Bundesinstitut
für Arzneimittel
und Medizinprodukte

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

[redacted]

ABTEILUNG Medizinprodukte
BEARBEITET VON Florian Strauch
TEL +49 (0)228 99 307-4006
E-MAIL [redacted]@bfarm.de

HAUSANSCHRIFT Kurt-Georg-Kiesinger-Allee 3
53175 Bonn
TEL +49 (0)228 99 307-0
FAX +49 (0)228 99 307-5207
E-MAIL poststelle@bfarm.de
INTERNET www.bfarm.de

Per E-Mail: [redacted]

Bonn, 20.10.2021

GESCHZ [redacted]

Ihre digitale Gesundheitsanwendung im Verzeichnis nach § 139e Fünftes Buch Sozialgesetzbuch (SGB V)

Name der DiGA: [redacted]
Hersteller: [redacted]
DiGA-ID: [redacted]
Versionsnummer der digitalen Gesundheitsanwendung: [redacted]
Softwareversion: [redacted]

Aufforderung zur Stellungnahme zur Einhaltung des Datenschutzes

Sehr geehrter Herr [redacted],

wir sind darauf aufmerksam gemacht worden, dass in Ihrer DiGA [redacted] eine regelmäßige Datenkommunikation mit dem US-Dienstleister Microsoft stattfindet. Unsere interne Prüfung hat dies bestätigt. In Ihrer Datenschutzerklärung schreiben Sie hierzu:

„Von uns erhobene, technische Daten informieren uns darüber, welche Hard- und Software Sie verwenden. Diese Abfrage erfolgt im Rahmen der Funktionsgewährleistung bei Abstürzen mittels Microsoft AppCenter (http://appcenter.ms) als Drittanbieter (Microsoft Corporation). Es werden bei Abstürzen folgende Informationen abgefragt:

1. *Geräteart (Hersteller und Version),*
2. *Betriebssystemversion,*
3. *App-Version der* [redacted] *sowie*
4. *Screen beziehungsweise Funktionsaufruf (Stelle innerhalb der App) des Absturzes.“*

Der Datenabfluss findet jedoch auch statt, wenn kein Absturz erfolgt ist. Dadurch ist zusammen mit der IP-Adresse die Erhebung von Nutzungsdaten möglich.

Dies ist nicht zulässig, da IP-Adressen als personenbezogene Daten einzustufen sind und eine Verarbeitung von personenbezogenen Daten außerhalb der EU oder Drittstaaten ohne Angemessenheitsbeschluss nach Artikel 45 Datenschutz-Grundverordnung (DSGVO) nicht zulässig und nach § 4 Absatz 3

der Digitale Gesundheitsanwendungen-Verordnung (DiGAV) ausgeschlossen ist (siehe auch Handreichung zu Datenverarbeitung außerhalb Deutschland, https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/Datenverarbeitung_ausserhalb_Deutschlands_FAQ.pdf?__blob=publicationFile).

Wir bitten Sie daher um unverzügliche Prüfung des Sachverhalts sowie um Stellungnahme zu den oben genannten Punkten bis zum 22.10.2021 um 12 Uhr an diga@bfarm.de.

Mit freundlichen Grüßen
Im Auftrag

Florian Strauch

Dieses Schreiben enthält in Übereinstimmung mit § 33 Absatz 3 Satz 1 SGB X nur eine Namenswiedergabe und keine Unterschrift.

[redacted]

[redacted]

Bundesinstitut für Arzneimittel und Medizinprodukte
Herr Florian Strauch
Kurt-Giesinger-Allee 3
53175 Bonn

[redacted]

[redacted] 10.2021

[redacted]

Hersteller: [redacted]

DIGA-ID: [redacted]

[redacted]

Stellungnahme zu Ihrer Nachricht vom 20.10.2021

Ihr GSCH-Zeichen: [redacted]

Sehr geehrter Herr Strauch,

danke für Ihr Schreiben vom 20.10.2021. In Ihrem Schreiben beziehen Sie sich auf eine Prüfung der Softwareversion [redacted]. Entsprechend des BfArM-Bescheides vom 25.08. ist im DiGA-Verzeichnis inzwischen Softwareversion [redacted] hinterlegt.

Unabhängig davon haben wir eine Prüfung des Sachverhaltes vorgenommen und führen diese nachfolgend im Detail aus. Augenscheinlich beziehen Sie sich auf EUGH und BGH Urteile, die im Kern festhalten, dass IP-Adressen personenbezogene Daten sind.

Der EUGH hat bereits in seiner Entscheidung von 2016 festgestellt, dass eine gesetzliche Regelung nur restriktiv ist, wenn die Verarbeitung solcher Daten zulässig ist, soweit dies technisch zum Besuch einer Seite / eines Dienstes erforderlich ist (v. 19.10.2016, Az. C-582/14). Die Speicherung von IP-Adressen muss sich an den Maßstäben des Datenschutzes messen lassen. Wir folgen daher Ihrer Aussage, dass IP-Adressen personenbezogene Daten sind.

Der EUGH hat jedoch darüber hinaus klargestellt, dass in eine Beurteilung einfließen muss, ob die rechtlichen Mittel den Betreiber allgemein hierzu in die Lage versetzen, eine Zuordnung vornehmen zu können und die IP-Adresse damit einer bestimmten Person zugeordnet werden kann.

[redacted] [redacted] [redacted]

[redacted]

Der BGH ((Urt. v. 16.05.2017, Az. VI ZR 135/13) gab dazu ebenfalls weitere klare Erläuterungen, sodass eine Interessenabwägung, ob eine IP-Adresse ein Personendatum ist oder eben nicht, im individuellen Einzelfall geprüft werden muss und nicht verkürzt werden darf. Es geht stets um die Abwägung zwischen dem Persönlichkeitsrecht Einzelner im Kontext zum Sicherheitsinteresse des Betreibers und damit der Analyse von Gefahren u.a. potentieller Angriffe. Die Fehler- und Absturzanalyse hat alleinig zum Ziel, diese technisch (ohne konkrete Nutzerwissen) aufzudecken, um Sicherheitslücken zu erkennen und zu minimieren. Bei Abstürzen handelt es sich um unerwünschtes Verhalten von Applikationen, welche unbedingt vermieden werden sollen. Abstürze sind potentielle Lücken für Angriffe.

Tatsächlich wird durch das BfArM aus unserer Sicht im Sinne der Nutzeranalyse und Datenerhebung leider die Tatsache (unabhängig von den Appherstellern) nicht geprüft, dass es sich bei den App-Store-Anbietern Apple und Google um ausländische Firmen handelt, welche eine Software zentral für Nutzer zur Verfügung stellen. Dabei prüft und speichert auch ein Store-Anbieter bereits die IP-Adresse bei Store-Nutzung und logt auch die Downloads von Applikationen. Dies ist bereits dort wichtig, damit auch die Nutzer über das Betriebssystem, nach einem Download, Updateinformationen erhalten. Darüber hinaus fragt aber auch der Store wiederkehrend, ob die App aktiv im Betriebssystem verwendet wird, abstürzt oder ggf. auch gelöscht wird (eventbezogene Übermittlung unabhängig vom DiGA-Hersteller). Die Einschränkung des BfArM, das DiGA-Hersteller Plattformdienste zu Absturzwecken auswerten können (beispielsweise über Einbindung von Zusammenführungsdiensten) ist tatsächlich wenig nachvollziehbar, da sie den Grundsatz der IT-Sicherheitsüberprüfung stark in der Möglichkeit beeinträchtigt, stetig Gefahrenminimierung zu betreiben. Damit ist die Nutzung von Store-Anbieter-Lösungen lt. übermittelter Interpretation ebenfalls nicht möglich. Vielmehr steht hier die Frage im Raum, ob ein Vertrieb über den App-Store der Betriebssystem-Anbieter (alle nicht Deutsch, sondern Amerikanisch) sowie die Nutzung dieser Betriebssysteme für die Bereitstellung von Diensten überhaupt erlaubt werden darf. Bei dieser Frage sollte klar werden, dass die verkürzte und einschränkende Argumentation aus Artikel 45 DSGVO so nicht bestehen kann und auch die Behauptung, dass die bloße Nutzung vom MS-Appcenter nicht zulässig wäre nach § 4 Absatz 3 DiGAV, welche eine Referenz zu § 134 SGB ist, nicht nachvollziehbar ist. Unabhängig von unserem Einzelfall sollte die Grundlage der Interpretation hier geprüft werden!

Ergänzend möchten wir noch konkret zu unserem Einzelfall Stellung nehmen:

Die [redacted] App wird über die Stores von Apple und Google bereitgestellt. Bei einem Download der App wird dem Store-Anbieter die IP-Adresse eines Nutzers mitgeteilt. Auch das Betriebssystem meldet Deinstallationen oder sucht nach Updates für Applikationen, um diese dem Nutzer via Store zur Verfügung zu stellen. Die IP-Adresse im Rahmen der App-Nutzung kann technisch nicht für eine Übermittlung außerhalb von Deutschland umgesetzt werden. Auch die Nutzung generell von Online-Diensten setzt eine Speicherung von IP-Adressen an Einwahlpunkten voraus – das ist eine wichtige Grundlage der IT-Sicherheit. Wenn deutsche Nutzer sich im Ausland befinden, findet durch die Telekommunikationsanbieter ebenfalls die Speicherung der IP des DiGA-Nutzers außerhalb von Deutschland statt. Alle diese Speicher-Aktionen finden unabhängig von einer Einbindung vom MS-Appcenter statt. Ein DiGA-Hersteller hat darauf keinen Einfluss.

Der Dienst vom MS-Appcenter speicherte ohne Bezug zu unserem System Absturzdaten. Abstürze sind dabei nicht nur vom Nutzer bemerkte „Schließvorgänge oder eingefrorene Services". Abstürze sind auch Nichtausführungen von eingeleiteten Events innerhalb der App – welche trotzdem eine

weitere App-Nutzung zulassen. Da uns selbst die IP-Adressen im Rahmen der DiGA Bereitstellungen so nicht vorliegen, können wir zu keinem Zeitpunkt eine Zuordnung vornehmen und damit sind Absturzdaten, die im Übrigen die App-Storeanbieter ohnehin einzeln sammeln (als amerikanische Bereitsteller des Stores), für uns tatsächlich nicht für eine Verbindung zu echten Nutzungsdaten geeignet. Uns hat in diesem Kontext ausschließlich interessiert, möglichst schnell eine dauerhaft stabile Software für unser Anwender zur Verfügung zu stellen.

Inzwischen ist unsere Software [redacted] stark im Einsatz und es ist gelungen durch die auch dem BfArM bekanntgegeben Anpassungen eine stabile Version zu etablieren. Gerne deaktivieren wir kurzfristig das MS-Appcenter, damit würden automatische Absturzmeldungen zukünftig nicht mehr generiert. Zwar erfolgt diese Anpassung von uns Hersteller nicht aus der notwendigen Erfüllung von gesetzlichen Auflagen im Rahmen der DiGA-Verordnung nach der Zulassung [redacted] erscheint jedoch zur Klarheit bzgl. der technischen Nutzung und Einschränkung auf den deutschen Rechtsraum angemessen.

Wir werden kurzfristig einen Antrag auf wesentliche Änderung im BfArM Webportal einreichen.

Herzliche Grüße

[redacted]