Daten in der Arbeitswelt

Mag. Martin Soucek

Ein Mensch – verschiedene Rollen

Der Sportverein ist ein gänzlich anderes Setting, als der Arbeitsplatz.

Die Rollentrennung ist auch ein Schutz den wir selbstbestimmt gestalten, um Kontrolle über mögliche negative Auswirkungen unserer Freizeitaktivitäten auf unser Berufsleben zu unterbinden.

Der Schutz des Privat- und Familienlebens ist in Artikel 8 EMRK geschützt. Die EMRK steht in Österreich im Verfassungsrang.

DAS DATEN-ICH

Die informationelle Privatsphäre --- „Selbstbestimmung“

Das deutsche Bundesverfassungsgericht erkennt bereits in den 1980er-Jahren im Rahmen des sogenannten Volkszählungsurteils: „In Zeiten der digitalen Datenverarbeitung gibt es kein belangloses Datum mehr.“

Wir müssen mit negativen Konsequenzen rechnen, wenn in den falschen Kreisen bekannt wird, dass wir gegen den Strom schwimmen oder eine unliebsame Meinung vertreten.

Die informationelle „Selbstbestimmung“

Haben Menschen den Eindruck, dass sie überwacht werden, dann passen sie Ihr Verhalten an das Verhalten an, von dem sie glauben, dass es von den Überwachenden gewünscht wird.

Dieser vorauseilende Gehorsam ist eine natürliche Reaktion des Menschen, die dem Selbstschutz dient.

Wir hängen in vielen Bereichen unseres Lebens von anderen Menschen ab.

Dienstverhältnis

Das Beschäftigungsverhältnis ist dabei von einer besonderen Abhängigkeit geprägt– finanziell, rechtlich und technisch.

Beispielsweise entscheidet unser/unsere Vorgesetzter/Vorgesetzte darüber, ob wir unsere Arbeit behalten können und auch im nächsten Monat noch ein Gehalt bekommen.

Arbeitnehmer

Das wirtschaftliche Interesse am Einsatz bestimmter Technologien und an der Effizienzsteigerung durch die Verarbeitung diverser (und vor allem immer mehr) Daten steht im permanenten Spannungsfeld zur Überwachung der ArbeitnehmerInnen und dem Schutz ihrer Persönlichkeitsrechte.

> ***Für die Digitalisierung sind Daten wie der Sand für den Strand!***
>
> ***(Digital human: Der Mensch im Mittelpunkt der Digitalisierung, Kai Anderson und Bettina Volkens, 2017)***

Bei der Deutschen Telekom heißt es (zur DSGVO): *„Es geht um das Vertrauen der Menschen in die Digitalisierung. Dafür braucht es hohe Standards, die für alle Unternehmen gelten, die ihre Dienste hier anbieten.“*
(TT 17.05.2018)

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) zielt nun darauf ab, das Grundrecht auf Datenschutz in der Europäischen Union zu stärken und das in den letzten Jahrzehnten entstandene Ungleichgewicht zwischen datenverarbeitenden Stellen und Betroffenen wieder ins Lot zu bringen.

Der Datenschutz und die Privatsphäre, sind notwendige Voraussetzungen für eine funktionierende Demokratie und ein selbstbestimmtes Leben.

DSGVO

Artikel 1 Abs 2 DSGVO

„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“

DSGVO

Im Englischen tut man sich ein wenig leichter, sind doch „safety“ (Maschinen-/Produkt-Sicherheit: Geht von der Maschine ein Risiko für den Menschen/die Umwelt aus?)

und „security“ (Daten-/IT-Sicherheit: Kann der Mensch bei der Maschine Schaden anrichten?)

von „privacy“ (Privatsphäre) relativ leicht zu unterscheiden.

Das Schutzobjekt sind also nicht die Informationen, die verarbeitet werden, sondern die Interessen der Personen, über die Informationen verarbeitet werden.

DSGVO- DSG

Hat man diesen zentralen Unterschied einmal verinnerlicht, fällt das Verständnis für die Materie allgemein um einiges leichter.

Aus der Sicht des Menschen (Arbeitnehmerin) ist ein für alle allzeit einsichtiges Panoptikum ist nicht wünschenswert.

Auch für die Gesellschaft insgesamt erscheint dies problematisch.

Das DSG 2000 (Ö) kennt/kannte auch den Schutz der personenbezogenen Daten der juristischen Person – dies war nicht haltbar im europäischen Kontext.

Personenbezogene Daten

Die Datenschutz-Grundverordnung (DS-GVO) definiert personenbezogene Daten in ihrem Artikel 4 Z 1 wie folgt:

Dies sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Personenbezogene Daten

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Die Systeme, die Daten über Arbeitnehmer „produzieren“ sind sehr vielfältig geworden.

Keine abschließende Aufzählung

- Lohn- und Gehaltsverrechnung
- Elektronische Zeiterfassungssysteme die Daten zu Ankommen und Gehen verwalten
- zentrale globale HR/HCM-Systeme
- e-learning
- Recruiting, Onboarding
- MitarbeiterInnen-Gespräche (360 Grad-Feedback)
- Self Service Portale (elektronischer Lohnzettel)
- Manager-Self-Service (auf Daten ihnen zugewiesener Beschäftigter zugreifen und gewünschte Analysen selbst durchführen)
- Online-Befragung (Zufriedenheit der Beschäftigten)
- Kollaborationssysteme (WhatsApp, Workplace by Facebook, Skype for Business, Microsoft Teams, SAP Jam)
- Vernetzte Kopier- und Druckstationen (Multifunktionsgeräte, die nach dem FollowMe-Prinzip arbeiten)
- „Internet der Dinge“, Big Data, (Personenbezogene Daten, von Beschäftigten und von Kundinnen fließen in großer Anzahl in diese Systeme)
- Zutrittssysteme, Schleusen („Vereinzelungsanlagen“)
- Videosysteme, Ticketsysteme (speichern alle Arbeitsschritte und Dokumentationen)
- „Enterprise-Resource-Planning“ (hier wird Personal- mit Finanzwirtschaft und Logistik verknüpft)

  Jeder User in einem solchen System hinterlässt „Bewegungsdaten“
- Arbeiten in der Cloud (MyAnalytics wertet aus, wie viel Zeit für welche Aufgabe verwendet wurde)

Verknüpfungen

Durch die Nutzung technischer Netze und Software-unterstützter Systeme zur Kommunikation werden immer mehr Daten der beteiligten Personen erfasst und können analysiert werden.

Neben den Metadaten (wer telefoniert wann mit wem) liefern Standortdaten (GPS, Funkzellenkoordinaten) und Inhaltsdaten zusätzliche Informationen über die Beteiligten einer Kommunikation. Die Zusammenführung dieser Informationen ermöglicht eine genaue Darstellung von Kontakten und Kommunikationsverhalten.

Der Großteil der Kommunikation findet im betrieblichen Umfeld über elektronische Post (E-Mail) statt, dies hat in den letzten Jahrzehnten zu umfassenden Veränderungen in den persönlichen und betrieblichen Arbeitsweisen geführt.
E-Mail ist zum bedeutendsten Kommunikationsmedium geworden, aber auch zu einer Gefahr für Betriebe (Viren, Spam).

„Persönliche“ E-Mail

Schon im Bereich der E-Mail-Kommunikation wird eine Vielzahl an personenbezogenen Daten verarbeitet. Insbesondere in denjenigen Fällen, in denen namensbezogene E-Mail-Adressen (Name@musterbetrieb.at) und keine funktionalen E-Mail-Adressen (office@musterbetrieb.at) verwendet werden, kann durch Software einfach dargestellt werden, mit welchen Personen und Gruppen wie intensiv Informationen ausgetauscht werden bzw. könnten betriebliche Regelungen (zB Verbot der privaten Kommunikation, Umsicht beim Öffnen von Anhängen aufgrund von Malware-Schadsoftware-Gefahr) zu Kontrollen des Kommunikationsverhaltens führen.

„Datenkrake Auto“

Die Daten können personenbezogen analysiert werden (ressourcenschonendes Fahrverhalten, Beanspruchung der Bremsen…)

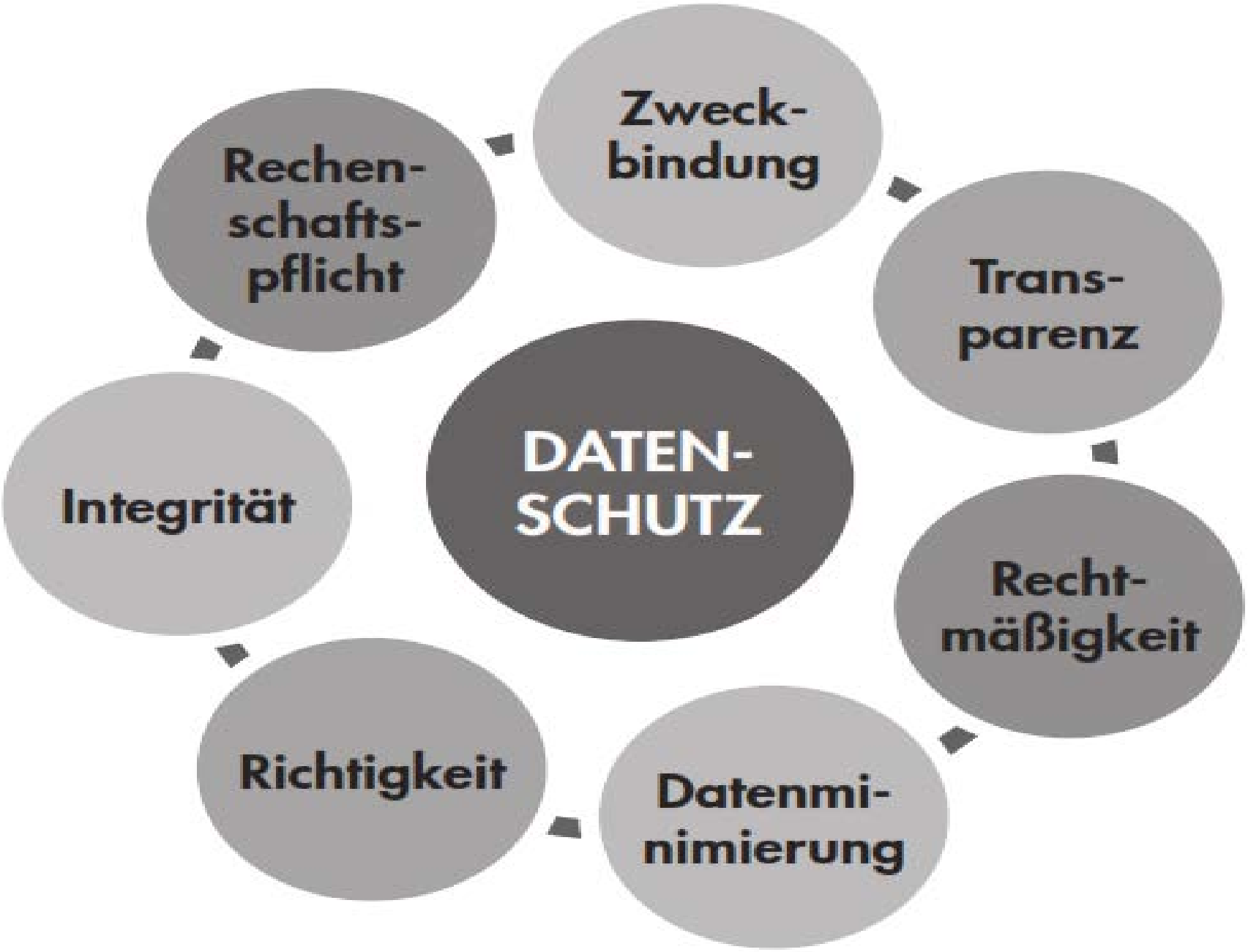
Die Datenermittlung auf das notwendige Ausmaß zu beschränken, hieße zB ein GPS-Fahrtenbuch benötigt lediglich die Übermittlung der Start- und Zielkoordinaten und keine permanente Aufzeichnung oder Übermittlung der Standortdaten.

Die DSGVO enthält wichtige Fortschritte

Die Grundprinzipien heißen Zweckbindung, Transparenz, Selbstbestimmung über die eigenen Daten.

Der Artikel 88 Datenverarbeitung im Beschäftigungskontext stellt eine typische Kompromissregel dar.

Bei sehr unterschiedlichen Sichtweisen der Mitgliedsstaaten war keine europaweite Vollharmonisierung durchsetzbar.


DATEN-
SCHUTZ
Zweck-
bindung
Trans-
parenz
Recht-
mäßigkeit
Datenmi-
nimierung
Richtigkeit
Integrität
Rechen-
schafts-
pflicht

Zweckbindung

Für das Arbeitsverhältnis wohl wichtigstes Grundprinzip ist die Zweckbindung.

Jede Datenverwendung muss einen rechtmäßigen Zweck verfolgen.

Verlangt das ein Gesetz?

Sind die personenbezogenen Daten für die Erfüllung eines Vertrags notwendig?

Die Frage Wozu? muss beantwortet werden.
Der Zweck muss festgelegt, eindeutig und rechtmäßig sein

Datenminimierung

Personenbezogene Daten sollen so sparsam wie möglich verwendet werden, um das Grundrecht auf Datenschutz zu gewährleisten.

Datenminimierung hängt eng mit jenem der Zweckbindung sowie der Rechtmäßigkeit zusammen.

Nur so viele Daten verarbeitet werden, als für den Zweck und dessen Umsetzung (unbedingt) notwendig sind.

Das geringste erforderliche Ausmaß und stets mit den gelindesten Mitteln.

Datenschutz durch Technik

„privacy by design“
größtmögliche Datensicherheit und größtmöglicher Schutz der Privatsphäre

„privacy by default“
datenschutzfreundliche Voreinstellungen

technische und organisatorische Maßnahmen
wenn das Fahrzeug privat genutzt wird, werden keine GPS-Daten gespeichert

Voreinstellung in Produkten, um Zweckbindung und Datensparsamkeit zu gewährleisten

GPS Daten, die zur Routenerstellung und Navigation verwendet werden, werden nicht übermittelt - lediglich die zur Führung des Fahrtenbuchs erforderlichen Start-Ziel-Koordinaten

Konzepte zum Löschen

Zugriffseinstellungen

Zertifizierungsverfahren als Nachweis möglich

Speicherbegrenzung

Um festzustellen, wie lange Daten gespeichert werden dürfen, ist es erforderlich, den Zweck der Datenverwendung zu kennen.

Falls es rechtliche Vorgaben der Datenspeicherung gibt, ist das der Zweck.

(Ö) Finanzamt: Steuerprüfung - sieben Jahre;
(Ö) Krankengeschichten: 10 Jahre vgl. (Ö) Ärztegesetz;
Gewährleistungsfristen etc.

Richtigkeit und Transparenz

Die verwendeten personenbezogenen Daten müssen richtig und aktuell sein.

Auch die Richtigkeit und Aktualität hängt davon ab, für welchen Zweck die Daten verwendet werden.

(z.B. historisches Dokument – wird nicht aktuelle personenbezogene Daten umfassen)

Ein Grundsatz lautet:
Die betroffenen Personen können immer nachvollziehen warum etwas mit ihren personenbezogenen Daten geschieht.

Rechenschaftspflicht

Der Verantwortliche muss nachweisen, dass bei Datenverwendungen die Grundsätze eingehalten wurden.

Der/Die Verantwortliche muss die Einhaltung der Grundsätze der Datenverarbeitung nachweisen können
(Art 5 Abs 2 DSGVO).

Zur Erfüllung der Rechenschaftspflicht wird eine schriftliche Dokumentation der Verarbeitungsvorgänge und ihrer genauen Rahmenbedingungen erforderlich sein.

Rechtmäßigkeit

die Einwilligung einer betroffenen Person

die Erfüllung eines Vertrages

eine rechtliche Verpflichtung

(Aufzeichnung der Arbeitszeit gemäß Arbeitszeitgesetz)

lebenswichtige Interessen erfordern die Datenverarbeitung

öffentliches Interesse erfordert die Datenverwendung

Auch die Verarbeitung zur Wahrung berechtigter Interessen der Verantwortlichen oder eines Dritten

Der Verantwortliche wird erklären müssen, worin seine berechtigten Interessen bestehen, um die Datenverarbeitung durchzuführen, und diese müssen dann mit den Interessen der Beschäftigten abgewogen werden.

Art. 88 DSGVO

Die nach Art. 88 DSGVO thematisch begrenzte Möglichkeit der Mitgliedsstaaten zur näheren Ausgestaltung des Beschäftigtendatenschutzes ist im Kontext mit dem Erwägungsgrund Nr. 155 zu sehen, wonach „insbesondere für Vorschriften über Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen“.

Da Beschäftigungsverhältnisse ein Abhängigkeitselement enthalten, dürfen insbesondere die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung verarbeitet werden dürfen, näher geregelt werden.

Die DSGVO beschneidet die nationalen betrieblichen und kollektiven Vereinbarungen nicht. Kollektivverträge und Betriebsvereinbarungen sind dezidiert dazu geeignet, den betrieblichen Datenschutz zu regeln. (Erwägungsgrund 155)

Verdünnter Wille

Einwilligungen im Zusammenhang mit dem Arbeitsverhältnis werden mit dem Begriff des „verdünnten Willens“ umschrieben. (Recht am eigenen Bild – Veröffentlichung im Rahmen des Arbeitsverhältnisses)

Einwilligung (Artikel 7 DSGVO)

Einwilligung muss freiwillig, spezifisch informiert, eindeutig und eine unmissverständliche Willensbekundung sein (Nachweis obliegt dem Verantwortlichen/Arbeitgeber)

Regelungen der Staaten

Die Regelungen der Staaten dürfen sich nur in den „limits of this regulation“, also innerhalb der DSGVO bewegen.

In Österreich besteht kein eigentliches Beschäftigtendatenschutzrecht, dies gilt auch für die Zukunft.

Dies wurde und wird? durch Verweise auf gesetzliche Bestimmungen insbesondere auf das Arbeitsverfassungsgesetz (DSG 1978 und DSG 2000) und das Arbeitsvertragsrechtsanpassungsgesetz (AVRAG) erreicht.

Die Gestaltungsmöglichkeiten der betrieblichen Sozialpartner in Österreich beruhen sehr stark auf Betriebsvereinbarungen im Datenschutzrecht.

Österreich

Die Öffnungsklausel des Art 88 DSGVO wurde im §11 DSG 2018, in der Fassung vor dem DatenschutzderegulierungsG 2018

Die „ursprüngliche“ Fassung vor dem DatenschutzderegulierungsG

„Das Arbeitsverfassungsgesetz– ArbVG, BGBl. Nr. 22/1974, ist, soweit es die Verarbeitung personenbezogener Daten regelt, eine Vorschrift im Sinne des Art. 88 DSGVO. Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt.”

Der Antrag auf Abänderung dieser Bestimmung lautet dann:

„§ 11. Die Befugnisse der Arbeitnehmerschaft nach dem 3. Hauptstück des Arbeitsverfassungsgesetzes - ArbVG, BGBI. Nr. 22/1974, insbesondere nach dessen §§ 89, 91, 96, 96a und 97, sowie die Mitwirkungsrechte in Bezug auf die Personalvertretung bleiben, soweit sie die Verarbeitung personenbezogener Daten betreffen, unberührt."

In der beschlossenen Fassung entfällt §11 eigentlich?, da er durch:

„§ 11 Verwarnung durch die Datenschutzbehörde …“ ersetzt wurde?

Relevante Judikatur (DSG 2000, ArbVG)

Einsichtsrechte des Betriebsrates in personenbezogene Beschäftigtendaten

Im gegenständlichen Fall begehrte der Betriebsrat Einsicht in die Gehalts- und Lohnabrechnungen aller MitarbeiterInnen. Da sich mehrere MitarbeiterInnen sowohl mündlich als auch schriftlich gegenüber der Geschäftsführung gegen die Übermittlung derartiger Unterlagen an den Betriebsrat aussprachen und um Geheimhaltung ihrer Daten ersuchten, gewährte der Arbeitgeber dem Betriebsrat keine Einsicht.

OGH: Das DSG 2000 (bzw. das DSG 2018, vgl. dessen § 11) steht den Befugnissen des Betriebsrates nicht entgegen.

Einsichtsrechte des Betriebsrates

Der OGH hat, der einhelligen Auffassung in der Lehre folgend, klar entschieden, dass dieses Einsichts- und Kontrollrecht nicht von der Zustimmung der einzelnen ArbeitnehmerInnen abhängig ist und weiters, gerade weil diesbezüglich eine ausdrückliche gesetzliche Ermächtigung oder sogar Verpflichtung („Pflichtbefugnis") des Betriebsrates besteht, auch nicht unter Hinweis auf den Datenschutz verweigert werden kann.
Es erfolgte der Hinweis, dass der Betriebsrat und dessen Mitglieder einer strengen Verschwiegenheitspflicht – mit der auch der Datenschutz gewahrt ist – unterliegen, somit eine Weitergabe oder Veröffentlichung von Daten einzelner ArbeitnehmerInnen unzulässig ist.

Fingerscanner

Der Einsatz von sog „Fingerscannern“ zur Erfassung der Kommens- und Gehens Zeiten ist zustimmungspflichtig (OGH 20.12.2006, 9 ObA 109/06d)

Es ist das gelindeste, zum Ziel führende Mittel zu wählen, andernfalls wird die Menschenwürde jedenfalls berührt und es ist von der Zustimmungspflicht des Betriebsrates auszugehen.

Im vorliegenden Fall kamen in einem Bezirkskrankenhaus mit rund 430 ArbeitnehmerInnen sog „Fingerscanner“ zum Einsatz. Diese dienten im Rahmen eines „biometrischen“ Zeiterfassungssystems der Feststellung der „Kommens- und Gehens Zeiten“ der ArbeitnehmerInnen.

Der Betriebsrat verweigerte den Abschluss einer Betriebsvereinbarung dazu, weil er darin einen unzulässigen Eingriff in die Persönlichkeitsrechte der ArbeitnehmerInnen erblickte.

Fingerscanner

Es solle vom der Arbeitgeber eine sonst in Großbetrieben übliche Zeiterfassungsart, zu. mit Magnetkarten, gewählt werden.

Fraglich war, ob durch den Einsatz des technischen Systems die Menschwürde berührt wird.

Mit der Anknüpfung an den Begriff „Menschenwürde“ erreicht der Gesetzgeber, dass die freie Entfaltung der Persönlichkeit des/der Arbeitnehmers/Arbeitnehmerin keinen übermäßigen Eingriffen ausgesetzt ist.

Für „biometrische Daten“ – dabei handelt es sich um Angaben über Personen, deren Identität mittels messbarer körperlicher Merkmale bestimmbar ist - gilt der Bedarf nach einem Schutz der Individualität allerdings in besonderer Weise, weil es zu einer Überschneidung der Abbildung körperlicher Merkmale und personenbezogener Informationen kommt.

Fingerscanner

Es verlangt die Fürsorgepflicht des/der Arbeitgebers/Arbeitgeberin von diesem, das für die ArbeitnehmerInnen schonendste, noch zum Ziel führende, Kontrollmittel zu wählen.

Die biometrische Vermessung der ArbeitnehmerInnen samt dem täglich notwendigen Vergleich mit den vorher gewonnenen biometrischen Vorlagen durch die Bedienung von Fingerscannern erreicht in Relation zum angestrebten, vergleichsweise trivialen Zweck (Erfassung der Kommens- und Gehens Zeiten, dh. Arbeitszeiterfassung) eine Intensität, die zufolge Berührung der Menschenwürde zustimmungspflichtig ist.

Dies bedeutet aber nicht, dass für bestimmte Zwecke der Einsatz biometrischer (Mitarbeiter) Daten gänzlich unzulässig wäre!

Beurteilung des Systems

Für die Beurteilung der Zustimmungspflicht ist die objektive Eignung des Systems maßgeblich.

Für die Frage der „vorgesehenen Verwendung“ ist der Leistungsumfang des konkret eingesetzten Programmpakets entscheidend.

Die Beurteilung hat daher anhand des gesamten installierten Systems zu erfolgen, dessen Grundlagen dem Betriebsrat offenzulegen sind.

Profiling

Die DS-GVO legt großen Wert auf das Verbot von Profiling, also dürfen Entscheidungen, die rein aufgrund von Algorithmen und maschinellen Berechnungen getroffen werden, die Einzelnen nicht unwesentlich in ihrem Leben beeinflussen. Zwar enthielt die derzeitige Gesetzeslage (DSG 2000) bereits einen solchen Passus, doch ist dieser unter „ferner liefen“ einzuordnen.

Es muss Auskunft darüber erteilt werden, ob Profiling erfolgt und wenn ja, welche Logik dahintersteckt und welche Auswirkungen dies vermutlich haben wird.

Judikatur!?

Risikoreiche Datenverarbeitung

Im Beschäftigungskontext kommen neben Bildaufnahmen durch Videoüberwachung und Bewegungsdaten durch GPS-Tracking va. die Verschneidungen größerer Datenmengen, zB. in Datenbanklösungen von SAP (Data-Warehouse, BI, HANA), oder die „systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet“, als risikoreiche Datenanwendungen in Frage, aber auch die umfangreiche Verarbeitung besonderer (bisher „sensibler“) Datenkategorien.

Im Verarbeitungsverzeichnis müssen nun auch Löschfristen angegeben werden.

Zweck-Mittel-Relation

Ist geklärt, dass sowohl der Zweck der geplanten Maßnahme als auch die Maßnahme selbst legitim ist, muss sichergestellt werden, dass sich sowohl die potenzielle Überwachung als auch die Datennutzung nur in jenem Rahmen bewegen, der unbedingt erforderlich ist, und nicht überschießende Maßnahmen zugelassen werden.

Generell sind jene Mittel und Wege zu bevorzugen, die weniger in die Privatsphäre eingreifen (zB. die Videoüberwachung nur an der Eingangstüre und nicht an jeder einzelnen Bürotür); die weniger Beschäftigte betreffen.

Zweck-Mittel-Relation

Eine technische Überprüfung sämtlicher elektronischer Ablagesysteme nur bei jenen Beschäftigten/Arbeitsplätzen, bei denen tatsächlich Viren gefunden wurden, anstatt alle Accounts durchzukämmen; bei denen die Beschäftigten möglichst selten kontrolliert werden (zB. wird eine unangekündigte Stichprobe einmal im Quartal mitunter ausreichen, um festzustellen, ob die Arbeitsqualität im Verkauf gehalten wird, dazu müssen nicht täglich „Mystery Shopper“ die Läden durchwühlen)

Kurzum muss festgestellt werden, ob die Relation zwischen den eingesetzten Mitteln und dem damit zu erreichenden Zweck gegeben ist.

Kontrolle

Gesondert geregelt und auf ihre Datenschutz-Konformität überprüft werden sollte die geplante Weitergabe von Daten an Dritte oder eine Auftragsdatenverarbeitung durch einen externen Dienstleister.

Das Kontrolle zur unselbstständigen Erwerbstätigkeit dazugehört, ist unbestreitbar, jedoch darf diese Kontrolle den vorgenannten Prinzipien nicht widersprechen!

Danke!

Für Ihr Interesse