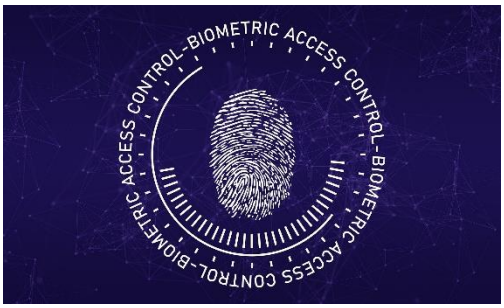

Zeiterfassung mittels Fingerprint - unzulässig ohne Einwilligung

Zeiterfassungssysteme sind in Betrieben mittlerweile üblich. Fast ausschließlich werden dafür automationsunterstützte Systeme verwendet, um einerseits den arbeitszeitrechtlichen Vorschriften nachzukommen und anderseits die Abrechnungsbasis für die geleistete Arbeitszeit zu schaffen.

Wie ist das aber mit **Zeiterfassungssystemen**, die biometrische Merkmale, zB **Fingerprint** nutzen?

Eine aktuelle Entscheidung des ArbG Berlin

In einer aktuellen Entscheidung des ArbG Berlin (16.10.2019, 29 Ca 5451/19) findet sich explizit folgende Aussage:

> *„Erfolgte die Zeiterfassung früher üblicherweise analog mittels Stechuhr, ist heute eine digitale Zeiterfassung, zum Beispiel über softwarebasierte oder webbasierte Zeiterfassungssysteme, teilweise auch per Smartphone oder Tablet, die Regel. Relativ neu ist die digitale Zeiterfassung mittels Fingerprint. Diese Form der Arbeitszeiterfassung soll unter anderem verhindern, dass Mitarbeiter für Kollegen „mitstempeln“ und hierdurch Arbeitszeitbetrug begehen.“*

Um ein derartiges System verwenden zu können, ist es notwendig, von den Mitarbeiter_Innen Referenzdaten mittels Fingerabdruck zu erheben; dazu ist nicht der gesamte Fingerabdruck notwendig, sondern sog. Minutien (individuelle, nicht vererbbare Fingerlinienverzweigungen). Der Minutiendatensatz wird sodann im Zeiterfassungsterminal gespeichert und zum Abgleich des Fingerabdrucks des

Mitarbeiters bei der An- und Abmeldung verwendet. Es ist nicht möglich, aus diesen Daten den Fingerabdruck der betroffenen Person wiederherzustellen.

Biometrische Daten iSd Art 9 DSGVO?

Nach Ansicht des Arbeitsgerichts Berlin handelt es sich bei den erhobenen (Referenz)-Daten um **biometrische Daten** nach Art 9 Abs. 1 DSGVO, die auch unter dem „besonderen Schutz“ des § 26 Abs. 3 BDSG (in D) stehen.

Die Verarbeitung dieser Daten, als Daten einer besonderen Kategorie des Art 9 DSGVO darf nur unter den sehr engen Voraussetzungen des Art 9 Abs 2 DSGVO erfolgen. Die Erhebung dieser Daten greift in das Recht auf informationelle Selbstbestimmung der Mitarbeiter*Innen in besonderer Art und Weise ein, und die Verarbeitung dieser besonderen Datenkategorien ist grundsätzlich verboten (siehe Art 9 Abs 1 DSGVO), sofern nicht eine der besonderen Voraussetzungen des Art 9 Abs 2 DSGVO („Erlaubnistatbestände“) erfüllt ist, die auch restriktiv auszulegen sind, da sie eine Ausnahme von einem Verarbeitungsverbot darstellen.

Das ArbG Berlin verwies darauf, dass folgende **Erlaubnistatsbestände** in Frage kommen:

- **ausdrückliche Einwilligung** (iSd Art 9 Abs 2 lit a DSGVO), wobei im Sinne der notwendigen Freiwilligkeit dann die Mitarbeiter*Innen auch eine Alternative zum Verarbeitungszweck haben müssen, um die Freiwilligkeit sicher zu stellen.
- **arbeits- und sozialrechtliche Notwendigkeit** (Art 9 Abs 2 lit b DSGVO), wobei diesbezüglich in D auch eine Spezialnorm (§ 26 Abs 1 BDSG) gegeben ist, die es in Ö nicht gibt, sodass sich in Ö die Rechtslage nach Art 9 Abs 2 lit b DSGVO richtet.

Prüfmaßstab für die Erforderlichkeit iZhg mit den arbeitsrechtlichen oder sozialrechtlichen gesetzlichen Regelungen.

Biometrische Merkmale darf ein Arbeitgeber nur dann verarbeiten, wenn dies für die **Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich** ist.

Zweck

Die Verarbeitung der Daten muss sich dafür eignen, zum Zweck der „Abwicklung des Beschäftigungsverhältnis“ zu erfolgen

Gelinderes Mittel

Es darf **kein anderes, gleich wirksames, das Persönlichkeitsrecht weniger beeinträchtigendes Mittel** existieren.

Interessensabwägung

Der **Zweck der Verarbeitung** (Zeiterfassung) muss mit **der Beeinträchtigung des Persönlichkeitsrechts** (Erhebung und Verwendung von biometrischen Daten) **in einem angemessenen Verhältnis stehen**. *„Je intensiver in das Persönlichkeitsrecht eingegriffen werden soll, desto schwerer muss der vom Arbeitgeber mit dem Verfahren verfolgte konkrete Zweck überwiegen. So wird das Interesse des Arbeitgebers an einer biometrischen Zugangskontrolle zu Bereichen mit sensiblen Geschäfts-, Produktions- und Entwicklungsgeheimissen eher überwiegen als bei einer angestrebten Zugangs-sicherung zu normalen Bürobereichen. So können biometrische Daten zwar zur Kontrolle beim Eintritt in Sicherheitsbereiche, nicht jedoch im Rahmen der Arbeitszeiterfassung verwendet werden (Gola / Heckmann, 13. Auflage 2019, Rn.-Nr. 157 zu § 26 BDSG).“*

Das ArbG Berlin führt dazu aus, dass es **vereinzelt vorgekommen** sei, dass es zum „**Mitstempeln**“ durch Kollegen gekommen sei, dies aber **nicht rechtfertigt, dass derart in die Persönlichkeitsrechte der Mitarbeiter*Innen eingegriffen wird**. Es verhielten sich die Mehrheit der Arbeitnehmer rechtstreu, sodass für diese Art der Kontrolle der Mitarbeiter*Innen kein Anlass bestehe,“ es sei denn, dass konkrete Umstände im Einzelfall (Nachweise über Missbräuche in nicht unerheblichem Umfang) die Erforderlichkeit einer solchen Maßnahme begründen können“.

Österreich:

Der OGH kam bereits im Jahr 2006 (20.12.2006, 9ObA109/06d) zu einem ähnlichen Ergebnis. In einem Bezirkskrankenhaus wurden Fingerscanner installiert, um durch die Datenerhebung die Arbeits- bzw. Anwesenheitszeiten der Beschäftigten zu erfassen. Eine Zustimmung des Betriebsrates mittels Betriebsvereinbarung lag nicht

vor, und es kam zu einer Unterlassungsklage des Betriebsrates gegen den Betriebsinhaber.

Auch dort führte der OGH aus, dass die gespeicherten Templates als personenbezogene Daten zu qualifizieren sind:

> *Bei biometrischen Daten handelt es sich nach einhelliger Auffassung um personenbezogene Daten sowohl iSd Art 2 lit a Datenschutz-Richtlinie 95/46/EG als auch iSd § 4 Z 1 DSG 2000. [...] Biometrische Verfahren speichern in der Regel nicht die biometrischen Rohdaten für spätere Identifikationsprozesse, sondern verwenden - wie auch im vorliegenden Fall - sog „Templates" (Datensätze). Diese enthalten in komprimierter Form die wesentlichsten Informationen des biometrischen Merkmals und reichen in der Regel aus, um in der Folge über Ähnlichkeitsvergleiche Personen reidentifizieren zu können (s Näheres Parziale/Riener-Hofer, juridikum 2004, 79 ua). Im Normalfall lässt sich aus dem Template das biometrische Merkmal nicht rekonstruieren.* ***Trotz der Einwegfunktion des Templates handelt es sich aber um ein personenbezogenes Datum, da die Identität des Betroffenen bestimmt oder bestimmbar ist.***
>
> *Bei der Preisgabe physischer (und psychischer) Charakteristika der Arbeitnehmer ist grundsätzlich größte Zurückhaltung geboten.*
>
> *Es kann aber nicht allgemein gesagt werden, dass schon allein der Einsatz biometrischer Daten genügt, um aus jeglichem Kontrollsystem, das auf solchen Daten aufbaut, ein wegen Berührens der Menschenwürde mitbestimmungspflichtiges System werden zu lassen; dies insbesondere dann nicht, wenn die Verfügungsgewalt über den Einsatz der biometrischen Daten ausschließlich beim betroffenen Arbeitnehmer liegt, der Arbeitgeber keinen unmittelbaren Personenbezug herstellen kann (zB bei einem Zutrittskontrollsystem, das nur zwischen „berechtigt" und „unberechtigt" unterscheidet, ohne den Zugang mit einer bestimmten Person zu verknüpfen), keine Relation mit anderen Daten hergestellt wird und keine Aufzeichnungen der Zutritte vorgenommen werden (Löschnigg, ASoK 2005, 37 [39 f, 42]; Preiss aaO § 96 Erl 7 [S 139] ua).*

Der OGH führte weiters aus:

> *Es ist* ***selbstverständlich legitim****, dass der* ***Arbeitgeber die Arbeitszeiten seiner Arbeitnehmer kontrolliert und erfasst****.*

*Die **Interessenwahrungspflicht** der **Arbeitnehmer** gebietet sogar, den Arbeitgeber dabei zu unterstützen (zB durch Aufzeichnungen; Bedienung einer Stechuhr; Verwendung von Magnetkarten).*

*Wie bereits ausgeführt, verlangt aber die **Fürsorgepflicht vom Arbeitgeber, das für die Arbeitnehmer schonendste - noch zum Ziel führende - Kontrollmittel** zu wählen.*

Fazit:

- Die **Verwendung von biometrischen Systemen** im Arbeitsverhältnis berührt die Menschenwürde und bedarf **zwingend einer Betriebsvereinbarung**. (OGH)

- Nach Ansicht des ArbG Berlin sind derartige **Datenverarbeitungen ohne** die freiwillige, jederzeit widerrufliche, informierte **Einwilligung** der Beschäftigten **nicht bzw. nur in besonderen Situationen zulässig** ist, da der Eingriff in die Privatsphäre unverhältnismäßig ist.

- Die **Verwendung derartiger biometrischer Systeme für Zutrittskontrollen**, zB für Geschäfts-, Produktions- oder Entwicklungsbereiche mit Vertraulichkeitscharakter wird jedoch **zulässig** sein, da das erhöhte Sicherheits- bzw. Vertraulichkeitserfordernis den Eingriff in das Persönlichkeitsrecht rechtfertigen kann.