Michael Wilmsen
Rechtsanwalt
U N T E R N E H M E R K A N Z L E I
RECHT & STEUERN

Erich-Zeigner-Allee 69-73 . 04229 Leipzig
Tel. 0341 / 4774728 . Fax 0341 / 4772547 . E-Mail: kanzlei@ra-wilmsen.net

Beschäftigtendatenschutz
- Teil 3 -

Am 25.05.2018 wird erstmals in Europa ein einheitlicher Datenschutz eingeführt. Dann startete die EU-Datenschutz-Grundverordnung (DS-GVO). Deren Vorgaben zum Beschäftigtendatenschutz hat Deutschland im neuen § 26 BDSG konkretisiert:

V. Spezialthemen

1. Datenschutz bei der Meldung der Arbeitsunfähigkeit

Zu den besonderen Kategorien personenbezogener Daten, die einen höheren Schutz verdienen, gehören die Gesundheitsdaten. Die Verarbeitung solcher Daten unterliegt daher besonderen Regeln. In diesem Zusammenhang stellt sich die Frage nach der korrekten Übermittlung einer Arbeitsunfähigkeitsbescheinigung.

Heutzutage werden Krankmeldungen auch per Telefon, Email oder Whats App übermittelt. AU-Bescheinigungen werden oftmals eingescannt und dann an den Vorgesetzten, irgendeine Person der Personalabteilung oder an die zentrale Adresse info@unternehmen.de gemailt. Dies steht konträr zu den datenschutzrechtlichen Bestimmungen.

Tipp: Der Arbeitgeber sollte seinen Arbeitnehmern schriftlich mitteilen, dass eine Krankmeldung nur postalisch oder mittels verschlüsselter Mail erfolgen darf. Zudem sollten nur die Personen die Krankmeldung als erste Ansprechpartner erhalten, die mit der Personalsachbearbeitung betraut sind. Der Arbeitgeber sollte hier für einen geregelten und strukturierten Prozess sorgen, der sich auch in der Dokumentation des Verfahrens wiederfindet.

2. Datenschutz bei Video- und Audioüberwachung

Die Videoüberwachung am Arbeitsplatz stellt naturgemäß einen erheblichen Eingriff in das Persönlichkeitsrecht der Beschäftigten als Betroffene da und ist datenschutzrechtlich ein Problem.

Videoüberwachung öffentlich zugänglicher Räume ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen.

Der Arbeitgeber muss bei einer offenen Videoüberwachung also genau abwägen. Dieses dürfte voraussetzen,

- dass berechtigte Interessen des Unternehmens an einer Überwachung vorliegen,
- die Videoüberwachung sowohl geeignet als auch erforderlich zur Wahrnehmung der berechtigten Interessen ist und
- keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen das Interesse an der Videoüberwachung überwiegen.

Zudem sind die Grundsätze der Datenminimierung und Speicherbegrenzung zu beachten. Die Maßnahme ist ebenfalls zu dokumentieren. Wichtig: Bei einer offenen Überwachung am Arbeitsplatz, der öffentlich zugänglich ist, darf regelmäßig weder die Intim- noch die Privatsphäre des Arbeitnehmers betroffen sein, sondern lediglich die weniger schutzwerte Sozialsphäre. Strafbar sind daher z.B. Aufzeichnungen von Toiletten oder Duschen sowie Umkleideräume.

Da die Videoüberwachung als erheblicher Eingriff in das Persönlichkeitsrecht gilt, unterliegen Videoüberwachungen hier der sogenannten Datenschutz-Folgeabschätzung nach DS-GVO (dazu demnächst gesondert).

Eine heimliche Videoüberwachung eines Arbeitnehmers kann zulässig sein zur Aufdeckung von Straftaten, wenn zu dokumentierende tatsächliche Anhaltspunkte für den Verdacht einer Straftat des Arbeitnehmers vorliegen.

Zudem muss die Videoüberwachung geeignet und auch erforderlich sein, um die Straftat aufzudecken. Zuletzt darf das schutzwürdige Interesse des Beschäftigten am Ausschluss der Erhebung, Verarbeitung oder Nutzung der Videoüberwachung nicht überwiegen. Art und Ausmaß der Nutzung der gewonnenen Daten müssen also im Hinblick auf den Anlass verhältnismäßig sein.

Auf eine vorgesehene Videoaufzeichnung ist hinzuweisen (zum Beispiel mittels eines Piktogramms). Diese muss auch den Hinweis enthalten, wer dafür verantwortlich ist, damit der Betroffene einen Ansprechpartner hat. Das Transparenzgebot aus Art. 5 DS-GVO ist dabei stets zu beachten.

Die Videoüberwachung muss umfassend dokumentiert werden: welche Anhaltspunkte begründen den Anfangsverdacht; weshalb wurde die Videoüberwachung notwendig; weshalb ist sie verhältnismäßig; gab es mildere Mittel; wenn ja, weshalb wurden diese nicht als ausreichend erachtet; weswegen muss es eine verdeckte Aufzeichnung sein. In dem nach

Art. 30 Abs.1 DS-GVO zu erstellenden Verarbeitungsverzeichnis soll die Videoüberwachung ausgewiesen und dokumentiert werden, welchem Zweck die Verarbeitung jeweils dient.

Die Daten der Videoüberwachung sind unverzüglich zu löschen, wenn sie zur Zweckerreichung nicht mehr notwendig sind.
Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können.

Für Audioaufzeichnungen gilt das gleiche wie für Videoaufzeichnungen.
Sollen Telefonate aufgezeichnet werden, müssen der Arbeitnehmer und der Angerufene auf die geplante Aufzeichnung hingewiesen werden, die einzelnen Bedingungen und der Zweck sollten hierbei erläutert werden. Der Hinweis auf die Aufzeichnung sollte dabei stets aktiv erfolgen. Das heimliche Mitschneiden von Telefongesprächen ist unzulässig. Entfällt der Zweck der Aufnahme, ist diese zeitnah zu löschen.

3. Datenschutz bei (privater) Email-Nutzung im Unternehmen

Grundsätzlich hat der Arbeitnehmer keinen Anspruch auf die private Nutzung der Betriebs-IT. Bei Nichtregelung ist der private Gebrauch verboten. Ein Anspruch kann sich aber ergeben, wenn der Arbeitnehmer mindestens sechs Monate mit stillschweigender Duldung des Arbeitgebers die Betriebs-IT auch zu privaten Zwecken nutzt.

Die Konsequenz daraus ist, dass der Arbeitgeber grundsätzlich weder vom Inhalt noch von den näheren Umständen (insbesondere Verkehrsdaten) der Telekommunikation Kenntnis nehmen darf.

Bei Ausschluss der Privatnutzung ist gleichwohl der allgemeine Datenschutz zu beachten.

Es hat – wenn keine Einwilligung vorliegt – eine Interessenabwägung zu erfolgen.

So sind die Interessen des Arbeitgebers gegen die Interessen des betroffenen Beschäftigten abzuwägen, wenn es darum geht, ob der Zugriff wegen unerwarteter Krankheit bzw. zur Archivierung von Emails zulässig ist.

Tipp: Der Arbeitgeber sollte die Privatnutzung von Internet, Email-Programmen und Telefonen ausdrücklich verbieten oder höchstens die Nutzung eines vom Dienstprogramm losgelösten Email-Accounts (wie google.com, web.de usw.) erlauben, um sich eine sinnvolle Kontrollmöglichkeit zu bewahren.

Keinesfalls genügt es aber pro forma die Privatnutzung zu verbieten und dann bewusst die Augen vor der Realität zu verschließen.
Das würde jedenfalls mit der Zeit zu einer geduldeten Privatnutzung führen, die wie eine gestattete Privatnutzung wirkt.