SPECTRUM-News Februar 2021

Neues Grundsatzurteil: Die TLS-Transportverschlüsselung bei E-Mails reicht idR. Aus und ist kein DSGVO-Verstoß

Wir möchten Sie nachfolgend über ein aktuelles Urteil des VG Mainz informieren, wonach die Auffassung der BStBK von April 2019 (siehe unteranderem die Infos zur E-Mail-Verschlüsselung auf unserer Homepage: https://www.spectrum-news.de/tls) bestätigt wird, dass eine Transportverschlüsselung (TLS) bei E-Mails von Berufsgeheimnisträgern wie Steuerberatern und Rechtsanwälten ausreichend ist und keinen Datenschutzverstoß darstellt solange keine Anhaltspunkte für einen erhöhten Schutzbedarf bestehen.

Hier das Urteil des VG Mainz (VG Mainz, Urt. v. 17.12.2020 - Az.: 1 K 778/19.MZ): Transportverschlüsselung bei E-Mails idR. ausreichend = kein DSGVO-Verstoß

Es reicht für die Einhaltung der datenschutzrechtlichen Vorschriften aus, wenn personenbezogene Daten über E-Mail ausgetauscht werden, bei der eine Transportverschlüsselung gegeben ist. Dies gilt auch bei Berufsgeheimnisträgern wie Anwälten, Steuerberater usw.. Etwas Anderes gilt nur dann, wenn Anhaltspunkte einen erhöhten Schutzbedarf rechtfertigten (VG Mainz, Urt. v. 17.12.2020 - Az.: 1 K 778/19.MZ).

Der Landesbeauftragte für Datenschutz und die Informationsfreiheit Rheinland-Pfalz monierte die E-Mail einer Rechtsanwaltskanzlei, die vertrauliche Daten per elektronischem Medium verschickt hatte. Es sei, so die Behörde, kein ausreichendes Schutzniveau nach Art. 32 DSGVO eingehalten worden. Die vorgenommene Transportverschlüsselung sei nicht ausreichend. Vielmehr hätte es auch einer Inhaltsverschlüsselung bedurft.

Dagegen klagte der Advokat und bekam Recht.

Das Gericht bewertete die Einstufung des Datenschutzamtes für rechtswidrig.

Auch Berufsgeheimnisträger (wie z.B. Anwälte, Steuerberater oder Notare) seien grundsätzlich nur verpflichtet, für eine ausreichende Absicherung auf dem Transportweg zu sorgen:

> *„Insgesamt ist davon auszugehen, dass die DSGVO im Normtext selbst ausdrücklich keine spezifischen Regelungen für Berufsgeheimnisträger enthält; vielmehr gelten grundsätzlich (...) die allgemeinen Vorschriften (...).*
>
> *Demnach bestimmen zunächst die Art. 9 und 10 DSGVO, welche Datenkategorien generell besonderen Schutz genießen (...). Pauschal kann daher (datenschutzrechtlich) zunächst nicht allein deshalb von einer besonderen Schutzbedürftigkeit ausgegangen werden, weil eine mandatsbezogene Kommunikation über E-Mail erfolgt (...). (...).*
>
> *Während die Transportverschlüsselung ohne weiteres **als weit verbreiteter Standard anzusehen sein dürfte**, trifft den Verantwortlichen bei der Implementierung einer Ende-zu-Ende-Verschlüsselung regelmäßig ein höherer Aufwand (...).*
>
> *Neben der Nutzung von derartigen E-Mail-Protokollen (z.B. S/MIME oder PGP), die allerdings auch auf*

Absender- und Empfängerseite entsprechende besondere Software und Kenntnisse erfordern, kommen letztlich auch einseitige Implementierungsmaßnahmen, wie z.B. Übersendung einer passwortgeschützten Datei, in Betracht (...).

Damit dürfte eine kostenschonende Implementierung zwar generell möglich und für den jeweiligen Verantwortlichen nicht von vornherein unzumutbar sein. Allerdings bedeutet dies nicht, dass dies zwingend zu einer entsprechenden Verpflichtung des Verantwortlichen führt. Schließlich können bei der Übersendung einer passwortgeschützten Datei unter Umständen (zivilrechtliche) Zugangsprobleme auftreten; auch fehlt es an einer ohne weiteres gegebenen Möglichkeit der Weiterleitung für den Empfänger (...)."

Etwas andere gelte nur dort, wo im Einzelfall besondere Umstände gegeben seien, die eine strengere Verschlüsselung rechtfertigen würden:

„Generell wird (...) die Verwendung einer Transportverschlüsselung datenschutzrechtlich - auch bei Berufsgeheimnisträgern - ausreichend sein, sofern keine Anhaltspunkte für besonders sensible Daten bestehen oder sonstige Umstände hinzutreten. Vielmehr ist die Kommunikation mittels (obligatorisch) transportverschlüsselter E-Mails auch im geschäftlichen Verkehr durchaus als sozialadäquat und wohl derzeit noch als (Mindest-)Stand der Technik einzustufen (...).

Ebenso gehört die etwaige (unbefugte) Kenntnisnahme Dritter von Inhalten der elektronischen Kommunikation - wie auch bei anderen (analogen) Kommunikationsformen - zum allgemeinen Lebensrisiko.

Besondere Anhaltspunkte, die einen erhöhten Schutzbedarf begründen und das bei einer hier vorliegenden Form der Transportverschlüsselung bestehende Restrisiko als nicht (mehr) angemessen erscheinen lassen, lagen hier nicht vor. Es handelte sich zunächst weder um Daten, die von Art. 9 und 10 DSGVO erfasst waren, noch kamen diese den dort genannten Datenkategorien auch nur nahe. Dabei dürfte auch anzunehmen sein, dass die vorgenannten Vorschriften tendenziell eng oder zumindest nicht schematisch auszulegen sind (...).

Schließlich war hier zudem keine „Bewertung" des Verhaltens oder der Leistungsfähigkeit des betroffenen Beschwerdeführers oder sonstiger Personen (vgl. ErwGr. 75 Satz 3 DSGVO) Gegenstand der E-Mail. Spezielle Indizien für einen naheliegenden Verlust der Vertraulichkeit lagen nicht vor („Eintrittswahrscheinlichkeit"); die sonstigen Umstände, Zwecke und der Umfang der Datenverarbeitung bieten ebenfalls keine Anhaltspunkte für einen in diesem Einzelfall wesentlich erhöhten Schutzbedarf. Allein die Tatsache, dass der Kläger und die Betroffenen (untereinander) in eine (jedenfalls außergerichtliche) rechtliche Auseinandersetzung verwickelt waren, reicht nicht aus."

SPECTRUM-Hinweis:

Mit dem SPECTRUM-NET Zusatz „Zwangs-TLS"-E-Mail-Verschlüsselung wird sichergestellt, dass E-Mails grundsätzlich TLS-verschlüsselt versendet oder empfangen werden, je nach eingestellter Option. Es ist optional und kostenlos möglich, dass im SPECTRUM-ASP- und im SPECTRUM-NET-Betrieb die Einstellung vorgenommen werden kann, dass alle ausgehenden E-Mails zwangsweise nur TLS-verschlüsselt verschickt werden. Sollte ein Empfänger die TLS-Verschlüsselung nicht unterstützen, wird die E-Mail nicht übertragen und der Absender bekommt den Hinweis, dass die Mail nicht verschickt wurde. Der Absender kann dann entscheiden, ob er dem Empfänger die Mail nicht TLS-Transport-verschlüsselt übertragen möchte. Hierzu kann der Absender die Empfänger-Adresse auf eine WhiteList setzen lassen (die Administration erfolgt bei SPECTRUM-ASP ohne zusätzliche Berechnung).