ARBEITS- UND DATENSCHUTZRECHT

AUGUST 2018

Beschäftigtendatenschutz

Auch im Rahmen von Beschäftigungsverhältnissen kommt es typischerweise zur Datenverarbeitung. Hierbei muss sich sowohl an den generellen Regelungen der EU-Datenschutzgrundverordnung (DSGVO) als auch aufgrund der Öffnungsklausel in Art. 88 Abs. 1 DSGVO an dem neuen § 26 Bundesdatenschutzgesetz (BDSG) orientiert werden.

1. Vergleich der alten Rechtslage mit der neuen Rechtslage

Die Regelungen zur Verarbeitung von personenbezogenen Daten gelten wegen § 26 Abs. 7 BDSG nicht nur für solche Daten, die in Dateisystemen gespeichert werden, sondern auch für die Verarbeitung in Papierform, mündlicher Form sowie rein faktische Handlungen.

a) Allgemeines

Der Beschäftigtendatenschutz war bereits im alten Bundesdatenschutzgesetz in § 32 BDSG-alt speziell geregelt. Durch die Einführung der DSGVO am 25.05.2018 kam es nicht zu einer Neuregelung auf EU-Ebene, vielmehr machte die Bundesrepublik von der Öffnungsklausel des Art. 88 Abs. 1 DSGVO Gebrauch und erließ für die Verarbeitung personenbezogener Daten von Beschäftigen spezifische Vorschriften in § 26 BDSG-neu. Damit wird das hohe nationale Datenschutzniveau aufrechterhalten, wobei zu beachten gilt, dass diese Vorschriften des Beschäftigtendatenschutzes nur in der Bundesrepublik gelten und EU-weit lediglich die Regelungen der DSGVO zu beachten sind.

Darüber hinaus finden die Regelungen des § 26 BDSG für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes und der Länder, einschließlich der Kommunen, keine Anwendung. Jedoch bezieht sich die Terminologie „Beschäftigte“ in § 26 Abs. 8 BDSG nunmehr auch ausdrücklich auf Leiharbeitnehmer, sowohl im Verhältnis zum Entleiher als auch zum Verleiher.

Nach wie vor dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Dies ist nach § 26 Abs. 1 Satz 1 und Abs. 4 BDSG-neu ausdrücklich auch auf Grundlage von Kollektivvereinbarung zulässig. Dazu gehören Tarifverträge, Betriebs- und Dienstvereinbarungen, soweit die inhaltlichen Vorgaben des Art. 88 Abs. 2 DSGVO beachtet werden.

Weder das BDSG-neu noch die DSGVO kennen einen grundsätzlichen Ausschluss der Einwilligung im Beschäftigtenkontext, auch wenn eine freiwillige und damit wirksame Einwilligung aufgrund des Über-Unterordnungsverhältnisses regelmäßig nicht in Betracht kommt. Eine freiwillige Einwilligung kann jedoch dann vorliegen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Dasselbe gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Jedoch sind hohe Anforderungen an den Zweck einer solchen Einwilligung zu stellen. Daher ist die Einwilligung überwiegend in Konstellation möglich, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. Da die Einwilligung der speziellen Form bedarf, wird so zugleich der Nachweispflicht des Arbeitgebers nach Art. 7 Abs. 1 DSGVO Rechnung getragen. Der Arbeitgeber hat über den Zweck der Datenverarbeitung in Textform aufzuklären und auf den jederzeit möglichen Widerruf hinzuweisen.

Zur Aufdeckung von Straftaten dürfen Daten dann verarbeitet werden, wenn dokumentierbare, tatsächliche Anhaltspunkte vorliegen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das Interesse der oder des Beschäftigen an dem Ausschluss der Verarbeitung nicht überwiegt. Dabei ist eine Verhältnismäßigkeitsprüfung anzustellen.

b) Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten sind solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Verarbeitung solcher Daten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt.

Ausnahmen geltend jedoch auch im Beschäftigtenverhältnis, insbesondere in den Fällen, in denen eine ausdrückliche Einwilligung vorliegt oder die Verarbeitung erforderlich ist, damit der Arbeitgeber oder der Beschäftigte die ihm oder ihr aus dem Arbeitsrecht, dem Sozialrecht und Sozialschutz erwachsenen Rechte ausüben und seinen Pflichten nachkommen kann.

c) Zweckänderung

In der Regel erfolgt die Erhebung und Verarbeitung von Daten im Beschäftigtenverhältnis überwiegend nach

§ 26 BDSG im Rahmen eines Über-Unterordnungsverhältnisses. Dies hat zur Folge, dass auch für neue bzw. geänderte Verwendungszwecke noch ein innerer Zusammenhang zum Beschäftigtenverhältnis bestehen muss. Somit ist eine Verwendung zu völlig anderen Zwecken - wie beispielsweise zu Werbezwecken - unzulässig, da dieser Zweck mit dem ursprünglichen Zweck unvereinbar ist.

2. Meldepflicht von Datenschutzverletzungen

In einer Zeit von Hacking, Phishing und sonstigen Cyberangriffen wuchs die Besorgnis, dass Unternehmen nicht genug tun, um den Schutz der Daten, die sie speichern, vor kriminellen Hackern sicherzustellen. Daher bestimmt die DSGVO nun, dass im Falle eines jeden solchen Angriffs diese Datenschutzverletzung innerhalb von 72 Stunden nach Bekanntwerden der Verletzung gemeldet werden muss.

Dies gilt selbstverständlich auch für Personaldaten. Hierbei ist die beachten, dass der Arbeitgeber seinen Mitarbeitern ohne unangemessene Verzögerung mitteilen muss, wenn ihre personenbezogenen Daten gestohlen wurden.

3. IT-Nutzung am Arbeitsplatz

Unternehmen fragen sich immer häufiger, ob sie ihren Beschäftigten die Nutzung der betrieblichen Informations- und Kommunikationstechnik zu privaten Zwecken erlauben sollen. Davon ist grundsätzlich abzuraten, da für den Arbeitgeber damit erhebliche Nachteile einhergehen.

Erlaubt man die private Nutzung der betrieblichen Mittel durch die Beschäftigten, ist der Arbeitgeber als Dienstanbieter im Sinne des TKG und TMG anzusehen und ist somit dem Fernmeldegeheimnis unterworfen. Dies hat konsequenter Weise zur Folge, dass der Arbeitgeber ohne Einwilligung des Beschäftigten bereits keinen Zugriff mehr auf die E-Mail-Accounts des Mitarbeiters hat. Dies betrifft nicht nur die privaten E-Mails des Beschäftigten, sondern auch die dienstlichen, soweit in dem Account diese nicht auseinander zu halten sind. Insgesamt ist zu sagen, dass ein Arbeitgeber, der als Dienstanbieter im Sinne des TKG bzw. TMG anzusehen ist und damit an das Fernmeldegeheimnis gebunden ist, die Zugriffsmöglichkeiten auch für die betrieblichen Kommunikationsergebnisse verliert. Selbstredend erschwert dies die Einhaltung gesetzlicher Dokumentations- und Aufbewahrungspflichten und macht den Arbeitgeber bei der Ausübung seiner Direktions- und Kontrollrechte von der Einwilligung seiner Beschäftigten abhängig. Vermeiden lässt sich dies nur durch eine strikte Trennung privater und dienstlicher Nutzung.

Soweit keine ausdrückliche Genehmigung der privaten Nutzung dienstlicher Kommunikationsmittel vorliegt, ist grundsätzlich von einem Verbot der privaten Internetnutzung am Arbeitsplatz auszugehen. Dabei ist jedoch zu beachten, dass eine Genehmigung auch konkludent aufgrund betrieblicher Übung entstehen kann, wenn der Arbeitgeber in Kenntnis der privaten Nutzung diese über einen längeren Zeitraum duldet

4. Überwachung der Beschäftigten durch den Arbeitgeber

Auswirkungen hat die erlaubte private Nutzung betrieblicher Mittel wie bereits ausgeführt auch auf eine Überwachung durch den Arbeitgeber. Hierzu hat das BAG bereits klargestellt, dass eine Kündigung nicht auf eine exzessive private Nutzung betrieblicher Mittel gestützt werden kann, wenn der Arbeitgeber dies aufgrund eines Keyloggers herausgefunden hat (Urteil vom 27.07.2017, Az.2 AZR 681/16).

Ein Keylogger ist eine Software, die die Tastatureingaben des Benutzers auf einem Rechner protokolliert. Keylogger und andere Maßnahmen zur Auswertung des Internetverhaltens sind nur dann unter engen Voraussetzungen erlaubt, wenn konkrete Tatsachen den Verdacht einer Straftat oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers begründen. Dazu reichen bloße Vermutungen nicht aus. Insbesondere kann die Nutzung entsprechender Software nur dann zulässig sein, wenn weniger einschneidende Mittel ergebnislos ausgeschöpft wurden und die Maßnahme insgesamt nicht unverhältnismäßig ist. Dabei ist eine Einzelfallbetrachtung anzustellen. Europäische Datenschutzbehörden sind derzeit der Meinung, dass Überwachungssoftware wie Keylogger sogar im Regelfall als unzulässig zu beurteilen sind.

Eine rechtswidrige Überwachung der Beschäftigten kann für die Arbeitgeber weitreichende Folgen haben. Dazu gehören zum einen Unterlassungs- und Schadenersatzansprüche des Beschäftigten gegen den Arbeitgeber aufgrund der Verstöße gegen das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung. Darüber hinaus handelt es sich bei einem solchen Vorgehen um einen Datenschutzverstoß, der nach Art. 83 DSGVO ebenfalls bußgeldbewehrt ist.

Carsten Ullrich
Rechtsanwalt | Fachanwalt für Arbeitsrecht

Telefon +49 (0)351 424 73 9-11
Telefax +49 (0)351 424 73 9-60

E-Mail ullrich@ullrich-rechtsanwaelte.de
Internet www.ullrich-rechtsanwaelte.de