IN DIESER AUSGABE:

Newsletter Juli 2019

Datenschutz

Liebe Leserinnen und Leser,

zu Beginn des Inkrafttretens der DS-GVO waren die neuen Bestimmungen für die meisten Unternehmen nur ein „Mehr“ an Bürokratie. Durch erste Erfahrungen mit den Datenschutzbehörden sowie rechtlichen Beurteilungen konkretisiert sich immer stärker, was die DS-GVO für die Praxis bedeutet. Mit diesem Newsletter möchten wir Ihnen künftig vierteljährlich einzelne Themen und ihre Bedeutung für die täglich Arbeit vorstellen.

Neues Gesetz zur Arbeitszeiterfassung

Der Europäische Gerichtshof hat am 14. Mai 2019 entschieden, dass Arbeitgeber künftig Systeme einrichten müssen, mit denen die tägliche Arbeitszeit ihrer Mitarbeiter systematisch und zuverlässig erfasst wird. Hintergrund dafür ist die Sicherstellung der Einhaltung von Arbeitszeitregeln sowie des Gesundheitsschutz von Arbeitnehmern.

Was bedeutet dies für den Datenschutz?

Grundsätzlich ist der Einsatz von Zeiterfassungssystemen datenschutzrechtlich unkritisch, sofern bestimmte Kriterien berücksichtigt werden. Arbeitet man z. B. mit externen Dienstleistern zusammen, muss ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) geschlossen werden. Der Zweck des Zeiterfassungssystems, die Funktionalität sowie die Zugriffsrechte müssen konkret definiert werden, damit besonders vertraulich zu behandelnde Personaldaten, wie z. B. Krankheit und andere Abwesenheitsgründe, vor unbefugter Kenntnisnahme geschützt sind. Die frei zugängliche Aufbewahrung von sogenannten Stempelkarten oder Speicherung dieser Informationen ist demnach ein absolutes „No-Go“.

Internetzugang im Unternehmensnetz

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit der E-Mail- und Internetnutzung am Arbeitsplatz ist es entscheidend, ob der Arbeitgeber die private Nutzung am Arbeitsplatz gestattet hat. Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber in diesem Fall Tele-kommunikationsdienste- bzw. Telemediendienste-Anbieter. Er ist somit grundsätzlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber nur mit Einwilligung des betreffenden Mitarbeiters erlaubt. Dies betrifft insbesondere Daten, aus denen sich ergibt, welche Internetseiten von wem, wann aufgerufen wurden. Es ist empfehlenswert, dass der Arbeitgeber die Erlaubnis einer Privatnutzung an Bedingungen knüpft. Hierfür bieten sich eine Regelungen zum zeitlichen Umfang der Privatnutzung als auch konkrete Verhaltensregeln

Fortsetzung Seite 2

Fortsetzung von Seite 1

für die private Nutzung an. Die Einwilligung des Arbeitnehmers erstreckt sich dann auf die Kontrolle der Einhaltung der Nutzungsregelungen durch den Arbeitgeber. Da beim privaten E-Mail-Verkehr noch andere Zugriffsmöglichkeiten im Vordergrund stehen, sollte im gemeinsamen betrieblichen Interesse im Vorfeld eindeutig festgelegt werden, ob bzw. wie der Arbeitgeber auf die betrieblichen Mails im gemischt-privat-betrieblichen Postfach zugreifen kann. Es bietet sich an, all dies in der Betriebsvereinbarung festzulegen.

Ist die private Internet- und E-Mailnutzung nicht gestattet, hat der Arbeitgeber grundsätzlich das Recht, anhand von Protokolldaten stichprobenartig zu prüfen, ob die Nutzung betrieblicher Natur war. Im ersten Schritt ist es in diesem Fall zulässig und ausreichend, wenn zunächst nur eine Auswertung des Surfverhaltens ohne Personenbezug vorgenommen wird und zwar ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung der einzelnen Beschäftigten. Grundsätzlich ist datenschutz-freundlichen Maßnahmen zur Begrenzung der Internetnutzung – z. B. Nutzung von black- und/oder whitelists – der Vorzug zu geben. Eine personenbezogene Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten zu werten.

Quelle:
Konferenz der unabhängigen Datenschutz-Behörden des Bundes und der Länder

Datenschutz im Onboarding-Prozess

Der erste Arbeitstag im neuen Unternehmen ist für mehr als die Hälfte der Arbeitnehmer maßgeblich für die Bindung an den neuen Arbeitgeber. Ein gut strukturierter Onboarding-Prozess ist daher für die Mitarbeiterbindung entscheidend. Da schon beim Onboarding z. B. auf Personalfragebögen oder Krankenkassenbescheinigung personenbezogene Daten erhoben werden, sind bereits hier einige datenschutzrechtliche Vorgaben zu beachten. In erster Linie Ist es wichtig, dass nur solche Daten erhoben werden, die für die Begründung des Arbeitsverhältnisses tatsächlich erforderlich sind. Aus Nachweisgründen ist es zudem nötig, die Kommunikation der Datenschutzinformationen sowie die Vertraulichkeitsverpflichtungen und Geheimhaltungserklärungen ausreichend zu dokumentieren. Es empfiehlt sich, den gesamten Onboarding-Prozess - z. B. mit Checklisten - zu standardisieren und Dokumente einheitlich zu gestalten. So kann vermieden werden, dass relevante Aspekte übersehen werden.

Geschäftsgeheimnisgesetz vom 26. April 2019

Nach dem neuen GeschGehG (Geschäftsgeheimnisgesetz) müssen Unternehmen all ihre Geschäftsgeheimnisse - von Kundenlisten bis hin zu Konzepten o. ä. - durch angemessene Maßnahmen schützen. Tun sie dies nicht, stellen diese Daten bzw. Informationen vor dem Gesetz kein Geschäftsgeheimnis mehr dar und sind somit nicht schützenswürdig. Die Wahl der Schutzmaßnahmen richtet sich nach der Einstufung des Geschäftsgeheimnisses. Sie reichen von der „sicheren Aufbewahrung“, über „Passwortregelungen“ bis hin zu „Hinweisen in Verträgen“ und „Kennzeichnung von Dokumenten“. Hierbei ergeben sich durchaus Synergien mit der DS-GVO. Kundendateien sollte man beispielsweise als ein Geschäftsgeheimnis einstufen, da sie für das Unternehmen einen wirtschaftlichen Wert darstellen, zum anderen können sie aber auch personenbezogenen Daten enthalten und fallen damit unter die DS-GVO. Erfüllt man die Vorgaben der DS-GVO, ist in diesem Fall auch das GeschGehG eingehalten. Es empfiehlt sich unbedingt, den Bestand an Unternehmensinformationen zu bewerten. Zudem sollte jedes Unternehmen bei der Nutzung von Informationen, die neue Mitarbeiter von ihrem vorherigen Arbeitgeber mitbringen, achtsam vorugehen. Verstöße gegen das GeschGehG gelten als Straftat und werden somit entsprechend geahndet.

Bei Rückfragen zu diesem Newsletter wenden Sie sich gern an Ihren Datenschutzbeauftragten der ANMATHO AG.