Bundesinstitut
für Arzneimittel
und Medizinprodukte

BfArM, Kurt-Georg-Kiesinger-Allee 3, 53175 Bonn

Herr Tim [redacted]

ABTEILUNG Verwaltung - Justitiariat
BEARBEITET VON [redacted]
TEL
E-MAIL

HAUSANSCHRIFT [redacted]

TEL
FAX
E-MAIL poststelle@bfarm.de
INTERNET www.bfarm.de

Bonn, 14. Juni 2022

GESCHZ [redacted]

IFG-Bescheid
Prüfliste zu digitalen Gesundheitsanwendungen (nach Digitale-Versorgung-Gesetz)
Ihre Zeichen und Nachricht vom: [#248439], 06.05.2022

Sehr geehrter Herr [redacted]

mit Ihrer Anfrage nach dem Informationsfreiheitsgesetz vom 06.05.2022, baten Sie um Auskunft zum Prüfverfahren von digitalen Gesundheitsanwendungen im Bundesinstitut für Arzneimittel und Medizinprodukte.

1.) Erfolgt eine Prüfung digitaler Gesundheitsanwendungen (siehe: https://diga.bfarm.de/de) durch das Bundesinstitut für Arzneimittel und Medizinprodukte vor Aufnahme auf die Seite?

Ja, diese Prüfung wird durch das BfArM ausgeführt.

a.) Falls ja: Wie genau wird die Prüfung durchgeführt? / Bereitstellung von: Prüflisten, Anweisungen zur Durchführung von Prüfungen oder Beispielen von Prüfergebnissen (sofern notwendig auch geschwärzt).

Die Prüfung der Anwendungen im Bereich Datenschutz und Datensicherheit unterteilt sich in zwei Bereiche:

1) <u>Plausibilitätsprüfung der Angaben der Antragsteller zu den Anlagen 1 und 2 der Digitale Gesundheitsanwendungen-Verordnung (DiGAV)</u>
In diesem eher formalen Prüfungsschritt wird überprüft, ob die Checklisten der Anlagen 1 und 2 vollständig und korrekt ausgefüllt wurden und angegebene Begründungen für „nicht zutreffend“-Antworten schlüssig sind. Des Weiteren wird geprüft, ob nötige Unterlagen ein-

gereicht wurden [Zertifikat zum Nachweis der Umsetzung eines Informationssicherheitsmanagementsystems (ISMS), Konformitätserklärung sowie Penetrationstest].

2) Inhaltliche Prüfung
Die Angaben in der Checkliste werden mit Hilfe des zur Verfügung gestellten Zugangs zur App bzw. zur Webanwendung überprüft. Hierzu werden die einzelnen Anforderungen der Anlagen 1 und 2 der DiGAV durchgegangen und so beispielsweise die Datenschutzerklärung geprüft, die Authentisierungsmethoden getestet und die Datenverbindungen analysiert. So wird zum Beispiel die Anforderung 3 der Anlage 1 der DiGAV (Datenschutz) „Erfolgt die Abgabe von Einwilligungen und Erklärungen der betroffenen Person durchgängig ausdrücklich, d. h. durch eine aktive, eindeutige Handlung der betroffenen Person?“ geprüft, indem nachgesehen wird, ob Einwilligungen vorausgewählt sind und die Einwilligung aktiv bspw. durch Setzen eines Häkchens durchgeführt werden muss. Des Weiteren werden die eingereichten Unterlagen (Zertifikat zum Nachweis der Umsetzung eines ISMS, Konformitätserklärung sowie Penetrationstest) überprüft.

Zukünftig werden die Prüfungen durch die Vorlage eines verpflichtenden Datenschutzzertifikats gemäß § 139e Absatz 11 des Fünften Buches Sozialgesetzbuch (SGB V) sowie eines Datensicherheitszertifikats gemäß § 139e Absatz 10 SGB V ersetzt.

Wenn Sie Einsicht in Unterlagen und Prüfergebnisse haben möchten, so bitten wir Sie dies für eine konkrete digitale Gesundheitsanwendung anzufordern. In diesem Fall wäre es möglich den Hersteller um Erlaubnis der Herausgabe von, eventuell geschwärzten, Unterlagen zu bitten.

2.) Muss eine erneute Prüfung erfolgen, sofern ein Update der Entwickler vorliegt (bspw. bei einer neuen Version einer Android-App)? Nach welchen Kriterien erfolgt eine neue Prüfung?

Der Hersteller einer digitalen Gesundheitsanwendung (DiGA) ist jederzeit verantwortlich für die Gewährleistung aller datenschutz- und informationssicherheitsbezogenen sowie sonstigen rechtlichen Anforderungen an sein Medizinprodukt. Sollte es ein Update einer App oder einer Anwendung geben, das Einfluss auf die Einhaltung der Datenschutz- und/oder Datensicherheitsanforderungen hat, so muss dies als wesentliche Veränderung angezeigt werden. In diesem Rahmen wird dann eine erneute Prüfung der App oder der Anwendung durchgeführt.

3.) Gab es Feststellungen im Kontext von bisherigen Prüfungen im Bereich Datenschutz bzw. IT-/Informationssicherheit, die zu einer "Nichtfreigabe" einer Anwendung geführt haben? Falls ja welcher Art waren diese (Statistik + Namen der Anwendungen)?

Die Ablehnung eines Antrags zur Aufnahme in das DiGA-Verzeichnis ist in der Regel auf unterschiedliche Gründe zurück zu führen, die neben Fragestellungen im Bereich Datenschutz und Datensicherheit häufig auch die Evidenz betreffen. Eine alleinige Ablehnung aus Gründen von mangelhaften Datenschutz und Datensicherheit gab es bisher erst einmal. Grund der Ablehnung war hier der Datenabfluss von personenbezogenen Daten, der nicht die Anforderung des § 4 Absatz 3 der DiGAV erfüllte [„Die Verarbeitung von personenbezogenen Daten zu den Zwecken nach Absatz 2 darf im Rahmen einer digitalen Gesundheitsanwendung durch die digitale Gesundheitsanwendung selbst sowie bei einer Verarbeitung personenbezogener Daten im Auftrag nur im Inland, in einem Mitgliedstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.“].

Zum Schutz von Betriebs- und Geschäftsgeheimnissen gemäß § 6 IFG dürfen die Namen der negativ beschiedenen digitalen Gesundheitsanwendungen nicht herausgegeben werden.

Rechtsbehelfsbelehrung
Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Bundesinstitut für Arzneimittel- und Medizinprodukte erhoben werden.

Mit freundlichen Grüßen
Im Auftrag

[redacted]