Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

einige unserer Kunden erhalten inzwischen im Rahmen der Nachverfolgung von Infektionsketten Aufforderungen von Gesundheitsämtern, in denen diese Kontaktdaten von Mitarbeitern erfragen. Hinweise, was zu beachten ist, finden Sie in dieser Beratungsinformation auf Seite 2.

Ferner informieren wir Sie in dieser Ausgabe über drei Themen, die regelmäßig im Arbeitgeberalltag relevant sind und im Unternehmen geregelt sein sollten: Die Nutzung dienstlicher Informationen durch Beschäftigte für private Zwecke, die private Nutzung von Internet und E-Mail sowie die Thematik der verdeckten Videoüberwachung.

Bleiben Sie gesund!

Ihr

Asmus Eggert

Inhalt

COVID-19-Pandemie: Meldung von Kontaktdaten an das Gesundheitsamt

Zur Eindämmung der COVID-19-Pandemie und zum Schutz von Mitarbeitern können personenbezogene Daten und insbesondere auch Gesundheitsdaten erhoben und verarbeitet werden. Darüber hatten wir Sie bereits in unserer Beratungsinformation 04/2020 ausführlich informiert.

Im Rahmen der Verfolgung von Infektionsketten können Verantwortliche (in der Regel Arbeitgeber, aber auch soziale Einrichtungen, Vereine etc.) mit Anfragen von Gesundheitsämtern konfrontiert sein, die Kontaktdaten abfragen, um ggfs. infizierte Personen erreichen zu können.

Arbeitgeber sind nicht primär gesetzlich verpflichtet, proaktiv Daten der Beschäftigten im Hinblick auf einen COVID-19 relevanten Sachverhalt an Gesundheits- oder Ordnungsbehörden zu melden. Diese Verpflichtung trifft nur meldepflichtige Personen nach § 8 des Infektionsschutzgesetzes (IfSG). Das sind Ärzte oder Personen anderer Heilberufe.

Auf der Grundlage der Generalklausel des § 16 Abs. 1 und Abs. 2 Satz 3 IfSG können Gesundheitsämter jedoch Unternehmen auffordern und verpflichten, personenbezogene Daten (Kontaktdaten etc.) ihrer Beschäftigten zu übermitteln. Rechtsgrundlage ist dann Art. 6 Abs. 1 Satz 1 lit. c), Art. 9 Abs. 2 lit. h) DSGVO.

Praxishinweis: Die Meldepflicht für Verantwortliche (Arbeitgeber, soziale Einrichtungen, Vereine etc.) entsteht nur gegenüber der zuständigen Behörde. Das ist hier das Gesundheitsamt. Hingegen wäre die Aufforderung der Polizei vom Schutzzweck des IfSG nicht gedeckt.

Stellen Sie rasches, aber bedachtes Handeln sicher: Binden Sie bei einer solchen Anfrage den Datenschutzbeauftragten vor dem Erteilen der Auskunft ein. Sie müssen insbesondere verhindern, dass Trittbrettfahrer diesen Auskunftsweg nutzen, um an Mitarbeiterdaten zu kommen. Dies wäre eine Datenpanne nach Art. 33 DSGVO. Regeln Sie diese Themen im Rahmen Ihrer Notfallpläne bzw. Richtlinien.

Was ist ein sog. Mitarbeiterexzess im Datenschutz?

Für das Vorliegen eines Exzesses kommt es primär darauf an, ob die Beschäftigten subjektiv eigene Interessen verfolgen und die objektive Zweckbestimmung nicht mehr den ihnen zugewiesenen Aufgaben entspricht. Der Beschäftigte muss also objektiv eigene Zwecke verfolgen. Als Konsequenz wird er dadurch zum Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO. Überschreitet er hingegen nur seine Befugnisse, handelt er nicht im Exzess.

Beispiele für Mitarbeiterexzesse: Ein Paketbote nutzt die zur Zustellung hinterlegten Kontaktdaten eines Kunden für einen persönlichen Kontaktversuch; eine Kellnerin nutzt im Rahmen der Pandemiebekämpfung erhobene Gäste-Kontaktdaten, um einen Gast zu privaten Zwecken anzurufen; ein Bankangestellter nutzt Kontoinformationen von Familienangehörigen für eine zivilrechtliche Streitigkeit.

Werden Beschäftigte im Exzess selbst zu Verantwortlichen, können sie selbst Adressat von Bußgeldern sein. Auch Schadensersatzansprüche kommen in Betracht.

Grundsätzlich liegt aber die Verantwortlichkeit für das schuldhafte Handeln von Beschäftigten beim Unternehmen. Das gilt auch für den Datenschutz. Die Aufsichtsbehörden leiten aus der DSGVO den aus dem Kartellrecht entlehnten funktionalen Unternehmensbegriff ab. Daraus folgt die Anwendung des allgemeinen Funktionsträgerprinzips. Folglich werden nicht nur alle internen und ausgelagerten Abteilungen als wirtschaftliche Einheit angesehen. Auch Einzelpersonen (z.B. Mitarbeiter) werden als Unternehmensteil betrachtet, wenn sie für das Unternehmen wirtschaftlich tätig sind. Irrelevant ist

dabei die konkrete arbeits- bzw. vertragsrechtliche Beziehung zur Einzelperson, solange die Unternehmensleitung einen bestimmenden Einfluss auf die Person hat.

Nach der Rechtsprechung zum funktionalen Unternehmensbegriff wird das Verhalten von Führungskräften ebenso wie das von Angestellten, Zeitarbeitern und anderen Externen als Handlung dem Unternehmen zugerechnet. Eine Kenntnis der Geschäftsführung eines Unternehmens des konkreten Verstoßes oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse"), sind jedoch ausgenommen.

Praxishinweis: Für Unternehmen besteht immer das Risiko, dass diesen das Handeln des Mitarbeiters zugerechnet wird. Je nach Fallkonstellation kann es sogar zu einer gemeinsamen Verantwortlichkeit kommen. Daher ist es wichtig, sich von einem exzessiven Handeln eines Beschäftigten deutlich zu distanzieren. Grundsätzlich ist durch Richtlinien und Arbeitsanweisungen sicherzustellen, dass der Aufgabenbereich der Mitarbeiter klar definiert ist. Wird ein Exzess bekannt, ist die Frage der Meldung dieses Vorgangs an die Aufsichtsbehörde gem. Art. 33 Abs. 1 DSGVO zu prüfen. Binden Sie den Datenschutzbeauftragten hier sofort ein.

Unternehmen werden zudem die Identität von Beschäftigten, die Daten von Kunden etc. im Exzess genutzt haben, im Rahmen des Auskunftsanspruch aus Art. 15 lit. c) DSGVO beauskunften müssen („Empfänger oder Kategorien von Empfängern").

Etwaige Schadensersatzansprüche bestehen oftmals gegenüber den Beschäftigten und den Unternehmen in Gesamtschuld.

LAG Köln: Kündigung wegen privater Nutzung von Internet und E-Mail

Im Beschäftigtendatenschutz ist heutzutage die Frage nach Möglichkeit und Umfang der privaten Nutzung von Internet und E-Mail am dienstlichen-PC außerordentlich relevant. Verbietet der Arbeitgeber die private Nutzung, hat er auch das Recht und sogar die Pflicht die Einhaltung zu kontrollieren. Stellt er dabei Verstöße fest, wird man als Arbeitgeber daraus arbeitsrechtliche Maßnahmen ableiten wollen. Das ist nur möglich, wenn die Auswertung von Browserverlauf und E-Mail-Nutzung datenschutzkonform erfolgt.

Das LAG Köln hat nun entschieden (Urteil vom 07.02.2020 – 4 Sa 329/19), dass gegen die Erhebung und Verarbeitung personenbezogener Daten und deren Auswertung zur Internet- und E-Mail-Nutzung am Arbeitsplatz bei bestehendem Verbot der Privatnutzung kein prozessuales Verwertungsverbot besteht.

Die Auswertung der Nutzung war aus Sicht des Gerichtes in dem verhandelten Fall auf Basis der Rechtgrundlage des § 26 Abs. 1 BDSG (§ 32 Abs. 1 BDSG a.F.) zulässig. Die Auswertungen belegten die Verstöße und begründeten in dem verhandelten Fall die Rechtmäßigkeit der fristlosen Kündigung. Hingegen sah das Gericht die durch den Mitarbeiter erteilte Einwilligung nicht als Rechtsgrundlage gemäß § 26 Abs. 2 BDSG (§ 4a Abs. 1 BDSG a.F.) an, denn die verwendete Einwilligung war unpräzise, zu weit gefasst und daher unwirksam.

Praxishinweis: Hier zeigt sich einmal mehr, dass die Einwilligung eine sehr problematische Rechtsgrundlage im Bereich des Beschäftigtendatenschutzrechts ist. Es sollte daher immer geprüft werden, ob eine andere Rechtgrundlage – wie hier § 26 Abs. 1 BDSG – genutzt werden kann.

Die Verarbeitung von Daten auf Grundlage des § 26 Abs. 1 S. 1 BDSG setzt die Feststellung der Erforderlichkeit voraus. Es ist daher für die Auswertung des Nutzungsverhaltens zu prüfen, ob diese

zwingend in Anwesenheit des Beschäftigten erfolgen muss, weil dies ggü. der Prüfung in Abwesenheit als milderes Mittel anzusehen sein könnte.

Das LAG hat dies im vorliegenden Fall verneint: *„Eine in Anwesenheit des Klägers durchgeführte Auswertung der Log-Dateien der Internet-Browser sowie der empfangenen/gesendeten E-Mails ist unter Berücksichtigung ihrer Zwecke und der besonderen Umstände des vorliegenden Falls jedoch kein gegenüber der ohne seine Hinzuziehung erfolgenden Auswertung milderes Mittel. Die Art und Weise der Auswertung wäre auch bei Anwesenheit des Klägers keine andere gewesen. Es handelt sich dabei – soweit es die Log-Dateien betrifft – um das Auslesen von automatisiert generierten Einträgen zu Tag, Uhrzeit und URLs bestimmter mittels des Browsers aufgerufener Internetseiten.“*

Die Auswertung der Internet- und E-Mail-Nutzung eines Mitarbeiters in dessen Abwesenheit ist daher grundsätzlich möglich, wenn durch entsprechende Richtlinien bzw. Betriebsvereinbarungen der entsprechende rechtliche Rahmen geschaffen wurde.

EGMR: Verdeckte Videoüberwachung von Beschäftigten

Die Videoüberwachung von Beschäftigten ist ein wiederkehrendes Thema im Datenschutz. Nicht zuletzt auf der Basis der Rechtsprechung des Bundesarbeitsgerichts (BAG) ist man davon ausgegangen, dass die Art. 13 und Art. 14 DSGVO einer heimlichen Überwachungsmaßnahme, wie verdeckten Videoaufnahmen, entgegen stünden.

Herrschende Meinung war daher, dass eine Videoüberwachung des betroffenen Beschäftigten nur mit einer (Vorab-)Unterrichtung zulässig sei. Der Europäische Gerichtshof für Menschenrechte (*EGMR)* akzeptiert in seinem Urteil vom 17.10.2019 (App. No. 1874/13 u. 8567/13 – López Ribalda u.a./Spanien) nun, dass besondere Situationen besondere Maßnahmen erfordern, soweit gewisse Voraussetzungen eingehalten werden. D.h. auch eine verdeckte Videoüberwachung ohne Ankündigung kann zulässig sein. Diese Entscheidung wird sicher auch Auswirkungen auf die Rechtsprechung des BAG haben.

Praxishinweis:
Grundsätze zur datenschutzkonformen Ausgestaltung einer Videoüberwachung
Wenn Sie eine Videoüberwachung planen, binden Sie den Datenschutzbeauftragten frühzeitig ein. Unterscheiden Sie zwischen der Überwachung von öffentlichem Raum und nicht-öffentlichem Raum. Beachten Sie die drei Phasen der Videoüberwachung: (1) Beobachten, (2) Aufzeichnen (Speicherung/Verwendung) und (3) personenbezogene Auswertung. Für die Durchführung einer Videoüberwachung ist eine Datenschutzfolgenabschätzung durchzuführen und die Videoüberwachung ist im Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Je nach Zweck stellt sie eine technische und organisatorische Maßnahme dar. Vergessen Sie nicht die grundsätzliche Einhaltung der Informationspflichten nach Art. 13 und 14 DSGVO. Bei einer verdeckten Überwachung klären Sie sorgfältig die Rahmenbedingungen in Abstimmung mit Ihrem Datenschutzbeauftragten.

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.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