Können Betroffene auf ein „angemessenes Datensicherheitsniveau“ verzichten?

Die Datenschutzkonferenz hat dem am 24. November 2021 mit einem neuen Beschluss eine recht klare Absage erteilt. Relevant ist dies z.B. für die Übermittlung sensibler Daten per Email, die immer wieder auf datenschutzrechtliche Bedenken stößt. Im Frühjahr 2021 hatte der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sich dazu noch abweichend positioniert und die Möglichkeiten für eine Einwilligung in ein niedrigeres Datensicherheitsniveau dargelegt. Was gilt nun?

„Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.“

So eindeutig beginnt der neue Beschluss der Datenschutzkonferenz vom 24.11.2021. Damit stellt sich die DSK gegen die vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HamBfDI) noch als möglich angesehene Einwilligung in ein geringeres Datensicherheitsniveau. Der HamBfDI hatte in seinem Vermerk aus dem Frühjahr 2021 dazu Stellung bezogen, ob Betroffene auf das nach Art. 32 DSGVO erforderliche Datensicherheitsniveau verzichten können.

Ein typischer Anwendungsfall in der Praxis ist die Frage, ob sensible Daten wie Gesundheitsdaten oder Steuerinformationen von Ärzten, Anwälten oder Steuerberatern per Email ohne eine Ende-zu-Ende-Verschlüsselung verschickt werden dürfen, wenn die betroffene Person damit einverstanden ist, eigentlich aber nach Art. 32 DSGVO die Verschlüsselung erfolgen müsste.

Zur Erinnerung: Art. 32 DSGVO gibt Datenverarbeitern, Verantwortlichen wie Auftragsverarbeitern, vor, ein für die Datenverarbeitungssituation angemessenes Niveau der Datensicherheit zu schaffen. Dies hat der Datenverarbeiter durch Abwägung der Risiken der Verarbeitung, der Implementierungskosten und der Art, Weise und des Umfangs der Datenverarbeitung zu ermitteln und entsprechende Maßnahmen zu treffen. Das Niveau und die zu treffenden Maßnahmen sind dabei nicht abschließend vorgeschrieben, sondern risiko- und situationsabhängig in eigener Verantwortung zu prüfen und festzulegen. Bei der Übermittlung sensibler Daten wie Gesundheitsdaten per Email wird es regelmäßig erforderlich sein, dass die Email-Kommunikation Ende-zu-Ende verschlüsselt ist. Eine reine Transportverschlüsselung ist regelmäßig nicht ausreichend. Zu datenschutzrechtlichen Problemen führt es, wenn eine der beiden Seiten dieses Verschlüsselungsniveau nicht einhalten kann oder will. In diesen Fällen stellt sich die Frage, ob solche Daten trotzdem versendet werden dürfen, wenn der Betroffene darin einwilligt.

Stellenwert der Selbstbestimmungsrechte der Betroffenen in Bezug auf Art. 32 DSGVO aus Sicht des HamBfDI

Die hier zu beantwortenden Rechtsfragen berühren die Grundfesten des Datenschutzrechts. Die DSK hält eine Einwilligung nach ihrem neuen Beschluss nur in dokumentierten Einzelfällen für denkbar, wenn der Betroffene ausdrücklich und eigeninitiativ darum bittet.

Nach der Analyse des HamBfDI ist dies eine Frage des (informationellen) Selbstbestimmungsrechts über personenbezogene Daten. Zwar sei es das Ziel der DSGVO, ein allgemeines, möglichst hohes und einheitliches Schutzniveau für personenbezogene Daten zu schaffen. Gleichzeitig solle aber auch das individuelle Selbstbestimmungsrecht der Betroffenen über ihre personenbezogenen Daten geschützt werden. Zum Selbstbestimmungsrecht gehört es nach Ansicht des HamBfDI auch, Entscheidungen darüber zu treffen, Daten unter einem suboptimalen Schutz verarbeiten zu lassen. Der HamBfDI vergleicht dies mit der Veröffentlichung sensibler Daten: Diese möge zwar in manchen Fällen nicht die objektiv klügste Entscheidung sein, es stehe dem Einzelnen aber zweifelsohne zu und es ist von der Rechtsordnung gedeckt, solche unklugen Entscheidungen über seine personenbezogenen Daten ohne Bevormundung zu treffen. So solle

es sich auch mit der Entscheidung über ein niedrigeres Schutzniveau bei der Datenübertragung verhalten.

Die DSK sieht dies nun deutlich restriktiver und begrenzt diese Fälle auf solche, in denen der Betroffene die Initiative ergreift. Dies dürfte systematische Angebote, in ein niedrigeres Schutzniveau einzuwilligen, ausschließen.

Jedenfalls: Verpflichtung der Verarbeiter

Selbst wenn danach dem Betroffenen die freie Entscheidung zugebilligt wird, ein niedrigeres Schutzniveau für seine personenbezogenen Daten zu wählen, bleiben die verantwortlichen Datenverarbeiter nach Art. 32 DSGVO verpflichtet, ein geeignetes und angemessenes Niveau sicherzustellen und anzubieten. Dabei merkt der HamBfDI an, dass es für die Bestimmung des Niveaus nicht auf den Einzelfall, sondern auf das typische, für solche Verarbeitungssituationen angemessene Niveau ankommt. Deshalb müssten Datenverarbeiter stets und unabhängig von dem möglichen Willen einzelner Betroffener die Vorkehrungen treffen, die zur Einhaltung des angemessenen Niveaus erforderlich sind. Im konkreten Fall der Email-Kommunikation heißt das, dass die Ende-zu-Ende-Verschlüsselung zumindest auf der eigenen Seite technisch und operationell ermöglicht werden muss.

Dadurch wird nach Ansicht des HamBfDI dann auch die Freiwilligkeit der Betroffenen gewahrt: Diese können zwischen einem angemessenen und abgesenkten Schutzniveau frei entscheiden, auch, weil der Verpflichtete auch ein angemessenes Schutzniveau anbietet. Die Einwilligung in ein suboptimales Schutzniveau ist nicht notwendig, um die Leistung erhalten zu können. Problematisch sind also dann vor allem solche Geschäftsmodelle, im Rahmen derer keine angemessenen Maßnahmen umgesetzt werden. Die Freiwilligkeit könnte sich dann allenfalls in der freiwilligen Teilnahme widerspiegeln. Dieses Problem potenziert sich, wenn es sich um Anwendungen handelt, die für die Betroffenen dringend notwendig sind und/oder keine Alternativen am Markt bestehen. Für die DSK reicht dies nicht – hier muss für eine wirksame Einwilligung zudem die Initiative vom Betroffenen ausgehen.

Einwilligung in niedrigeres Niveau möglich?

Nach der DSK ist eine Einwilligung in ein niedrigeres Datensicherheitsniveau damit nur in vereinzelten Ausnahmefällen zulässig. Der HamBfDI hatte dies noch weiter gesehen. In jedem Fall muss eine Einwilligung die Voraussetzungen der Art. 6 Abs. 1 UAbs 1 lit. a, Art. 7 DSGVO erfüllen, also insbesondere nach angemessener Aufklärung dokumentiert für den Einzelfall erteilt werden.

Noch einmal zusammengefasst bestehen also die folgenden Voraussetzungen:

1. Der Verantwortliche oder Auftragsverarbeiter hat das erforderliche Datensicherheitsniveau nach Maßgabe des Art. 32 DSGVO geschaffen. Die Möglichkeit der Einwilligung des Betroffenen soll nicht genutzt werden, um Kosten zu sparen und den Betroffenen niedrigere Datensicherheit „aufzudrücken".

2. Die Einwilligung des Betroffenen muss die strengen Anforderungen der Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO und Art. 7 DSGVO erfüllen, bei sensitiven Daten auch des Art. 9 Abs. 2 lit. a DSGVO. Insbesondere muss die Einwilligung freiwillig und informiert erfolgen.

3. Die Einwilligung muss, nach DSK-Position, im Einzelfall ausdrücklich auf Initiative des Betroffenen abgegeben werden. Systematische Angebote dürften damit nicht vereinbar sein. Der DSK-Beschluss begrenzt die Möglichkeiten damit erheblich

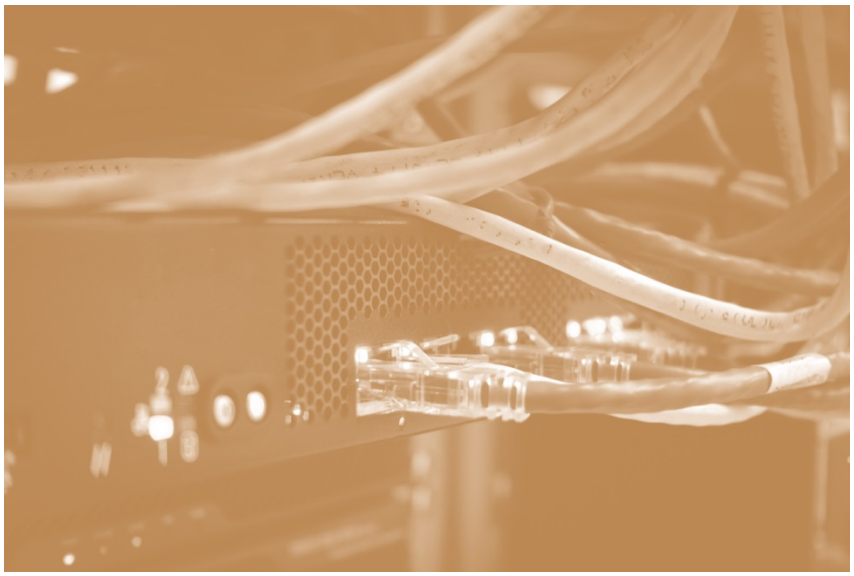
Kritik

Die Position der DSK ist mit Blick auf das informationelle Selbstbestimmungsrecht kritikwürdig: Es überzeugt kaum, dass Betroffene zwar in die Datenverarbeitung als solche einwilligen können, nicht aber in ein reduziertes Sicherheitsniveau. In der Praxis darf mithin der Arzt auch auf Anforderung des Patienten die Gesundheitsunterlagen nicht per einfacher Email übersenden. Ob sich diese Ansicht durchsetzt, ist fraglich – ein Beschluss der DSK jedenfalls bindet weder Verantwortliche, noch Aufsichtsbehörden. Er markiert indes das Risiko, ob Aufsichtsbehörden gegen eine

bestimmte Verarbeitung einschreiten werden oder nicht. Gleichzeitig wird man die DSGVO auch im europäischen Kontext und ggf. losgelöst von der deutschen Grundrechtstheorie verstehen müssen. Die Diskussion ist an dieser Stelle ganz sicher nicht beendet.

Der Vermerk des HamBfDI ist abrufbar unter:
https://datenschutz-hamburg.de/assets/pdf/Vermerk-Abdingbarkeit_TOMs.pdf

Der Beschluss des DSK ist abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf



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