Gesundheitsversorgung in Zeiten der Datenschutz-Grundverordnung (DSGVO)–
Wissenschaftliche Tagung am 18.09.2018 an der Goethe-Universität Frankfurt am Main

Datenschutzrechtliche Zulässigkeit von Apps im Gesundheitswesen

Dr. Nils Ipsen, LL.M., Rechtsanwaltskanzlei lindenpartners

1. Für Apps im Gesundheitswesen gelten zwar grundsätzlich die gleichen datenschutzrechtlichen Anforderungen wie für andere Verarbeitungen von Gesundheitsdaten. Jedoch besteht eine besonders große Anfälligkeit für Datenschutzverstöße, da Apps typischerweise auf Smartphones oder Tablets installiert sind, die die Nutzer nahezu ständig dabeihaben und über die sie einen Großteil ihrer Kommunikation abwickeln. Aus diesem Grund stellen sich einige datenschutzrechtliche Probleme mit besonderer Schärfe.

2. Jede Verarbeitung von Gesundheitsdaten durch Apps setzt voraus, dass eine gesetzliche Ausnahme vorliegt, da Gesundheitsdaten als besonders sensible Daten nur in bestimmten Ausnahmefällen verarbeitet werden dürfen (Art. 9 DSGVO). Zusätzlich muss auch ein allgemeiner Rechtfertigungsgrund gegeben sein (Art. 6 DSGVO).

3. In der Regel sind die Anforderungen der gesetzlichen Ausnahme und der erforderlichen Rechtfertigungen durch eine Einwilligung zu erfüllen. Diese Einwilligung muss ausdrücklich erfolgen, nur schlüssiges Verhalten reicht nicht. Überdies muss sie vor der ersten Datenverarbeitung vorliegen. Im Idealfall sollten die erforderlichen Einwilligungen deswegen bereits beim Download der App eingeholt werden.

4. Daneben bestehen auch andere Möglichkeiten, die Ausnahme- und Rechtfertigungsanforderungen zu erfüllen. Diese bleiben jedoch auf bestimmte Sonderfälle beschränkt. Die Verarbeitung zum Zwecke der Gesundheitsvorsorge kann z.B. nur dann als Ausnahme vom Verbot der Verarbeitung von Gesundheitsdaten dienen, wenn ein (Berufs-)Geheimnisträger die Verarbeitung verantwortet (Art. 9 Abs. 3 DSGVO).

5. Für die Analyse des Nutzerverhaltens durch Apps ist grundsätzlich eine gesonderte Einwilligung erforderlich. Gegenwärtig verdrängt die DSGVO insofern die bisher anwendbaren §§ 12, 13, 15 TMG. Eine (erneute) Änderung der Rechtslage wird voraussichtlich erfolgen, wenn die E-Privacy-Verordnung in Kraft tritt.

6. Die Grundsätze des Datenschutz by Design und des Datenschutz by Default spielen eine zentrale Rolle für Apps. Insbesondere muss der Nutzer steuern können, in welchem Umfang die App über die Schnittstellen auf die Funktionen des Gerätes zugreifen kann. Gerade Apps können potentiell auf die vielfältigen Funktionen der mobilen Endgeräte (z.B. Kamera, Mikrofon, Standort, Daten anderer Apps) und damit zusätzliche Daten zugreifen.

7. Apps sind so zu programmieren, dass sie dem Grundsatz der Datensparsamkeit genügen. Soweit möglich, muss der Nutzer die App anonym nutzen können. Sind anonyme Daten nicht ausreichend, sollten die Daten zumindest möglichst weitgehend pseudonymisiert werden.

8. Die App hat durch technische und organisatorische Maßnahmen ein angemessenes Sicherheitsniveau zu gewährleisten (Art. 32 DSGVO). Dabei ist insbesondere eine hinreichend sichere Authentifizierung und Datenübertragung vorzusehen. Die eingesetzte Technik muss die Einhaltung der Datenschutzgrundsätze dauerhaft gewährleisten. Das heißt, dass es eines regelmäßigen Abgleichs mit dem aktuellen Stand der Technik bedarf.

9. Eine Datenschutzerklärung ist erforderlich (Art. 13, 14 DSGVO). Insbesondere muss konkret erläutert werden, auf welche Daten die App zugreift (z.B. Kamera, Mikrofon) und wie diese Daten verarbeitet werden. Da Apps auf den vergleichsweise kleinen Bildschirmen der mobilen Endgeräte genutzt werden, ist zudem besonders auf die Verständlichkeit der Erklärung zu achten. Es kann sich deswegen anbieten, zusätzlich eine Kurzinformation bereitzustellen, die die wesentlichen Punkte enthält.

10. Neben den datenschutzrechtlichen Anforderungen der DSGVO sind auch die (nicht durch die DSGVO verdrängten) Anforderungen des Telemediengesetzes zu beachten. So besteht z.B. eine Impressumspflicht bei geschäftsmäßig angebotenen Apps (§ 5 TMG).