Technische Überprüfung:

Plattform- und Geräteunabhängigkeit	
App-Version und Betriebssystem	
Datentransport verschlüsselt ja/nein (https/http)	
Registrierung ja/nein und in welcher Form	
Nutzung von Analyse-Diensten (z.B. Google Analytics) und Werbenetzwerken	
Benötigte Zugriffsmöglichkeiten	
Analyse der AGB/Datenschutzangaben	

App-Monitoring – allgemeine Informationen

Bei der durchgeführten Analyse bzw. beim Monitoring von Apps geht es darum, sicherheits- und datenschutzrelevante Aspekte der App zu bewerten. Dabei geht es zunächst um Plattform(un)abhängigkeit, d. h. es wird einerseits untersucht, ob die Apps grundsätzlich auf den beiden größten App-Plattformen von Apple/iOS (und ggf. weiteren Anbieter) verfügbar sind und auf verschiedenen Endgeräten funktionieren und für diese optimiert sind. Anschließend wird die Sicherheit der Datenströme und des Datentransports bewertet. D. h., es wird überprüft, ob die Daten über eine gesicherte https-Verbindung übertragen werden. Dies gilt insbesondere für sensible und persönliche Daten wie etwa Passwörter oder Angaben zum Gesundheitszustand. Zur Analyse der Kommunikation der Apps wird Charles Proxy verwendet. Erfolgt die Kommunikation über ein http-Protokoll, zeigt dies an, dass die Kommunikation unverschlüsselt ist. Werden viele Datenströme mit Verwendung eines http-Protokolls angezeigt, ist dies ein Anzeichen dafür, dass bei dieser App genauer hingesehen werden sollte und insbesondere zu schauen ist, welche Daten bzw. Kommunikationsvorgänge über eine http-Verbindung transportiert werden.

Es wird weiterhin erfasst, ob für die App-Nutzung eine Registrierung vorgenommen werden muss und welche Daten dabei anzugeben sind (E-Mail, Log-in über Facebook, Angabe persönlicher oder gesundheitsbezogener Informationen etc.). Idealerweise ist keine Registrierung notwendig, das Anlegen eines Nutzerkontos kann jedoch je nach angebotenen Funktionalitäten notwendig werden. Überprüft wird auch, ob sich der Nutzer mit seinem Klarnamen anmelden muss oder ggf. auch eine „anonyme“ (funktionsfähige) E-Mail-Adresse und Nutzernamen verwenden kann.

Im Anschluss wird analysiert, ob die Anwendung Webtracking-Dienste, bspw. Google Analytics, verwendet und ob dies DSGVO-konform erfolgt. Die Nutzung entsprechender Webanalysedienste ist rechtlich grundsätzlich legal und entspricht den berechtigten

Interessen der Hersteller, sofern bestimmte Voraussetzungen erfüllt werden. Der Hersteller ist etwa angehalten, die Rechtsgrundlage zu nennen, transparent in der Datenschutzerklärung über das Webtracking zu informieren (Tool, Betreibergesellschaft, welche Daten werden gespeichert und verarbeitet), eine Anonymisierung der IP-Adresse des Nutzers vorzunehmen, eine Widerspruchsmöglichkeit sowie eine Opt-out-Option/ein Opt-out-Cookie anzubieten. Sicherzustellen ist auch, dass das auftragsdatenverarbeitende Webanalyseunternehmen, sofern es in einem Drittstaat wie den USA Daten verarbeitet, nach der EU-US-Privacy-Shield (Grundlage für Datenübermittlungen in die USA, mit dem bestimmte Nutzerrechte, z. B. Recht auf Auskunft, verbunden sind) zertifiziert ist. In diesem Zusammenhang wird auch überprüft, ob seitens des Entwicklers Werbenetzwerke in der App verwendet werden.

Anschließend folgt eine Zusammenstellung der Zugriffsrechte bzw. App-Berechtigungen, die der Nutzer der App gewähren muss. Dabei handelt es sich sowohl um „normale“ Berechtigungen, die für eine stabile Anwendung notwendig sind, als auch um weitergehende und ggf. zustimmungspflichtige Berechtigungen. Hier geht es nicht allein um die Anzahl der Berechtigungen, sondern vielmehr um die Notwendigkeit und Nachvollziehbarkeit (z. B. benötigt ein „einfaches“ Symptomtagebuch im Regelfall keinen Zugriff auf den ungefähren oder genauen Standort)

Des Weiteren werden abschließend noch die Allgemeinen Geschäftsbedingungen (AGB) des jeweiligen App-Herstellers analysiert. Der Fokus liegt hier auf den Angaben zum Datenschutz bzw. zur herstellerbezogenen Nutzung der bereitgestellten Daten – mit dem Ziel, die zuvor analysierten Ergebnisse mit den Angaben in den AGBs abgleichen zu können und eventuell vorhandene Widersprüche bzw. noch offene Fragen an den Hersteller herausfiltern zu können. Bei dieser Analyse spielen die Angaben über „Erhebung, Verarbeitung und Nutzung personenbezogener Daten“, „Nutzung von Analysediensten und Cookies“, „Rechte des Nutzers“, „Einwilligung in die Datenverarbeitung“, „Widerspruchsmöglichkeiten“, „Speicherorte der Daten“ und „Datenschutzbeauftragter“ eine wichtige Rolle. Auch ein vollständiges Impressum sowie eine Aufklärung über die Grenzen der App sind hierbei wichtig.

Hinzugefügt werden muss in diesem Zusammenhang, dass über dieses Verfahren und aus rechtlichen Gründen nicht zu erkennen oder herauszufinden ist, was konkret mit den erhobenen Daten passiert bzw. ob der Hersteller die Daten (rechtswidrig) an Dritte weitergibt. Ein Weiterverkauf der Daten kann nicht zweifelsfrei ermittelt werden. Offenkundig wird lediglich, ob die AGBs dies erlauben würden oder ausschließen.

-