Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

ich hoffe es geht Ihnen und Ihren Familien gut und Sie behalten auch in Zeiten der Corona Pandemie Ihren Optimismus und machen das Beste aus der Situation! Vielleicht bleibt aktuell ja auch etwas mehr Zeit für die Dinge, die immer liegen geblieben sind und endlich angegangen werden sollten. Das Thema „Datenschutz“ gehört natürlich üblicherweise nicht zu den liegen gebliebenen Themen ;-). Sollte dies aber doch der Fall sein, dann haben wir mit unserer Beratungsinformation den idealen Einstieg in das Thema.

In Ergänzung unseres bestehenden individuellen Beratungsangebots möchten wir Sie über aktuelle Datenschutzthemen aus Rechtsprechung, der Arbeit der Aufsichtsbehörden und der Politik informieren sowie mit Praxishinweisen und Hintergrundberichten aus unserem Team auf dem Laufenden halten. Dazu erhalten Sie heute unsere Beraterinformation mit dem Schwerpunkt „Covid-19“.

Die Corona-Pandemie stellt uns alle vor neue Herausforderungen. Auch der Datenschutz ist davon betroffen. Zum Beispiel im Beschäftigtendatenschutz stellen sich diverse Fragen. So ist zu klären, ob etwa vom Arbeitgeber Covid-19-Daten von Mitarbeitern und Kunden erhoben werden dürfen und was bei einer Verlagerung von Arbeitsplätzen ins Home-Office zu beachten ist. Wir unterstützen Sie als Ihr Datenschutzteam in all diesen Fragestellungen und laden Sie ein, sich per Telefon und E-Mail an uns zu wenden. Wir sind für Sie da!

Bleiben Sie gesund!

Ihr

Asmus Eggert

Inhalt

Verarbeitung von Gesundheitsdaten von Beschäftigten im Rahmen der Corona-Pandemie.....2
Ungeplant ins Home-Office – Muster-Arbeitsanweisung steht zur Verfügung.....2
Messenger-Dienst und Videokonferenzsysteme – Ein wachsender Bedarf.....3
Passwörter – BSI ändert Beratungsansatz zur IT-Sicherheit.....4
Datenlecks – Patientendaten in einer Cloud- Datenbank.....4

Verarbeitung von Gesundheitsdaten von Beschäftigten im Rahmen der Corona-Pandemie

Grundsätzlich ist eine Verarbeitung von Gesundheitsdaten – als besonders schützenswerte Daten - nur unter den restriktiven Bedingungen der DSGVO möglich. Viele Unternehmen fragen nun, was hier zu beachten ist.

Zur Eindämmung der Corona-Pandemie und zum Schutz von Mitarbeitern können personenbezogene Daten durchaus erhoben und verwendet werden, wenn

a. bei einem Mitarbeiter eine Corona-Infektion festgestellt wurde,
b. Kontakt mit einer nachweislich infizierten Person bestanden hat oder sonst der ernstlich begründete Verdacht einer Corona-Infektion besteht oder
c. sich dieser im relevanten Zeitraum in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet aufgehalten hat.

In diesen Fällen dürfen durch den Arbeitgeber alle Daten, einschließlich Gesundheitsdaten, erhoben und verarbeitet werden, die notwendig sind, um eine Ausbreitung des Virus unter den Mitarbeitern bestmöglich zu verhindern oder einzudämmen. Hierbei gilt, dass keine Daten auf Vorrat, sondern nur für diesen konkreten Zweck (Eindämmung der Corona-Pandemie und Schutz der Mitarbeiter) zu erfassen sind. Die erhobenen Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Es geht darum, verhältnismäßig zu agieren.

Aus dem Transparenzgebot der DSGVO und den Informationspflichten gemäß Art. 12 ff DSGVO sind die Mitarbeiter über die Verarbeitung von personenbezogenen Daten im Zusammenhang mit der Corona-Pandemie zu informieren.

Nach Wegfall des jeweiligen Verarbeitungszwecks, grundsätzlich also spätestens mit dem Ende der Pandemie, müssen die erhobenen Daten unverzüglich gelöscht werden. Es gilt der Grundsatz: So kurz wie möglich, so lange wie nötig!

Besondere Relevanz wird dieses Thema auch im Zusammenhang mit der graduellen Aufhebung der Corona-Beschränkungen erhalten. Denn in diesem Zuge wird es darum gehen zum Schutz der Mitarbeiter Maßnahmen zur Vermeidung von Ansteckung einzuführen (Regelmäßige Fiebermessung vor Beginn der Wiederaufnahme der Arbeit im Office, Schutz von Mitarbeitern mit Vorerkrankung und damit ggf. notwendige Erhebung von Vorerkrankungen etc.).

Wir haben für Arbeitgeber ein Muster mit Hinweisen erstellt, das Sie nutzen können. Bei Bedarf können Sie dieses bei Ihrem Datenschutz-Berater anfordern.

Ungeplant ins Home-Office – Muster-Arbeitsanweisung steht zur Verfügung

Nachdem bundesweit Kontaktsperren angeordnet worden sind, haben viele Arbeitgeber ihren Mitarbeitern erlaubt oder diesen angeordnet, zum Erhalt der Arbeitsfähigkeit und aus Gesundheitsfürsorge vorerst von zu Haus aus zu arbeiten. Darum waren ad hoc Voraussetzungen für die Einrichtung eines temporären Home-Office zu schaffen.

Dass auch für diese Arbeitsplätze grundsätzlich die gleichen Datenschutzanforderungen gelten wie im Unternehmen, ist eigentlich selbstverständlich. Die Umsetzung in der Praxis zeigt jedoch, dass das nicht immer möglich ist. Oft können die Mitarbeiter die technischen und organisatorischen Maßnahmen nicht oder nicht gleich sicherstellen. Insbesondere dann, wenn die Umsetzung spontan

und ohne großen Vorlauf erfolgte. Oft wissen die Beschäftigten auch nicht, was hier von ihnen erwartet wird, weil sich um diese Themen sonst der Arbeitgeber kümmert.

Auch wenn die Aufsichtsbehörden diese Sondersituation anerkennen und wie etwa das Unabhängige Datenschutzzentrum Schleswig-Holstein die Unternehmen und Mitarbeiter mit entsprechenden Hinweisen unterstützen, sollten Unternehmen kurzfristig mit den Beschäftigten im Home-Office klären, ob ausreichende Sicherheitsmaßnahmen bestehen. Ist das nicht der Fall, sollten gemeinsam Lösungen entwickelt werden, wie ein vertretbarer Mindeststandard im Datenschutz gewährleistet und umgesetzt werden kann.

Praxishinweis: Wir haben für Arbeitgeber eine Muster-Arbeitsanweisung für diese Situation erarbeitet, die Sie nutzen können, um den Beschäftigten deutlich zu machen, welche Pflichten sie im Home-Office zu beachten haben. Bei Bedarf können Sie dieses bei Ihrem Datenschutz-Berater anfordern.

Auch haben wir unsere Muster Home-Office Richtlinie (Telearbeit) überarbeitet, die für die Fälle gedacht ist, dass die Mitarbeiter jetzt oder nach der Pandemie planmäßig die Möglichkeiten von Home Office nutzen sollen können. Auch diese stellen wir unseren Kunden gerne zur Verfügung.

Messenger-Dienst und Videokonferenzsysteme – Ein wachsender Bedarf

In den letzten Jahren hat sich der Einsatz von Videokonferenzsystemen und Messengerdie nsten in der Kundenbeziehung, aber auch in Projekt- und Unternehmensteams, deutlich ausgeweitet. Mit dem rasanten Anstieg der Mitarbeiter, die im Zusammenhang mit den Kontaktsperren zur Bekämpfung der Corona-Pandemie im Home-Office arbeiten, hat sich nochmals ein deutlicher Schub ergeben. Das ein Unternehmen nicht bedenkenlos ein Videokonferenzsystem oder einen Messengerdienst beschaffen und einsetzen kann, zeigen die aktuellen Meldungen um das Videokonferenz-Tool Zoom.

Praxishinweis: Grundsätzlich muss mit dem Tool-Anbieter ein Auftragsverarbeitungsvertrag abgeschlossen werden. Zusätzlich ist zu prüfen, in welchem Land die vom Tool verarbeiteten Daten gehostet werden bzw. in welchem Land der Tool-Anbieter seinen Sitz hat. Sollte das Hosting außerhalb der EU erfolgen bzw. der Sitz des Anbieters außerhalb der EU liegen, so ist zu prüfen, ob der Anbieter im EU-US-Privacy Shield registriert ist. Falls eine solche Registrierung vorliegt, kann der Anbieter genutzt werden. Ist das Unternehmen nicht im EU-US-Privacy Shield registriert, kann eine datenschutzkonforme Nutzung über die Vereinbarung von Standarddatenschutzklauseln (im Englischen: Standard Data Protection Clauses) nach Art. 46 Abs. 2 lit c DSGVO. In allen Fällen müssen Sie beim Einsatz mit Kunden etc. über den Einsatz des Tools in der Datenschutzinformation informieren.

Ist die Entscheidung für ein Tool gefallen, sind auch bei der Nutzung einige Punkte zu beachten:

- Das Tool sollte in der Lage sein, Daten verschlüsselt zu senden.
- Die Datenschutzeinstellungen sollten anpassbar sein und richtig konfiguriert werden.
- Soll der Videocall aufgezeichnet werden, sind die Teilnehmer darüber vorab zu informieren. Dieser Mitschnitt ist nach einem festgelegten Zeitraum zu löschen.
- Wird der Bildschirm geteilt, ist sicher zu stellen, dass hier nur die für den Call relevante Daten und Informationen zu sehen sind. Es sollten daher nur die relevanten Applikationen und deren benötigten Fenster geöffnet sein.
- Der Arbeitsplatz für den Call sollte so gewählt sein, dass im Hintergrund ein neutraler Hintergrund abgebildet wird (einige Tools bieten die Option den Hintergrund über Weichzeichnung zu neutralisieren). Es sollten insbesondere keine Dritten im Hintergrund zu

sehen sein. Auch sollten im Hintergrund keine nicht für die Veröffentlichung gedachten Unternehmensinformationen oder (speziell im Home-Office) keine personenbezogenen Informationen zu erkennen sein.
- Die Teilnehmer müssen individuell eingeladen und zur Teilnahme berechtigt sein. Das anonyme Mithören bzw. Mitschauen muss ausgeschlossen sein.

Vor dem Einsatz der Messengerdienste und Videokonferenz-Systeme sind die Mitarbeiter zu den Datenschutzthemen zu sensibleren. Das kann über eine Arbeitsanweisung geschehen. Ggfs. ist der Datenschutzbeauftrage vorab einzubinden. Sollten Sie Unterstützung benötigen, sprechen Sie uns an.

Passwörter – BSI ändert Beratungsansatz zur IT-Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine unabhängige und neutrale Stelle und versteht sich als die Cyber-Sicherheitsbehörde des Bundes. Sie will die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft gestalten. Dazu bietet sie Kunden aus Verwaltung und Wirtschaft Dienstleistungen in den vier Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an.

In der 2020er-Ausgabe des BSI-Grundschutz-Kompendiums hat das BSI nun die Regelung des Passwortgebrauchs (ORP.4.A8) geändert: Die bisher geltende Verpflichtung, Passwörter regelmäßig zu ändern sowie feste Regeln für Länge und Komplexität vorzuschreiben, ist entfallen. In den letzten Jahren hat sich in der Security-Community die Ansicht verfestigt, dass solche festen Passwortregeln mehr schaden als nützen. Es hatte sich gezeigt, dass sich die Nutzer als Folge oft für zu schwache und schematisierte Passwörter entschieden haben.

Stattdessen gilt nun: *„In Abhängigkeit von Einsatzzweck und Schutzbedarf müssen sichere Passwörter geeigneter Qualität gewählt werden. Das Passwort muss so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort darf nicht zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden* (ORP.4.A22).“ Es bleibt bei dem Grundsatz, dass ein Passwort gewechselt werden muss, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

Das wird zu einer Entlastung der Mitarbeiter führen und sicher auch der IT-Abteilungen.

Datenlecks – Patientendaten in einer Cloud- Datenbank

In der letzten Zeit häufen sich Medienberichte, dass Ärzte oder Krankenhäuser Patientendaten in ungeschützten bzw. nicht ausreichend gesicherten Datenbanken verarbeiten. Aufgedeckt werden diese Fälle von Sicherheitsteams, die das Internet regelmäßig und gezielt durchkämmen und nach offenen Servern und nicht abgesicherten Datenbanken suchen. Ende Januar wurde über einen Fall in Frankreich berichtet, bei dem in einer Datenbank ca. 900.000 Dateien einsehbar waren, die offenbar aus Patientenakten stammten.

Die Patientendaten waren von Ärzten, die die Tools eines bestimmten Anbieters nutzen, in der vermeintlich sicheren medizinischen Cloud des Anbieters abgelegt worden. Die Sicherheitsforscher hatten dort Zugriff auf hochsensible Bilder, Videodateien und Unterlagen zu Eingriffen im Bereich plastischer Chirurgie, dermatologischer Behandlungen und Patientenberatungen, die von Kliniken mit der Technologie des Anbieters durchgeführt wurden.

Praxishinweis: Diese Fälle zeigen, wie wichtig die Auswahl von Tools und Cloud-Dienstleistern ist. Diese werden in der Regel als Auftragsverarbeiter tätig werden. Stellen Sie als Verantwortlicher sicher, dass Ihren Pflichten als Verantwortlicher nachkommen. Prüfen Sie auch in seit längerem laufenden Projekten, dass die Dienstleiter die notwendigen technischen und organisatorischen Maßnahmen getroffen haben und einhalten.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Yanick Röhricht, Asmus Eggert

Internet: www.mip-consult.de, www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 55 Abs. 2 RStV: Asmus Eggert