FRT CONSULT GMBH
IT Dienstleistungen & Business Dienstleistungen

frtpartner

Telefon: 09221 / 900 - 0
Telefax: 09221 / 900 - 111
Kontakt: info@frtconsult.de
Adresse: Kurt-Schumacher-Str. 23
95326 Kulmbach

Datenschutz-Newsletter IV / 2021

Aktuelles rund um den Datenschutz

Verarbeitung des 3G-Status im Beschäftigungsverhältnis

In den letzten Wochen erreichten uns eine Vielzahl von Anfragen zur Abfrage und Speicherung des 3G-Status von Mitarbeitern. Im Folgenden fassen wir die zentralen datenschutzrechtlichen Aspekte zusammen.

Die Überprüfung hat datensparsam zu erfolgen. Dafür eignet sich insbesondere die CovPassCheck-App.

Auf der Rechtsgrundlage der Einwilligung ist inzwischen eine Speicherung des Nachweises beim Arbeitgeber möglich, § 28b Abs. 1 IfSG. Andernfalls ist eine solche Speicherung unzulässig.

Sofern eine Speicherung des 3G-Status erforderlich ist (unter anderem, wenn zum Beispiel eine tägliche Kontrolle durch den gleichzeitigen Zugang vieler Mitarbeiter Verzögerungen im Betriebsablauf bedeuten würden), dürfen das Vorhandensein eines gültigen Nachweises, die Art des Nachweises und deren Gültigkeitsdauer dokumentiert werden (Grundsatz der Datensparsamkeit).

Die Speicherung in der Personalakte ist dabei unzulässig. Sie muss zwingend gesondert erfolgen.

Da es sich hier um Gesundheitsdaten handelt, ist besondere datenschutzrechtliche Sorgfalt geboten, um keine Datenschutzverletzungen zu riskieren.

Insbesondere ist hierbei an die Sensibilisierung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter, die Beschränkung des Zugangs zu den Daten und die Datensicherheit zu denken. Die technischen und organisatorischen Maßnahmen sind zu dokumentieren, Art. 30 Abs. 1 DSGVO.

Die erhobenen Daten sind spätestens am Ende des sechsten Monats nach ihrer Erhebung zu löschen, § 28b Abs. 3 IfSG, beziehungsweise zum Zeitpunkt des Wegfalls der Rechtsgrundlage.

Dies gilt nicht, sofern die Verarbeitung auf eine andere Rechtsgrundlage gestützt werden kann, beispielsweise zur Anpassung des betrieblichen Hygienekonzepts auf Grundlage der Gefährdungsbeurteilung, § 28b Abs. 3 IfSG.

Aufgrund von fortwährenden Änderungen in Gesetzen und Verordnungen kann diese Übersicht nur als Momentaufnahme verstanden werden.

Warnstufe Rot: Java-Sicherheitslücke 'Log4Shell'

Derzeit wird vor Angriffen gewarnt, die durch eine Sicherheitslücke der weit verbreiteten Log4j-Java-Protokollierungsbibliothek entstehen.

Gemäß Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) handele es sich um eine „extrem kritische Bedrohungslage".
Folglich wurde die Cyber-Sicherheitswarnung der Warnstufe Rot veröffentlicht.
Diese Sicherheitslücke muss von Server-Administratoren entweder durch vorläufige Notmaßnahmen oder durch ein Update geschlossen werden.
Weitere datenschutzrechtliche Informationen hat das Bayerische Landesamt für Datenschutzaufsicht unter https://www.lda.bayern.de/de/thema_log4shell.html zusammengefasst.

Bußgelder und Schadensersatzansprüche vermeiden

Bei Verstößen gegen die DSGVO drohen Geldbußen von bis zu vier Prozent des Umsatzes.
Die Datenschutzaufsichtsbehörden haben dazu ein Konzept zur Bußgeldbemessung vorgelegt (vgl. unser Datenschutz-Newsletter IV / 2019).
Gründe für verhängte Bußgelder sind beispielsweise eine fehlende Rechtsgrundlage (vgl. III / 2020) oder mangelhafte technische und organisatorische Maßnahmen (vgl. IV / 2020). Beschwerden von Betroffenen sind dabei oftmals Prüfungsanlass für Aufsichtsbehörden.
Zivilrechtliche Schadensersatzansprüche sind meist die Folge von nicht ausreichenden Auskünften an die Betroffenen.
Der Verantwortliche kann daher finanzielle Risiken erheblich minimieren, wenn er insbesondere den Außenauftritt (Homepage, Newsletter unter anderem) auf Datenschutzkonformität überprüft und Prozesse für Anfragen von Betroffenen bereithält, um fristgerecht und inhaltlich vollständig auf diese reagieren zu können.

Großbritannien plant eigenständiges Datenschutzrecht

Erst im Juni 2021 bekam Großbritannien den Angemessenheitsbeschlusses durch die Europäische Kommission. Nun plant die britische Regierung eine eigenständigere Datenschutzpolitik, die sich von den Vorgaben der DSGVO lösen soll. Dies könnte den Status als sicheres Drittland gefährden.
Bereits zum Zeitpunkt des Erlasses hatte der Europäische Datenschutzausschuss (EDSA) wegen der nationalen Regelungen zur Massenüberwachung durch Polizeibehörden und Geheimdienste Bedenken hinsichtlich des angemessenen Datenschutzniveaus im Vereinigten Königreich geäußert.
Ein Sprecher der EU-Kommission wies nach den Reform-Ankündigungen der britischen Regierung nun ausdrücklich darauf hin, dass man den Angemessenheitsbeschluss auch vor Ablauf der Vier-Jahres-Frist aussetzen oder beenden könne und dies bei Dringlichkeit auch unverzüglich geschehen kann.

Stand: 20. Dezember 2021

Alle Beiträge sind nach bestem Wissen zusammengestellt. Eine Haftung für deren Inhalt kann jedoch nicht übernommen werden. Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

Thomas Hesz, RA/StB; Marcel Peetz (M.Acc.), StB; Maria Gayer, RAin; Stefan Gräbe
Zertifizierte Datenschutzbeauftragte (TÜV)
Telefon: 09221 / 900 - 0
edsb@frtconsult.de www.frtpartner.de