

Zum Begriff „Zugang“: Der Begriff „Zugang“ stellt auf die objektiv vorhandene technische Kommunikationseinrichtung ab, also z.B. auf die Verfügbarkeit eines elektronischen Postfachs. Zugegangen ist eine Willenserklärung, wenn sie derart in den Machtbereich des Empfängers gelangt ist, dass bei Annahme gewöhnlicher Verhältnisse damit zu rechnen ist, dass er von ihr Kenntnis erlangen kann.¹ Diesem individuellen Erfordernis wird durch das Kriterium der „Eröffnung“ des Zugangs Rechnung getragen. Der Empfänger eröffnet seinen Zugang durch entsprechende Widmung. Dies kann ausdrücklich oder konkludent erfolgen. Im Einzelfall wird hier die Verkehrsanschauung, die sich mit der Verbreitung elektronischer Kommunikationsmittel fortentwickelt, maßgebend sein.² Demzufolge kann davon ausgegangen werden, dass Behörden, Firmen oder Rechtsanwälte, die auf ihren Briefköpfen eine E-Mail-Adresse angeben, damit konkludent ihre Bereitschaft erklären, Eingänge auf diesem Weg anzunehmen.³ Sie haben durch organisatorische Maßnahmen sicherzustellen, dass z.B. E-Mail-Postfächer regelmäßig abgefragt werden. Gegenteiliges müssen sie ausdrücklich erklären, z.B. durch Hinweise auf ihrem Briefkopf oder auf ihrer Internetseite. Beim Bürger wird hingegen die bloße Angabe einer E-Mail-Adresse auf seinem Briefkopf heute noch nicht dahingehend verstanden werden können, dass er damit seine Bereitschaft zum Empfang von rechtlich verbindlichen Erklärungen kundtut. Insbesondere entspricht es zumindest heute noch nicht der Verkehrsanschauung, dass der Private täglich seine E-Mails abrufen. Bei ihm kann in aller Regel von der Eröffnung eines Zugangs nur ausgegangen werden, wenn er dies gegenüber der Behörde ausdrücklich erklärt hat.⁴

253

Zum Signaturgesetz: Aufgabe des Signaturgesetzes ist es sicherzustellen, dass für den Empfänger der Daten die Identität des Absenders (die Authentizität) und die Unverfälschtheit der Daten (die Integrität) erkennbar ist. Das wiederum soll mit Hilfe eines mehrstufigen Verfahrens erfolgen: Zunächst muss der Zeichnungsberechtigte (der Nutzer) seine handschriftliche Unterschrift bei einer Zertifizierungsstelle hinterlegen. Daraufhin erhält er eine elektronische Signatur in Form von verschlüsselten Informationen auf einer Chipkarte, die einer ec-Karte sehr ähnlich sieht, und einer separaten Geheimzahl. Über ein Kartenlesegerät, das an den heimischen Computer angeschlossen ist, kann sich der Nutzer dann anmelden und ausweisen. Gibt er dann noch die ihm zugewiesene Geheimzahl ein, hat er das entsprechende Dokument unverwechselbar unterschrieben (dieses Verfahren entspricht dem mittlerweile als Standard geltenden HBCI-Chipkartenverfahren beim sog. internet-banking). Insgesamt folgt daraus auch, dass eine Signatur mit einem Pseudonym, wie das bspw. bei den sog. Internet-Auktionen üblich ist, unzulässig ist (§ 3a II S. 3 VwVfG).

254

¹ St. Rspr. vgl. nur BGHZ 137, 205, 208; BGH NJW 2002, 2391, 2393.

² Vgl. BGH NJW 2002, 1565.

³ Wie hier Schlatmann, DVBl 2002, 1005, 1008 f.; Schmitz/Schlatmann, NVwZ 2002, 1281, 1285.

⁴ Vgl. Schmitz/Schlatmann, NVwZ 2002, 1281, 1285; Yildirim, DVBl 2002, 241, 242.