahlung an den Rechnungsaussteller verweigern oder – sofern „Doppel-Zahlung" bereits erfolgt ist – eine Erstattung vom Rechnungsaussteller verlangen, wenn er die Rechnung nicht per Ende-zu-Ende-verschlüsselter E-Mail versendet hat, sondern lediglich „transportverschlüsselt". Natürliche Personen können sich dabei unmittelbar auf das Urteil des OLG Schleswig-Holstein berufen; juristische Personen haben das entgegenstehende Urteil des OLG Karlsruhe zu überwinden, das außerhalb der DSGVO gerade keine Ende-zu-Ende-Verschlüsselung fordert. In keinem der Verfahren war jedoch die technisch korrekte Lösung, eine digitale Signatur, Gegenstand. Sie könnte das nötige Argument liefern.[33]
- Das OLG Schleswig-Holstein hat in der fehlenden Ende-zu-Ende-Verschlüsselung dann einen Verstoß gegen Art. 32 DSGVO angenommen, wenn die Gefahr einer Rechnungsmanipulation mit einem „hohen finanziellen Risiko" (konkret ging es um € 15 000,00) bei einem Verbraucher als Rechnungsempfänger zu vermeiden ist.

Damit lässt sich zwar keine gerichtliche Aussage zu einer generellen Ende-zu-Ende-Verschlüsselungspflicht von E-Mails ableiten. Auf den Prüfstand sind allerdings zahlreiche weitere Situationen zur E-Mail-Kommunikation zu stellen, die in den Augen der Verfasser nicht weniger schutzbedürftig sind als eine Rechnung in Höhe von € 15 000,00 gegenüber einem Verbraucher, zum Beispiel:

- Kommunikationen bei verschwiegenheitsverpflichteten Berufsträgern,
- digitaler Datenaustausch zwischen Unternehmen im Rahmen von Vertraulichkeitsvereinbarungen (sogenannte „NDA", zum Beispiel bei Unternehmenstransaktionen – „M&A" – oder Entwicklungsprojekten),[34]
- behördliche Datenkommunikation, sei es im Polizei-, Gesundheits- oder oft vernachlässigten Sozialrecht.

IV. ZUGFeRD und XRechnung

Das Postulat des OLG Schleswig-Holstein nach der Verschlüsselung bei elektronischen Rechnungen drängt die Frage nach der Relevanz bei der sogenannten „E-Rechnung" auf. Denn das OLG verweist in Fällen, in denen der Rechnungsempfänger keine Ende-zu-Ende-Verschlüsselung hat, wie „eh und je" auf den Papierweg.[35] Dieser Gedanke sollte sich auf die fehlende Signatur übertragen lassen.

Die Pflicht zur E-Rechnung versperrt diesen Weg, allerdings nur bei unternehmerischen Rechnungsadressaten (was im Fall des OLG Schleswig-Holstein gerade nicht zutraf, siehe unten Ziffer 1).

Gleichwohl bringen die Aussagen des OLG Schleswig-Holstein zur E-Mail-Sicherheit Aspekte mit sich, die auch für die Rechnungsübermittlung im unternehmerischen Rechtsverkehr relevant sind und somit die Frage herausfordern, ob die bisherigen Vorkehrungen für E-Rechnungen den erforderlichen Sicherheitsanforderungen gerecht werden (siehe unten Ziffern 2 bis 4).

1. Pflicht zur E-Rechnung im unternehmerischen Verkehr gemäß § 14 Abs. 2 UStG

Zum 1. 1. 2025 hat § 14 UStG die elektronische Rechnung („E-Rechnung") eingeführt nebst der Pflicht, per E-Rechnung abzurechnen (vorgesehen als „XRechnung" oder ZUGFeRD, siehe unten Ziffer 2 und 3). Die Hinweise der Finanzverwaltung zum Umgang mit der E-Rechnung sind dem BMF-Schreiben 15. 10. 2024 zu entnehmen:[36]

- Ab 1. 1. 2025 müssen Unternehmer elektronische Rechnungen empfangen, sichtbarmachen und archivieren können.
- Gemäß § 14 Abs. 2 Nr. 1 UStG ist die E-Rechnung Pflicht für alle Umsätze in Höhe von mehr als € 250,00 in Deutschland, die gegenüber einem deutschen Unternehmer abgerechnet werden. Bis zum 31. 12. 2026 sind auch im unternehmerischen Verkehr noch Papierrechnungen zulässig, dies gilt sogar bis zum 31. 12. 2027, wenn der Rechnungsaussteller im Vorjahr nicht mehr als € 800 000,00 Umsatz erwirtschaftet hat (§ 27 Abs. 38 UStG).
- Gegenüber Verbrauchern bleibt jedoch auch nach dem 1. 1. 2028 – wie vom OLG Schleswig-Holstein vorgeschlagen – die Papierrechnung möglich, jedenfalls aus rechtlicher Sicht.[37]

Bei der E-Rechnung soll der Auftragnehmer statt einer Papier-Rechnung eine XML-Datei mit den Rechnungsdaten verschicken. Der Auftraggeber könne diese, so der Plan, automatisch in sein System einlesen, müsse keine Daten für eine Überweisung manuell übertragen und hat auch gleich die kompletten Buchungssätze in seiner Buchhaltung. Nebenbei erleichtert sich die Prüfung des Finanzamts.

2. XRechnung

XML ist eine Auszeichnungssprache. Über (theoretisch) menschenlesbare Markierungen, sogenannte Tags, lassen sich einzelne Datenfelder in dem Rechnungsdatensatz markieren. Ein naives Beispiel für eine XML-Rechnung könnte wie folgt aussehen:

```
<XML-Rechnung>
 <Rechnungssteller>
 <Firma>Beispielfirma</Firma>
 ...
 </Rechnungssteller>
 <Empfaenger>...</Empfaenger>
 <Positionen>
 <Position>
 <Anzahl>2</Anzahl>
 <Einheit>Std.</Einheit>
 <Leistung>Beratung</Leistung>
 <Einheitspreis>200.00</Einheitspreis>
 </Position>
 ....
 </Positionen>
</XML-Rechnung>
```

33 Siehe Fn. 30 und Fn. 32.
34 *Deusch/Eggendorfer*, K&R 2015, 11, 16.
35 Abschnitt II Ziffer 2., a), bb), (1), (cc), (ccc) der Urteilsgründe.
36 BMF, 15. 10. 2024 – III C 2 – S 7287-a/23/10001 :007 BStBl 2024 I S. 1320; dazu auch *Langer/Artinger*, K&R 2024, 464 ff.
37 Allerdings darf der unternehmerische Rechnungsempfänger X- und ZUGFeRD-Rechnungen seit 1. 1. 2025 nicht mehr zurückweisen, wie dies § 14 Abs. 1 S. 7 UStG i. d. F. bis 31. 12. 2024 ermöglichte (§ 27 Abs. 38 UStG.

In der realen XRechnung sind die XML-Tags etwas länger, die Daten verschachtelter, mehr Daten enthalten und damit die Lesbarkeit noch schlechter.[38] Sie ist nicht zum unmittelbaren Lesen durch Menschen gedacht. Diese sollten ein Anzeigeprogramm dafür nutzen. Wer kein DATEV nutzen will, findet mit Quba eine OpenSource-Lösung,[39] die auf allen gängigen Betriebssystemen läuft.

3. ZUGFeRD

Weil noch nicht jeder die XRechnung lesen kann, hat das Forum elektronische Rechnung Deutschland (FeRD) das Format ZUGFeRD veröffentlicht: Dieses kombiniert eine XRechnung mit der PDF-Version der Rechnung – es gibt also eine Version für das menschliche Auge und eine für einen digitalen Prozess.[40]

4. Sicherheitslücke: Fehlende Signatur

Was auf den ersten Blick hervorragend klingt, ist aus Sicht der IT-Sicherheit ein mehrfacher Fehlgriff. Der Fall des OLG Schleswig-Holstein liefert das Praxisbeispiel dazu:

Als Betrüger im PDF die Position der Bankverbindung zu finden, automatisch zu ersetzen und dabei auch die individuelle Formatierung zu wahren (ist die IBAN z. B. mit oder ohne Leerzeichen angegeben, steht sie in der Fußzeile oder rechts in einer gesonderten Spalte), ggf. noch den Banknamen und die BIC zu tauschen, sind programmiertechnisch ein hoher Aufwand.

Anders in der XRechnung: Durch die XML-Tags ist die Bankverbindung eindeutig markiert, der Zugriff darauf schnell und effizient möglich. Ein automatisches Austauschen der Daten damit trivial. Die Manipulation im Fall des OLG Schleswig-Holstein ist mit der E-Rechnung viel einfacher zu begehen.

Wenn die Tatbegehung einfacher und damit wahrscheinlicher wird, sollte man erwarten, dass Gegenmaßnahmen von Anfang an vorbereitet sind. Weit gefehlt: Die technisch einzig geeignete Maßnahme, eine Signatur, die im Übrigen sogar in der XRechnung zu verpacken gewesen wäre, ist nicht vorgesehen. Manipulation ist also nicht zu erkennen.

5. Sicherheitslücke: Redundanz

Doch damit nicht genug: Bei ZUGFeRD kann die XRechnung von der PDF-Datei abweichen. Beide sind zwar in eine Datei gepackt, aber die XRechnung ist technisch unabhängig vom PDF-Inhalt. Vermutlich ist man davon ausgegangen, dass beide zugleich erstellt werden, hat aber keine Täter einkalkuliert, die nachträglich manipulieren.

Fatal daran: Wer sich die PDF-Rechnung ansieht, sie in die Buchhaltung zieht und automatisch überweisen lässt, merkt gar nicht, dass die Daten von der automatisch verarbeiteten XRechnung abweichen.

Bevor jetzt die Rechtsprechung in Analogie zum beA[41] auf die Idee kommt, man könne ja manuell nachprüfen, ob die Inhalte übereinstimmen, bietet es sich als Versender an, die ZUGFeRD-Datei im PDF-Viewer zu signieren. Die Signatur umfasst die eingebettete XRechnung. So gibt es immerhin einen Workaround. Der funktioniert allerdings nicht immer: Der in den Quba-Viewer integrierte PDF-Viewer prüft noch nicht die PDF-Signatur.

Wieso allerdings das Konzept ZUGFeRD noch nicht einmal eine PDF-Signatur vorsieht, wenn schon die XRechnung unsigniert ist, erschließt sich nicht.[42]

V. Fazit und Ausblick

Die Autoren freut es, dass das OLG Schleswig-Holstein ihre Ansicht teilt, wonach Ende-zu-Ende-Verschlüsselung von E-Mails Stand der Technik und erforderlich ist.[43] Leider traut der Senat aber der Verschlüsselung mehr zu, als sie leisten kann: Die geeignete Maßnahme zum Schutz von Daten vor Manipulationen ist eine digitale Signatur.

Da die derzeit verfügbaren Formate der verpflichtenden E-Rechnung keine Signatur vorsehen, ist allerdings mit einer Häufung solcher Vorfälle zu rechnen. Im ZUGFeRD-Format, das XRechnung und PDF ungeeignet verschmilzt, ist zudem nicht sichergestellt, dass die Daten beider Elemente miteinander übereinstimmen.

Bis die Sicherheitslücken der XRechnung behoben sind, ist eine PDF-Signatur eine Übergangslösung als Work-Around.

Generell ist es wünschenswert und zu empfehlen, dass Signaturen zum Standard werden, denn durch den Nachweis der Absendereigenschaft erschweren sie auch alle anderen Betrugsversuche und weitere Taten wie Phishing.

Dr. Florian Deusch

ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

Prof. Dr. Tobias Eggendorfer

ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme“ an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT-Berater und Datenschutzbeauftragter tätig.

38 Die vollständige Spezifikation findet sich unter https://www.xoev.de/sixcms/media.php/13/200-XRechnung-2020-06-30.pdf, ein lesbares Beispiel findet sich in *Eggendorfer*, Schwer verrechnet, Linux Magazin 04/2025, S. 50 ff.

39 https://quba-viewer.org/.

40 Das in Ziffer 1 genannte BMF-Schreiben bezeichnet in Rn. 30 den „strukturierten Datenteil“ einer ZUGFeRD-Rechnung als „XML-Datei“. Dabei nutzt das BMF den Gattungsbegriff, tatsächlich sieht die ZUGFeRD-Spezifikation (https://www.ferd-net.de/publikationen-produkte/publikationen/detailseite/zugferd-232-deutsch) ausschließlich das konkrete Format „XRechnung“ vor. XML ist lediglich eine Auszeichnungssprache, die von Grafiken über Textdokumente bis Datenbanken alles beschreiben kann. Eine XML-Datei ist eine Datei, die XML-formatierte Daten enthält. XRechnung gibt das konkrete, in dem Fall ausschließlich zulässige XML-Format wieder. Dadurch ist XRechnung die technisch korrekte Bezeichnung. Da den Autoren stets auch der korrekte technische Sachverhalt am Herzen liegt, nutzt dieser Beitrag in Abweichung zum BMF den technisch korrekten Ausdruck.

41 https://www.brak.de/newsroom/news/anwaelte-muessen-komplette n-schriftsatz-im-bea-ueberpruefen/; wobei eine manuelle Prüfung des Absenders nicht zielführend wäre, wenn ein Dritter die XRechnung nach der Prüfung ändert.

42 Die Sicherheitslücken wurden über den Common Vulnerability Disclosure Prozess dem BSI am 7. 2. 2025 gemeldet. Aus technischer Sicht diskutiert sie *Eggendorfer*, Schwer verrechnet, Linux Magazin 04/25, S. 50 ff.

43 *Deusch/Eggendorfer*, (Fn. 25).

Hinweise der Redaktion:

Siehe hierzu auch die Beiträge von *Eggendorfer/Schmidt-Wudy*, eIDAS 2.0 – „Sicherheit trotz und wegen Verschlüsselung“?, K&R 2024, 13 ff. und *Deusch/Eggendorfer*, Vom Irrglauben an die Geheimhaltung durch TLS bei E-Mails, K&R 2022, 577 ff. sowie das Urteil des OLG Schleswig-Holstein, vom 18. 12. 2024 – 12 U 9/24, K&R 2025, 272 ff. (in diesem Heft).