COVID-19-UNIT

DATENSCHUTZRECHT

SCWP SCHINDHELM

INHALTSVERZEICHNIS

Stand der Beiträge: 01.04.2020
Wir weisen darauf hin, dass sich aufgrund der gegenwärtigen Dynamik die Rechtslage jederzeit ändern kann. Auf Rückfrage können wir Ihnen gerne den dann aktuellen Sachstand erläutern.

Herausgeber, Medieninhaber, Redaktion: Zimányi & Fakó Rechtsanwälte | Lövőház u. 30 | 1024 Budapest | Registernummer: 2019 | Register: Budapester Anwaltskammer (H-1055 Budapest, Szalay u. 7.) | Tel: +36 1 270-9242, Fax: +36 1 270-9241 | budapest@scwp.hu | Zimányi & Fakó Rechtsanwälte ist Mitglied der SCWP Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien | Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr und können im Einzelfall die individuelle Beratung nicht ersetzen. Die Haftung der Autoren oder der Herausgeberin ist ausgeschlossen. | 2015 © Zimányi és Fakó Ügyvédi Iroda.

DEUTSCHLAND: DATENSCHUTZ IM HOME-OFFICE – WAS IST ZU BEACHTEN?

I. COVID-19: „HOMEOFFICE FÜR ALLE“

Die Verbreitung von COVID-19 hat dazu geführt, dass möglichst viele Mitarbeiter in das Homeoffice geschickt wurden, um das Gebot er sozialen Distanz effizient umzusetzen. Viele Unternehmen waren darauf nicht vorbereitet und haben die Möglichkeiten genutzt, die sich gerade geboten haben. Je länger die Situation andauert, umso wichtiger ist es jedoch, nach zu justieren und die Vorgaben der DS-GVO zu beachten. Hier sind insbesondere die technisch-organisatorischen Maßnahmen nach Art. 32 DS-GVO einzuhalten.

II. WELCHE GERÄTE DARF DER MITARBEITER VERWENDEN?

Der Mitarbeiter sollte nach Möglichkeit ein Endgerät des Arbeitgebers nutzen oder ein eigenes Gerät, das er ausschließlich für berufliche Zwecke verwendet. Eine Vermischung von beruflicher und privater Verwendung sollte dringend vermieden werden. Auch die Verwendung privater E-Mailkonten ist tabu.

III. WELCHE ARBEITSPROGRAMME SIND ZU VERWENDEN?

Um Hackern keine Chance zu geben, sollte darauf geachtet werden, dass keine veralteten Betriebssysteme zum Einsatz kommen. Diese sind eine beliebte Angriffsplattform für Viren, insbesondere Spy-Software.

IV. WAS IST BEI DER ONLINE-ZUSAMMENARBEIT ZU BEACHTEN?

Es gibt zahlreiche Angebote zur Durchführung von Videokonferenzen und Onlinezusammenarbeit. Hier gilt es, auch das Kleingedruckte zu lesen. Viele beliebte Services, insbesondere von Anbietern aus den USA, sind nicht datenschutzkonform, da sie die Datenverwendung für anderweitige Zwecke vorsehen oder gar eine Datenweitergabe an Dritte, z. B. bestimmte Betreiber sozialer Netzwerke. Oft ist ein Open-Source-Angebot die bessere, weil sicherere Alternative.

V. DARF IM HOMEOFFICE GEDRUCKT WERDEN?

Ausdrucke sollten nach Möglichkeit vermieden werden. Sind Ausdrucke zum Arbeiten zwingend erforderlich, muss für den Mitarbeiter auch ein Schredder oder eine ähnlich effiziente Methode zur Verfügung stehen, um Dokumente danteschutzkonform zu vernichten.

VI. WO DÜRFEN DOKUMENTE GESPEICHERT WERDEN?

Die Speicherorte für Dokumente sollten abschließend durch den Arbeitgeber bestimmt werden. Instruktionen zu der Verwendung von Clouds und zu Speicherungen außerhalb der Arbeitsebene sind zu erteilen.

VII. WIE IST DER ARBEITSPLATZ ZU GESTALTEN?

Zwischen Kindern und Küche ist es für manche gegenwärtig schwierig, einen ruhigen Arbeitsplatz zu finden. Dennoch sollte darauf geachtet werden, dass die Vertraulichkeit der beruflichen Tätigkeit gegenüber den anderen Haushaltsmitgliedern gewahrt bleibt.

VIII. SOLLTE EINE ABREDE MIT DEM MITARBEITER GETROFFEN WERDEN?

Eine gesonderte Abrede mit dem Mitarbeiter ist sehr zu empfehlen. Hier können der technische Status Quo und Verhaltensregeln festgehalten werden. Gerne sind wir Ihnen bei der Erstellung behilflich.

Karolin Nelles
Karolin.nelles@schindhelm.com

SPANIEN: WIE WIRD MIT GESUNDHEITS- UND STANDORTDATEN IN ZEITEN VON COVID-19 UMGEGANGEN?

I. DIE RECHTMÄSSIGE VERARBEITUNG VON PERSONENBEZOGENEN DATEN ZURZEIT

Die europäische Datenschutzgrundverordnung (DSGVO) sieht auch die Erhebung und Verarbeitung von personenbezogenen Daten ohne das ausdrückliche Einwilligung der betroffenen Person vor. Diese Ausnahmen können, in der durch das Coronavirus produzierte Krise in verschiedenen Szenarien Anwendung finden. Jene Ausnahmen beruhen vor Allem auf dem öffentlichen Interesse und/oder gesetzlich festgelegten Pflichten des Verantwortlichen der Datenverarbeitung.

In diesem Zusammenhang - Verarbeitung von Daten im Unternehmensbereich - hat die spanische Datenschutzbehörde „AEPD“ (Agencia Española de Protección de Datos) einen Bericht vom 11 März 2020, herausgegeben. In diesem wird analysiert welche rechtliche Grundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Auftreten der Krankheit in den Unternehmen besteht, wobei nach Ansicht der AEPD folgende Punkte von wesentlicher Bedeutung sind:

Rechtmäßigkeit der Verarbeitung begründet durch berechtigtes Interesse des Verantwortlichen - ohne die Erteilung der ausdrücklichen Einwilligung der betroffenen Person -, auf Grund von öffentlichem Interesse (Art. 6.1.e DSGVO) und um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6.1.d DSGVO). Dabei muss man diesem letzten Punkt in der aktuellen Lage eine gesonderte Wertung zukommen lassen, da es nicht nur um das Interesse der betroffenen Person, sondern auch um die Interessen von dritten geht.

Außerdem kann eine Datenverarbeitung auch durch sektorale Gesetze vorgeschrieben werden, und erübrigen dadurch die Notwendigkeit, eine ausdrückliche Einwilligung einzuholen.
Ein weiterer wichtiger Bereich in Verbindung mit der aktuellen Lage ist die Verarbeitung von Gesundheitsdaten, die durch die Ausnahmen die im Art. 9 DSGVO festgelegt sind, legitimiert wird:

- Erfüllung der Verpflichtungen im Bereich des Arbeitsrechts und Schutz der sozialen Sicherheit
- Schutz lebenswichtiger Interessen der betroffenen Person oder anderer natürlicher Personen, wenn die betroffene Person physisch oder rechtlich nicht in der Lage ist, ihre Einwilligung zu geben
- Öffentliches Interesse in Hinsicht auf die öffentliche Gesundheit (Art. 9.2.i)
- Erhebliches öffentliches Interesse
- Gesundheitsvorsorge oder Arbeits-medizin; u. a. Beurteilung der Arbeitsfähigkeit, medizinische Diagnostik, etc.

Gleichwohl der vorhergehenden Ausnahmen, schließt der Bericht der AEPD damit, dass auch in Zeiten einer Krise, die Rechte und Garantien jedes einzelnen in Bezug auf die Verarbeitung personenbezogener Daten sicherzustellen sind, va. die Grundsätze der DSGVO nach Art. 5.

II. ERFASSUNG VON STANDORTDATEN

Ein weiterer Aspekt, der im vorliegenden Bericht noch nicht in Betracht gezogen wurde, sind die neusten Entwicklungen in Bezug auf die

Erfassung von Standortdaten der Bürger, um die Infektionsketten nachvollziehen zu können und gegebenenfalls Kontaktpersonen frühzeitig zu warnen, um die Ausbreitung des Virus weiter eindämmen zu können, aber eventuell auch zum Durchsetzen von Quarantänen und Ausgangssperren.

Dieses Vorhaben wird nicht nur von der spanischen Regierung geprüft, sondern wird von Staaten weltweit in Betracht gezogen. Dabei stoßen die Staaten aber auf mehrere Probleme in dem Bereich des Datenschutzes.

Bisher wurde in den verschiedenen Beispiellösungen immer die Einwilligung der betroffenen Personen vorausgesetzt, welches mit der Aktivierung der App eingeholt werden soll, um somit die Erhebung und Verarbeitung der Standortdaten nach Art. 6 DSGVO legitimiert. Die derzeitige Gesetzgebung sieht jedoch bereits Situationen, wie die gegenwärtige vor, die die Anforderungen flexibler macht, sofern bestimmte Garantien erfüllt sind. In diesem Zusammenhang hat die Spanisch Datenschutzbehörde am 26/03/2020 ein Mitteilung veröffentlich in der die Grundlagen für die Verarbeitung von Gesundheits- und Standortdaten beschrieben werden.

Ein anderer Vorschlag sieht jedoch die Anonymisierung der Daten vor, wodurch jedoch die spätere Warnung von Kontaktpersonen nichtmehr möglich wäre und die erhobenen Daten somit nur noch einen Statistischen Nutzen hätten.

Nun wurde der Orden SND/297/2020 vom Gesundheitsministerium, vom 27 März veröffentlich, dessen Ziel ist es, einige der Mechanismen in der Gesundheitskrise zu digitalisieren und zu beschleunigen. Die Entwicklung einer App zur Selbsteinschätzung, bei der nur auf die Standortdaten zugegriffen wird, um zu verifizieren ob sich die betroffene Person in seiner Heimatprovinz aufhält.

Außerdem sieht der Beschluss auch vor, dass die Standortdaten von Mobilfunknutzer anonym von den Netzbetreibern an das nationale Statistikinstitut weitergeleitet werden, damit analysiert werden kann, wo sich die Personen vor und während des Alarmzustandes aufgehalten haben.

Bisher sind noch keine definitive Entscheidung getroffen worden und auch noch ist keine App bzw. Website des Gesundheitsamtes veröffentlich worden.

Zu allerletzt noch ein Tipp an unsere Kunden, in Zeiten der Krise gibt es leider auch immer Personen, die sich die besonderen Umstände zu Nutzen machen möchten und es daher in den letzten Tage vermehrt zu Phishing Attacken und E-Mails mit gefährlichen Anhängen kommt. Sobald sie den Verdacht haben, dass eine erhaltene E-Mail nicht vom eigentlichen Versender versandt worden sein könnte, löschen sie diese oder versuchen sie die Echtheit auf einem anderen Weg zu prüfen, bevor sie einen Anhang öffnen.

Klaus Maziul
k.maziul@schindhelm.com

Jose Tornero Marín
j.tornero@schindhelm.com

TSCHECHIEN: SMART QUARANTÄNE

I. HINTERGRUND

Seit 30.03.2020 testet die Gesundheitsbehörde in der Tschechischen Republik das Pilotprojekt der „Smart Quarantäne“. Das Ziel der Smart Quarantäne ist eine schnelle Identifizierung von Infizierten Personen, nachstehendes Testen auf die Erkrankung Covid-19 und entsprechende Isolierung von Kontakten der infizierten Person mit Anwendung der Informationstechnologien. Diese Maßnahme soll das bestehende Flächenverbot des freien Personenverkehrs, welches riesige negative Auswirkungen auf die Wirtschaft hat, mildern.

II. WIE DAS FUNKTIONIEREN SOLL?

Zur Trassierung der Kontakte werden die Daten über die Bewegung der infizierten Person mittels der rückwirkenden Lokalisierung ihres Mobiltelefons und Bankkarten dienen. Zu dieser Lokalisierung wird eine Einwilligung der infizierten Person zur Verarbeitung ihrer personenbezogenen Daten nach der DSGVO eingeholt. Die Telekommunikations-anbieter und Banken werden die Daten einer privaten technologischen Firma – Keboola Czech mitteilen, die eine „Bewegungskarte“ ausfertigt und mittels ihrer „call center“ mit der infizierten Person den gesetzpflichtigen epidemiologischen Fragebogen ausfüllt.

Die Informationen von dem Fragebogen werden der Gesundheitsbehörde übergeben. Die eigenen Lokalisierungsdaten werden im Fragebogen nicht angeführt, der Fragebogen beinhaltet jedoch eine ganze Reihe von personenbezogenen Daten der infizierten Person und ihrer möglichen Kontakte.

Die möglichen Kontakte der infizierten Person werden nachstehend durch die Gesundheitsbehörde angesprochen, d.h. ohne Feststellung ihrer personenbezogenen Daten mit der Hilfe des Telekommunikationsanbieters und der Hausbank. Die Leute können auch eine mobile Applikation „Smart Quarantäne“ nutzen, in deren Rahmen sie die Einwilligung zur Verarbeitung ihrer Daten vorab erteilen. In diesem Falle werden sie automatisch über den möglichen Kontakt mit einer infizierten Person informiert.

III. ÜBEREINSTIMMUNG MIT DSVGPO?

Eingliederung einer privaten technologischen Firma in diesem Projekt ist als ein Vorteil präsentiert. Dem Staat werden keine Lokalisierungsdaten übergeben. Die Verarbeitung von den an die Telekommunikationsanbieter und Banken mitgeteilten Daten ist durch eine informierte Einwilligung des Datensubjektes begründet. Die Einwilligung ist jederzeit zu widerrufen.

Strittig scheint jedoch die Verarbeitung von epidemiologischen Daten durch die private Firma, welche auch die Kontakte der infizierten Person betreffen, die aber keine Einwilligung zur Datenverarbeitung erteilt haben. Unklar ist auch die Stellung der einzelnen Teilnehmer (Verantwortlicher vs. Auftragsverarbeiter) und ihre Kompetenzen im Sinne DSGVO.

Grundlegende Frage wird die Effektivität einer solchen Maßnahme, weil die Nutzung der Smart Quarantäne nur auf die Subjekte, welche die Einwilligung erteilt haben, beschränkt ist. Die Antworten auf diese und weitere noch offene Fragen kann die Auswertung der Ergebnisse des Pilotenprojekts Smart Quarantäne in Kürze bringen.

JUDr. Eva Scheinherrová
scheinherrova@scwp.cz

Herausgeber, Medieninhaber, Redaktion: SCWP Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien | Lotterstraße 14 | 49078 Osnabrück | schindhelm.com | Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr und können im Einzelfall die individuelle Beratung nicht ersetzen. Die Haftung der Autoren oder der Herausgeberin ist ausgeschlossen.