Keine Abdingbarkeit von technischen und organisatorischen Maßnahmen

Art. 32 DS-GVO (§ 26 KDG) verpflichtet den Verantwortlichen dazu, technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Bereits unter der Geltung der früheren Rechtslage, § 9 BDSG a. F. , § 6 KDO, wurde in Praxis und Lehre darüber diskutiert, ob diese Regelung zur Disposition von Betroffenen steht, mit der Konsequenz, dass diese den Verantwortlichen von dieser Verpflichtung befreien können.

Diese Frage wird u. a. bei der Versendung von E-Mails virulent. Können Betroffene rechtswirksam in die unverschlüsselte Versendung von personenbezogenen Daten und ggf. auch von solchen besonderer Kategorie, einwilligen?

Neu aufgekommen ist diese Frage, nachdem ein Vermerk der Hamburger Datenschutzaufsicht[1] bekannt geworden ist. Darin wird die Ansicht vertreten, der Verantwortliche könne grundsätzlich ein niedrigeres Schutzniveau wählen, wenn Betroffene darin einwilligen.

Die gegenteilige Ansicht wurde in einem Beschluss der Österreichischen Datenschutzbehörde[2] vom 16.11.2018 vertreten. Eine Einwilligung im Sinne des Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO sei schon deshalb nicht statthaft, weil die Einwilligung an dieser Stelle nicht dazu diene, eine Rechtsgrundlage für die Datenverarbeitung zu schaffen, sondern um von – gegebenenfalls erforderlichen – Datensicherheitsmaßnahmen zum Nachteil von Betroffenen abweichen zu können.

Einigkeit besteht zwischen beiden Behörden soweit sie vom Verantwortlichen die Gewährleistung eines angemessenen Schutzniveaus fordern. Der Verantwortliche muss also entsprechende technische und organisatorische Maßnahmen bei sich etabliert haben und vorhalten. Die Einwilligung Betroffener kann nach beiden Ansichten nicht dazu führen, Verantwortliche von der Erfüllung einer europäischen Verordnung zu dispensieren. Art. 32 Abs. 1 DS-GVO lässt dem Verantwortlichen keine Wahlmöglichkeit hinsichtlich der grundsätzlichen Gewährleistungspflicht.[3]

Es bleibt dann die Frage, ob Betroffene auf die Anwendung der vom Verantwortlichen grundsätzlich bereitgestellten Sicherungsmaßnahmen durch eine Einwilligung verzichten können. Diese Frage brauchte die Österreichische Datenschutzbehörde nicht zu klären, da die Voraussetzungen dafür in dem zu entscheidenden Fall nicht gegeben waren. In ihrem Vermerk spricht sich die Hamburgische Datenschutzbehörde für die Möglichkeit einer Abdingbarkeit von technisch-organisatorischen Maßnehmen aus, wenn Betroffene unter der o. g. Voraussetzung eine entsprechende Einwilligung erteilt haben. Wenn Betroffen mit einer Einwilligung darüber entscheiden können, „ob“ ihre personenbezogenen Daten verarbeitet werden können, müssen sie erst recht entscheiden können, „wie“ diese verarbeitet werden.

---

[1] https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf
[2] DSB-D213.692/0001-DSB/2018 vom 16.11.2018
[3] Jandt in Kühling/Buchner, DS-GVO BDSG 3. Auflage 2020, Rn. 40

Diese Schlussfolgerung ist keineswegs zwingend. Die Möglichkeit der Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO (§ 8 KDG) steht systematisch im Zusammenhang mit der Frage der Zulässigkeit der Datenverarbeitung, nicht aber mit den spezifischen Pflichten bei der Umsetzung.[4] Die Einwilligung erlaubt nur überhaupt die ansonsten verbotene Verarbeitung personenbezogener Daten. Dies muss aber in datenschutzkonformer Weise geschehen. Die rechtfertigende Wirkung, die Art. 6 Abs. 1 lit. a DS-GVO (§8 KDG) der Einwilligung zugesteht, bezieht sich systematisch nur auf das „Ob" der Verarbeitung, nicht aber auch vollumfänglich auf das „Wie".[5] Würde man die Einwilligung so weit für zulässig erachten, wie dies im Vermerk der Hamburger Datenschutzbehörde zum Ausdruck kommt, handelte es sich nicht mehr um eine Einwilligung, sondern um einen Verzicht auf Datenschutz. Noch in seinem Tätigkeitsbericht 2018 hat der Hamburgische Datenschutzbeauftragte zur alten Rechtslage einen Verschlüsselungsverzicht nur dann für zulässig angesehen, wenn die „Umstände der Verarbeitung" einen solchen rechtfertigen.[6] Als Beispiel für solche Umstände wurden dort medizinische Notfälle und wechselnder Auslandsaufenthalt benannt. Aus solchen rechtfertigenden Umständen kann aber keine generelle Aussage abgeleitet werden. Insoweit leidet der neue Vermerk darunter, dass die Frage der Zulässigkeit einer so weitreichenden Einwilligung ausschließlich aus Sicht Betroffener in den Blick genommen wird. Aus Sicht von Verantwortlichen ermöglicht diese Rechtsauffassung es, Betroffene gleich zu Beginn eines Vertragsverhältnisses eine entsprechende Einwilligungserklärung unterzeichnen zu lassen, um sich auf diese Weise die Möglichkeit einer vereinfachten Kommunikation zu sichern. Dabei ist es kein Hindernis, dass der Verantwortliche eine Verschlüsselungstechnik vorhalten muss, die er aber praktisch nicht nutzt.

Für die Gewährleistung eines einheitlichen Datenschutzniveaus innerhalb der Europäischen Union und um eine naheliegende Umgehung datenschutzrechtlicher Vorschriften zu vermeiden, ist die Möglichkeit der Abbedingung von technisch-organisatorischen Maßnahmen durch eine Einwilligung Betroffener abzulehnen.

Darüber hinaus ist zu berücksichtigen, welche Art der Verschlüsselung zu wählen ist. Bei der Transportverschlüsselung (TLS) wird die Übertragung der E-Mail zwischen den beteiligten E-Mail-Servern gesichert durch Verschlüsslung übertragen.[7] Generell wird die Verwendung einer Transportverschlüsselung datenschutzrechtlich ausreichend sein, sofern keine Anhaltspunkte für besonders sensible Daten bestehen oder sonstige Umstände hinzutreten.[8] Die Kommunikation mittels obligatorisch transportverschlüsselter E-Mails ist auch im geschäftlichen Verkehr durchaus als sozialadäquat und wohl derzeit noch als Stand der Technik einzustufen.[9]

Eine Ende-zu-Ende-Verschlüsselung zeichnet sich demgegenüber dadurch aus, dass eine Entschlüsselung des Inhalts nur den Kommunikationspartner (Absender und Empfänger) möglich ist, also nur derjenige den Inhalt der Nachricht zur Kenntnis nehmen kann, der auch den passenden Entschlüsselungsmechanismus hat.

---

[4] Jandt Kühling/Buchner, DS-GVO BDSG 3. Auflage 2020, Rn. 40
[5] Paal in Pall Pauly, DSGVO 3. Auflage 2021, Rn. 4a
[6] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit TB 2018, S.121.
[7] Ausführliche Darstellung https://www.kdsa-ost.de/images/CONTENT/KDSA/Mbericht/dok/5._KDSAost-TB_2020.pdf Seite 59 ff.
[8] VG Mainz Urteil vom 17.12.2020 - 1 K 778/19.MZ
[9] Gasteyer/Säljemar, NJW 2020, 1768 [1771

Bei personenbezogenen Daten, die unter Art. 9 oder Art.10 DS-GVO (§ 4 Nr. 2, §12 KDG) fallen, sind in jedem Fall „besondere Schutzmaßnahmen“ zu ergreifen, da insoweit schon aufgrund der allgemeinen datenschutzrechtlichen Wertung stets von einem hohen Risiko ausgegangen werden muss.[10] Eine angebrachte „besondere Schutzmaßnahme“ wäre z.B., die zu übermittelnden sensiblen Daten in eine passwortgeschützte ZIP Datei als E-Mail-Anlage zu versenden. Eine mit Passwort geschützte PDF-Datei wäre eine weitere Möglichkeit. Den damit verbundenen Implementierungsaufwand kann man in Bezug auf die Vertraulichkeit vernachlässigen. Bei einer fehlerhaften Zustellung einer Nachricht mit sensiblen Informationen an falsche Empfänger, z.B. durch einen Tippfehler bei Eingabe der E-Mail-Adresse, würde TLS nicht mehr den erforderlichen Schutz bringen. Sobald die Nachricht beim Empfänger in seinem Postfach eingegangen ist, liegt diese im Klartext vor. Ein solcher Fehlversand wäre deshalb als Datenschutzverstoß zu werten, da die erforderliche Sorgfalt bei der Versendung personenbezogener Daten besonderer Kategorie außer Acht gelassen wäre.

Sind die sensiblen Informationen in einer verschlüsselten Anlage enthalten, wo das „Geheimnis“ (Passwort) um die Anlage zu entschlüsseln nur den berechtigten Empfängern bekannt ist, können alle anderen Empfänger (Dritte) nicht auf den Inhalt der Anlagen zugreifen. Sie würden nur Kenntnis von dem unverschlüsselten Inhalt in der E-Mail-Nachricht erlangen. Die sensiblen Informationen in der Anlage bleiben geschützt.

KDSA Ost
Die Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des
Katholischen Militärbischofes

[10] VG Mainz Urteil vom 17.12.2020 - 1 K 778/19.MZ