Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungsbedarf:

Die Industrie möchte ein rudimentäres Usability-Tracking und Crash-Reporting verwenden. Ohne diese Tracking-Daten fehlen ein wichtiges Indiz von Fehler und verwendeten Produktfunktionen. Ohne Tracking ist die Verbesserung von neuen Produktfunktionalitäten deutlich erschwert.

Änderungen in gemSpec_Frontend_Vers

Tracking im ePA-FdV

Im Folgenden sind die Anforderungen an **Tracking-Informationen** beschrieben.

A_15256_01 - ePA-Frontend des Versicherten: Verbot von Werbe~~- und Usability~~-Tracking
Das ePA-Modul Frontend des Versicherten und das ePA-Frontend des Versicherten DÜRFEN ein Werbe~~- und Usability~~-Tracking NICHT verwenden.<=

Im Folgenden wird unter Tracking Usability-Tracking sowie Crash-Reporting verstanden.

A_18766 - ePA-Frontend des Versicherten: Verbot von Tracking für ePA-Modul FdV
Das ePA-Modul Frontend des Versicherten DARF ein Tracking NICHT verwenden.<=

A_18767 - Tracking-Funktionen – Keine Weitergabe von Sicherheitsmerkmalen
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen implementiert, dass in den übermittelten Tracking-Informationen keine Sicherheitsmerkmale enthalten sind. <=

Hinweis: Sicherheitsmerkmale sind die Gerätekennung (DeviceID) und Session-Daten wie z.B. geheime oder private Schlüssel, Authentifzierungs- oder Autorisierungsbestätigungen.

A_18768 - Tracking-Funktionen – Verarbeitung und Auswertung der Tracking-Daten
Der Hersteller des ePA-Frontend des Versicherten SOLL die Verarbeitung und Auswertung der gesammelten Tracking-Daten des ePA-Frontends des Versicherten selbst durchführen und nicht von einem Drittanbieter durchführen lassen. <=

A_18769 - Tracking-Funktionen – Keine direkt identifizierenden personenbezogenen Daten
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen nutzt, dass die Tracking-Daten keine Daten enthalten, die natürliche Personen direkt identifizieren. <=

Hinweis: Personenbezogene Daten mit direktem Personenbezug sind bspw. Namen von natürlichen Personen.

© gematik – öffentlich_Entwurf

Tracking Anforderungen für Trackingdaten ohne Einwilligung

A_18770 - Tracking-Funktionen – Ohne Einwilligung des Nutzers
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, sicherstellen, dass die Tracking-Daten

- sich nur auf eine Nutzersession (von der ersten Interaktion des Nutzers mit dem ePA-Modul FdV bis zum Schließen des ePA-Modul FdV bzw. bis zum Inaktivitätstimeout) beziehen und nicht mit anderen Sessions des Nutzers verknüpft werden,
- weder personenbezogene noch pseudonymisierte personenbezogene Daten enthalten,
- keine nutzerbezogenen IDs oder gerätespezifischen IDs der Nutzergeräte enthalten,
- keinen Rückschluss auf Versicherte, deren Vertreter, Leistungserbringer oder Kostenträger ermöglichen, insbesondere Rückschlüsse anhand des Nutzerverhaltens über die Zeit oder über Nutzersessions hinweg,
- nicht durch die Verknüpfung mit personenbezogenen Daten aus anderen Quellen de-anonymisiert werden können.

<=

Hinweis: Andere Quellen sind z.B. Webtracker, Tracker von anderen Apps oder Trackingmerkmale des Betriebssystems (z.B. Hardware IDs, Network IDs oder Advertising IDs).

Hinweis: Der Nutzer muss über das Tracking im ePA-FdV informiert werden, bevor die Trackingdaten erhoben werden. Zum Beispiel in den Nutzungsbedingungen des ePA-FdVs.

A_18771 - Tracking-Funktionen – Generierung von Nutzersession basierte Trackingmerkmale

Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, beim Start einer Nutzersession die Nutzersession-ID zufällig neu generieren. <=

Anforderungen zur Einwilligung zum Session-übergreifenden Tracking

A_18772 - Tracking-Funktionen - Opt-in
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass diese Tracking-Funktionen bei der Installation des FdV standardmäßig deaktiviert sind und nur nach expliziter Einwilligung durch den Versicherten als Nutzer des FdV aktiviert werden (Opt-in). <=

A_18773 - Tracking-Funktionen – Kopplungsverbot
Das ePA-Frontend des Versicherten DARF, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpft, die Nutzung des ePA-Modul FdV NICHT an die Aktivierung dieser Trackingfunktion koppeln. <=

Hinweis: Das FdV muss voll-funktional ohne aktiviertes Tracking nutzbar sein.

A_18774 - Tracking-Funktionen - Einwilligungsinformation des Nutzers

© gematik – öffentlich_Entwurf

Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, den Versicherten vor der Einwilligung in die Aktivierung dieser Tracking-Funktionen in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen anzeigen:

- welche Daten durch die Tracking-Funktionen erhoben werden,
- zu welchen Zwecken die Daten erhoben werden,
- welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Nutzers möglich wären,
- wer die Empfänger der Daten sind,
- wie lange die Daten gespeichert werden.

<=

Hinweis: Diese Anforderung ist nicht durch einen alleinigen Verweis auf die AGB oder Nutzungsbedingungen des FdVs erfüllbar. Verständliche Form bedeutet eine kurze nicht juristische Erklärung zum Zweck des Trackings. Leicht zugängliche Form bedeutet direkt im FdV.

A_18775 - Tracking-Funktionen – Aktivierung erst nach Lesebestätigung der Einwilligungsinformationen
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, sicherstellen, dass die Einwilligung des Nutzers in die Aktivierung der Tracking-Funktionen erst erfolgt, wenn der Nutzer bestätigt, die angezeigten Einwilligungsinformationen gelesen zu haben.

A_18776 - Tracking-Funktionen – Deaktivierung ist jederzeit möglich
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass aktivierte Tracking-Funktionen jederzeit durch den Nutzer des FdVs deaktiviert werden können.

A_18777 - Tracking-Funktionen – Neue Generierung der Pseudonyme ist jederzeit möglich
Das ePA-Frontend des Versicherten SOLL, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass eine neue Generierung der pseudonymen Identifier jederzeit durch den Nutzer des FdVs veranlasst werden kann. <=

A_18778 - Tracking-Funktionen – Verbot von mehrmaligen Einwilligungsabfragen

Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass der Benutzer der App maximal einmal eine Abfrage zur Einwilligung des Trackings angezeigt bekommt. <=

Hinweis: Wenn der Benutzer seine Einwilligung zum Tracking nicht erteilt, darf das FdV den Nutzer nicht solange nach seiner Einwilligung fragen, bis der Nutzer diese erteilt.

© gematik – öffentlich_Entwurf