## Wie viel Sicherheit muss sein?

*Übermitteln Behörden Dokumente mit sensiblem Inhalt auf elektronischem Weg, stellt sich die Frage, welche Sicherheitsanforderungen dabei einzuhalten sind. In einer aktuellen Entscheidung hat das Verwaltungsgericht Frankfurt am Main klargestellt: Bei der elektronischen E-Mail-Kommunikation von Behörden ist grundsätzlich eine einfache Transportverschlüsselung notwendig, aber auch auseichend, um den datenschutzrechtlichen Anforderungen zu genügen.*

Der Stand der Digitalisierung in deutschen Behörden wird häufig kritisiert. In der Regel herrscht dabei weitestgehend Einigkeit darüber, dass die Möglichkeiten des technischen Fortschritts, insbesondere in der elektronischen Kommunikation, nur langsam und unzureichend umgesetzt werden.

In dem nun von dem VG Frankfurt/Main entschiedenen Fall wehrte sich der Antragsteller jedoch gerade gegen eine behördliche Übermittlung von Dokumenten per E-Mail, weil er Bedenken hinsichtlich der Sicherheit der elektronischen Kommunikation hegte.

Als Händler von Produkten, die unter das Kriegswaffenkontrollgesetz fallen, ist der Antragsteller seit dem 1. April 2020 dazu verpflichtet, Meldungen über seine Kriegswaffenbestände elektronisch an das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) zu übermitteln (§ 10 Abs. 3 Satz 1 KrWaffKontrGDV). In diesem Zusammenhang hat auch das Bundesamt selbst die Vorgänge in seinem Aufgabenbereich weitestgehend auf den elektronischen Rechtsverkehr umgestellt und über die Antragsgegnerin mehrfach E-Mails mit personenbezogenen Daten des Antragstellers an diesen versandt. Dabei hielt es sich an die vom Bundesamt für Sicherheit und Informationstechnik (BSI) herausgegebenen Empfehlungen für IT-Sicherheit, wonach für den Versand von E-Mails hier eine einfache Transportverschlüsselung notwendig, aber auch ausreichend sei.

Bei einer Transportverschlüsselung handelt es sich um eine Verschlüsselung auf dem Übertragungsweg der E-Mail, die von den meisten E-Mail Providern standardmäßig angeboten wird. Hiermit wird die E-Mail-Kommunikation zwischen den Servern des Absenders, des Providers und des Empfängers verschlüsselt und vor dem Zugriff Dritter geschützt. Zu unterscheiden ist dies von der „Ende-zu-Ende-Verschlüsselung", bei der es sich um eine Verschlüsselung des Inhalts einer E-Mail handelt.

Dem Antragsteller ging die gewählte Transportverschlüsselung nicht weit genug. Er verlangte eine qualifizierte Verschlüsselung und regte an, die E-Mails mittels der Software Chiasmus verschlüsseln zu lassen. Grund hierfür war die Befürchtung, durch die seiner Ansicht nach unzureichende Verschlüsselung als Händler von Kriegswaffen identifiziert werden zu können. So könne er leicht Opfer von Kriminellen werden, die an die von ihm vertriebenen Produkte gelangen wollten.

Im einstweiligen Rechtsschutzverfahren versuchte er daher, der Antragsgegnerin die Übermittlung von seinen personenbezogenen Daten auf elektronischem Wege ohne höhere Sicherheitsstandards untersagen zu lassen. Das VG Frankfurt/Main sah einen entsprechenden öffentlich-rechtlichen Unterlassungsanspruch des Antragstellers jedoch nicht gegebenen und lehnte seinen Antrag vollumfänglich ab.

**Elektronische Kommunikation im allgemeinen Verwaltungsverfahren**

Dazu führte das Gericht aus, dass die Übermittlung elektronischer Dokumente im allgemeinen Verwaltungsverfahren zulässig ist, soweit der Empfänger hierfür einen Zugang eröffnet (§ 3a Abs. 1 VwVfG). Dieser Grundsatz gilt nach den spezialgesetzlichen Vorschriften auch für die Kontroll- und Dokumentationspflichten nach dem Kriegswaffenkontrollgesetz.

Die gewählte Ausgestaltung der elektronischen Kommunikation mittels einer Transportverschlüsselung genüge zudem den datenschutzrechtlichen Anforderungen und verletze den Antragsteller daher nicht in seinen Rechten.

**Verarbeitungsgrundsatz der Integrität und Vertraulichkeit**

Dabei stellte das Gericht auf den Grundsatz der „Integrität und Vertraulichkeit“ aus Art. 5 Abs. 1 lit. f DSGVO ab. Hiernach muss bei der Verarbeitung personenbezogener Daten eine angemessene Sicherheit gewährleistet sein. Dies schließt die Vornahme geeigneter technischer und organisatorische Maßnahmen (sog. „TOM“) zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung der personenbezogenen Daten ein. Hierzu gehört auch, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten, noch die Geräte, mit denen diese verarbeitet werden, benutzen können (Erwägungsgrund 39 Satz 12 DSGVO).

**Technische Anforderungen an die Sicherheit der Verarbeitung**

Hinsichtlich der technischen Anforderungen für die sichere Verarbeitung personenbezogener Daten trifft Art. 32 DSGVO konkretere Vorgaben: Es sind diejenigen Maßnahmen zu treffen, die unter Berücksichtigung von acht Kriterien ein dem Risiko angemessenes Schutzniveau gewährleisten. Diese acht Kriterien sind: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

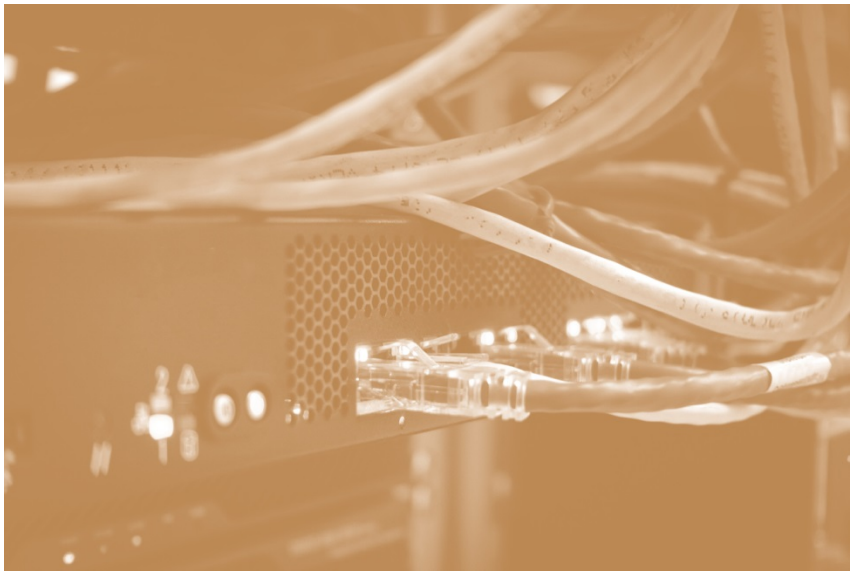
Hieraus folgerte das Gericht, dass lediglich eine unverschlüsselte elektronische Kommunikation unzulässig sei. Die Vorschrift mache jedoch keine Vorgaben in Bezug auf einzusetzende Verschlüsselungsalgorithmen oder bestimmte Schlüssellängen. Insofern habe die Antragsgegnerin durch die gewählte Transportverschlüsselung organisatorische Vorkehrungen zur Wahrung der Integrität und Vertraulichkeit nicht nur angestrebt, sondern bereits getroffen. Auf datenschutzrechtlicher Grundlage genüge dies gegenwärtig noch dem Standard, der zu verlangen sei.

**Höhere Anforderungen für sensible Daten oder besondere Datenkategorien?**

Offen ließ das Gericht allerdings die Frage, ob andere Maßstäbe angelegt werden müssen, wenn die elektronische Kommunikation die Verarbeitung personenbezogener Daten besonderer Kategorien im Sinne von Art. 9, 10 DSGVO betrifft.

Auch ob höhere Anforderungen an die Sicherheitsmaßnahmen für die Fälle gelten, in denen ein „Interesse krimineller und ressourcenreicher Dritter“ zu befürchten sei, ließ das Gericht unberücksichtigt, weil der Antragsteller ein solches Interesse Dritter im einstweiligen Rechtsschutzverfahren nicht ausreichend glaubhaft gemacht hatte.

Für diese hat jedoch bereits das VG Mainz mit Urteil vom 17. Dezember 2020 ausgeführt, dass insofern u.U. qualifizierte Schutzmaßnahmen zu ergreifen sind. Sofern aber keine Anhaltspunkte für besonders sensible Daten bestehen oder sonstige Umstände hinzutreten, sah auch das VG Mainz die Verwendung einer Transportverschlüsselung bei der elektronischen Kommunikation von Berufsgeheimnisträgern – in diesem Fall: Rechtsanwälten – für datenschutzrechtlich ausreichend.



## Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

## Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de