1. Kapitel
Einleitung

Wolfgang Goricnik/Josef Grünanger

I. Einleitung

Mitarbeiterkontrolle oder genauer **„Kontrollunterworfenheit“** ist dem **Arbeitsvertrag immanent.** AN schulden nach dem arbeitsvertraglichen Synallagma „sorgfältiges Bemühen“ und erhalten im Gegenzug Entgelt vom AG. Diese Kontrolle des arbeitsvertraglich Geschuldeten ist grds zulässig, weil jede Vertragspartei die Einhaltung der vertraglich vereinbarten Leistung überprüfen darf. Allerdings folgt aus der besonderen arbeitsvertraglichen Beziehung, die sich insb aus der **persönlichen Abhängigkeit** der **AN** ergibt, die ihre Person in die fremdbestimmten betrieblichen Abläufe einbringen (müssen), dass **Kontrollen** durch den AG **nicht schrankenlos** durchgeführt werden dürfen. Oder **semantisch** formuliert: „**Kontrolle ist nicht** mit **Überwachung** gleichzusetzen“. Die Grenzen zwischen erlaubter „Kontrolle“ und unerlaubter „Überwachung“ sind aber in vielen Fällen nur schwer zu erkennen. Ein **Ziel** dieses **Handbuches** ist deshalb auch das **praxisorientierte Herausarbeiten** dieser **Grenzen,** insb auch anhand veranschaulichender Beispiele. **1.1**

Der Begriff **„Arbeitnehmerdatenschutz“** ist der **österreichischen Rechtsordnung** bis dato **fremd.** Ein **eigenes AN-Datenschutzrecht** ist (im Gegensatz zur BRD) auch **nicht vorgesehen.** Neben anderen rechtspolitischen Nachteilen dieser **legistischen Lücke,** wie **mangelnde arbeitsrechtliche Rechtssicherheit,** kann diese legistische Lücke nach Anwendbarkeit der **EU-Datenschutz-Grundverordnung (DSGVO) ab** dem **25. 5. 2018** zu einem nationalen Souveränitätsverlust dergestalt führen, dass gemäß dem in der DSGVO grds vorgesehenen „One-Stop-Shop“-Verfahren über Fragen (auch) des österreichischen AN-Datenschutzrechts für europaweit agierende Konzerne vorab dann „federführend“ am Sitz ihrer (ausländischen) Hauptniederlassung entschieden werden könnte. Die DSGVO, die kraft ihres Verordnungscharakters grds ein europaweites datenschutzrechtliches **Voll-Harmonisierungsziel** anstrebt, würde mit einer sogenannten **„Öffnungsklausel“** in ihrem **Art 88** nämlich die weitgehende **Möglichkeit** eines **eigenen nationalen AN-Datenschutzrechts** (auch iSe eigenständig österreichischen unternehmerischen Standortes mit eigenen Datenschutz-Lösungen) eröffnen, von welcher Möglichkeit der **Gesetzgeber** des DSG 2018 letztlich aber **keinen Gebrauch** gemacht hat. **Ob** vermittels dieser Öffnungsklausel, die auch „Kollektivvereinbarungen“ ermächtigt, „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext“ vorzusehen, diesbezüglich **über** die **betriebsverfassungsrechtlichen Gestaltungsmittel** des **KollV und** der **BV** – quasi subsidiär – ein **branchen- und betriebsspezifisches AN-Datenschutzrecht österreichischer Prägung** erreicht wird, wird sich **zukünftig erweisen.** **1.2**

1.3 **Für** das **Arbeitsrecht** sind – abgesehen von kollektiven Rechten von BR ua zur „Kontrolle der arbeitgeberseitigen Kontrolle" – zur Ermittlung entsprechender **individueller Rechtspositionen** der AN deshalb (vorläufig) also weiterhin **nur** die **allgemeinen Persönlichkeitsrechte** und die **allgemeinen datenschutzrechtlichen Regelungen** (insb in der DSGVO) heranzuziehen; **lediglich** zur Regelung der Bildverarbeitung findet sich – so wie schon bisher zur Videoüberwachung – eine **isolierte Schutznorm zugunsten von AN** (unter dem Titel der **Unzulässigkeit von Bildaufnahmen zum Kontrollzweck**) im DSG 2018.

1.4 Im Folgenden soll zum besseren Verständnis noch kurz die **wesentliche Änderung** des **datenschutzrechtlichen Rechtsschutzes per 1. 1. 2014** sowie **per 25. 5. 2018** dargestellt werden, zumal das Thema der zulässigen Verwendung von AN-Daten in den letzten Jahren praktisch nur von datenschutzrechtlichen E der DSK bzw DSB (und nicht von arbeitsgerichtlichen E) behandelt wurde:

1.5 Nach der DSG-Novelle 2013 (BGBl I 2013/57), die in Entsprechung des Urteils des EuGH 16. 10. 2012 (C-614/10, *Kommission*/Österreich, ECLI:EU:C:2012:631) gemäß der europarechtlichen Vorgabe in der DSRL (Art 28 Abs 1 Unterabsatz 2 RL 95/46/EG) die völlige Unabhängigkeit der Datenschutzkommission (DSK) gewährleisten sollte, wurde mit der DSG-Novelle 2014 (BGBl I 2013/83) per 1. 1. 2014 die **neue unabhängige Datenschutzbehörde (DSB)** mit den Agenden der DSK betraut, die bundesverfassungsgesetzlich (Anlage zum BGBl I 2012/51) mit diesem Datum aufgelöst wurde. Diese Datenschutzbehörde ist aus Gesichtspunkten der Unabhängigkeit anders als die Kollegialbehörde DSK als **monokratische Behörde** eingerichtet (die Behörde ist also nicht mehr paritätisch besetzt), der ein **weisungsfreier „Leiter der Datenschutzbehörde"** (aktuell *Andrea Jelinek*) vorsteht. Bei der DSK anhängige Verfahren waren von der Datenschutzbehörde fortzuführen.

1.6 Per 1. 1. 2014 wurde überdies die generelle große Verwaltungsreform insb zum Ausbau des gerichtlichen Rechtsschutzsystems (auch iSd „Gerichtsgarantie" des Art 47 GRC) in Kraft gesetzt, die dann den **Instanzenzug im Datenschutzrecht** um **eine Instanz erweitert** hat: Von der Datenschutzbehörde geht dieser nunmehr an das neue **Bundesverwaltungsgericht** (mit voller Kognitionsbefugnis) und von dort (allenfalls) als Revision zum Verwaltungsgerichtshof; daneben ist auch die Erhebung einer Beschwerde beim VfGH (wie bisher) möglich. Das neue Bundesverwaltungsgericht entscheidet in Datenschutzangelegenheiten gemäß dem „Materiengesetz" DSG 2018 durch einen Senat. Der Senat besteht aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der AG und der AN. In einem derartigen Verfahren kommt der (belangten) DSB Parteistellung zu; gegen aufhebende oder abändernde E des BVwG kann die DSB Revision an den VwGH erheben. Das Verfahrensrecht findet sich im Verwaltungsgerichtsverfahrensgesetz (VwGVG) BGBl I 2013/33 idF BGBl I 2018/57, das Organisationsrecht im Bundesverwaltungsgerichtsgesetz (BVwGG) BGBl I 2013/10 idF BGBl I 2018/22.

1.7 Gem dem Regelungsauftrag des Art 51 Abs 1 DSGVO sehen die §§ 18 ff DSG 2018 die **DSB nunmehr** als **nationale „Aufsichtsbehörde" zur Überwachung** der **(unionsweit einheitlichen)** Anwendung der **DSGVO** vor. Die DSB hat insb eine **Liste der Verarbeitungsvorgänge** zu erstellen und **als VO kundzumachen,** für die die **neue Datenschutz-Folgenabschätzung** (an Stelle der bisherigen Vorabkontrolle) **durchzuführen** ist („Black

List"). Die DSB kann **des Weiteren** eine **Liste** der Arten von Verarbeitungsvorgängen erstellen und als VO veröffentlichen, für die **keine Datenschutz-Folgenabschätzung erforderlich** ist („White List"). Diese VO wurde bereits erlassen (BGBl II 2018/108). Mittlerweile wurde auch die VO über Verarbeitungsvorgänge erlassen (BGBl II 2018/278), für die jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V). Beide VO beziehen das Vorliegen von BV in die datenschutzrechtliche Beurteilung von Datenverarbeitungen ein.

1.8 **Grds neu** sind kraft der europarechtlichen Vorgabe die **Befugnisse der DSB,** selber **drastische Geldbußen** (insb direkt gegen Unternehmen) **bis** zur Höhe von **EUR 20 Millionen** (!) **oder** bis zu **4% des gesamten weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres zu **verhängen,** je nachdem, welcher der Beträge höher ist. Nicht zuletzt Höhe und Modus dieser effektiven Sanktionierungsmöglichkeit von Verstößen, die an das europäische Wettbewerbsrecht gemahnt, haben schon zu einer deutlich **gestiegenen unternehmerischen Awareness** der Bedeutung von Datenschutzrecht geführt.

1.9 Diese seitens der EU gesteigerte Bedeutung des Datenschutzrechts ist nicht nur dem **Datenschutz** (insb von Konsumenten) geschuldet, sondern besonders dem **Funktionieren des europäischen Binnenmarktes** (vor allem hinsichtlich des Verbrauchervertrauens auf einen effektiven grenzüberschreitenden Datenschutz und des Vertrauens in die Sicherheit entsprechender digitaler Dienste, aber auch hinsichtlich entsprechender – neuer – auf der zunehmenden Digitalisierung beruhender Geschäftsmodelle iSd **Entwicklung** einer **eigenständigen EU-Datenwirtschaft**).

A. Entwicklung und Bedeutung des Gegensatzpaares von Mitarbeiterkontrolle und AN-Datenschutz

1.10 Sowohl „Mitarbeiterkontrolle" als auch „Arbeitnehmerdatenschutz" werden in der betrieblichen Praxis zunehmend bedeutender. Dies hat mehrere Ursachen. Zu nennen ist insb der immer schneller ablaufende technische Fortschritt. Aufgrund dieses technischen Fortschrittes können AG heute so viele (hauptsächlich digitale) Informationen über ihre AN wie noch nie zuvor – und das auch noch dazu immer billiger – erlangen. Gerade iZm dem Einsatz cyber-physischer Produktionssysteme (CPPs) im Rahmen der sogenannten vierten industriellen Revolution (Schlagwort „Industrie 4.0") und der damit einhergehenden Mensch/Maschine-Kommunikation werden laufend Unmengen an Daten generiert, die in vielen Fällen (gerade im Arbeitsleben) zumindest personenbeziehbar sind. An Hand dieser „Datenspuren" wäre es ein leichtes Unterfangen, AN erstens in Echtzeit und zweitens feinkörnig zu kontrollieren oder gar zu überwachen. Entsprechendes gilt für den flächendeckenden Einsatz modernster IKT (insb Kollaborationsplattformen, zB „Workplace by Facebook"). Hier ist insb rechtlich beschränkend zu fragen, welche Informationen bzw Daten überhaupt ermittelt, gespeichert und zu welchen Zwecken und von wem diese Informationen bzw Daten (personenbeziehbar) ausgewertet werden dürfen.

1.11 Denn die **neuen Datensammlungs- und Datenanalyse-Werkzeuge** iVm erschwinglicher Rechenleistung zur entsprechenden Auswertung in immer mehr Richtungen (zB den Grad der „inneren Kündigung" eines AN) unabhängig vom Primärzweck der Datenermittlung bzw überhaupt losgelöst von einem ursprünglichen bestimmten Zweck der Datenermittlung (dh insb **Datenermittlung „auf Vorrat"**) können einerseits zwar dabei

helfen, die Betriebsabläufe iSe **Effizienzsteigerung** besser zu analysieren und auch Wahrscheinlichkeiten und Korrelationen einzusetzen, um entsprechende **Vorhersagen** zu treffen (Stichwörter „Big Data" bzw „Smart Data"); gleichzeitig steigen damit aber die Gefahren einer Aushöhlung der geschützten Privatsphäre des einzelnen AN **(Stichwort „Profiling"),** des unbehaglichen Gefühls einer (technisch ja leicht möglichen) immerwährenden Kontrolle sowohl der Arbeitsleistung als auch des Verhaltens am Arbeitsplatz (mit dem Verständnis einer **permanenten Bewährungspflicht**) sowie des immanenten Zwanges zu Konformismus im Betrieb **(Stichwort „Post-Panoptismus").**

1.12 Der Gesetzgeber tut sich weiters zunehmend schwerer, zeitnah auf die laufenden technischen Entwicklungen und gesellschaftlichen Strömungen, die sich naturgemäß auch auf das Arbeitsleben auswirken (man denke nur an den rasant **wachsenden Anteil** von **„Social Media"** an zwischenmenschlicher Kommunikation), zu reagieren. Die DSRL (RL 95/46/EG) der Europäischen Union stammte etwa aus dem Jahr 1995. Es kann angenommen werden, dass die Verhandlungen zu dieser DSRL bereits Jahre davor begonnen haben. Zu dieser Zeit steckte das Internet in den Kinderschuhen, und die Mobiltelefonie begann den europäischen Binnenmarkt gerade erst zu erobern. Mit der Datenflut, mit der wir es heute aufgrund dieser – sich noch dazu stetig verbessernder – Technologien (man denke nur an die Entwicklung von den ersten Mobiltelefonen bis hin zur neuesten Smartphone-Generation, eigentlich leistungsstarken Computern im Scheckformat) zu tun haben, wurde damals sicher nicht gerechnet, und es konnte darauf auch keine Rücksicht genommen werden, zumal sich ja auch immer wieder neue Formen von Datenanwendungen entwickeln (zB die RFID-Technologie als **„Internet der Dinge"**). Obwohl die **DSGVO** auf die Implikationen eingeht, die der Einsatz des Internet und die Ausweitung der Globalisierung mit sich bringen, neue technologische Möglichkeiten und Gefahren (zB das „Profiling") berücksichtigt und angesichts der raschen technologischen Entwicklungen grds einen **technikneutralen Ansatz beibehält,** stellt sich die grds **Frage,** ob die **evolutionäre Weiterentwicklung des Datenschutzrechtes** mit einer sogenannten **„disruptiven" technologischen Entwicklung Schritt halten** kann.

1.13 Die jüngste Datenschutz-Regelung in Österreich, nämlich das **DSG 2018, basiert auf** der **DSGVO** bzw **implementiert diese** lediglich in schlanker Form, wobei von vielen fakultativen Öffnungsklauseln nicht oder nur restriktiv Gebrauch gemacht wird. Dies hat zur Folge, dass **in der Praxis** (nach wie vor) in vielen Fällen **Rechtsunsicherheit** bestehen wird, weil die anzuwendenden Normen oft einen abstrakten oder generalklauselhaften Inhalt haben und deshalb einen weiten Raum für Interpretation offenlassen (vor allem auch angesichts der **verschiedenen authentischen Sprachfassungen** der DSGVO); **detaillierte Regelungen fehlen vielerorts** (bzw **darf sie** der **Gesetzgeber** gem der Rechtsnatur der DSGVO **europarechtlich** gar **nicht erlassen**), wobei dem Gesetzgeber zu Gute zu halten ist, die mit der DSG-Novelle 2010 geschaffenen speziellen Regelungen für die Videoüberwachung in den §§ 50a ff DSG 2000 auch im DSG 2018 beibehalten bzw sogar nachgeschärft zu haben (unter dem Titel der Bildverarbeitung samt mitverarbeiteten akustischen Informationen in § 12f DSG 2018).

1.14 Aus unserer Sicht sollte ein **ausreichender AN-Datenschutz** idS auch zu einer diesbezüglichen **Vertrauenskultur am Arbeitsplatz** führen, sodass eine fortschreitende Technisierung und Digitalisierung der Arbeit nicht als Bedrohung der Persönlichkeit und

Individualität angesehen, sondern als simpler Produktivitätsfaktor ohne Auswirkung auf die soziologischen Machtverhältnisse im Betrieb erlebt wird. Ein weiterer Grund für die Zunahme von Mitarbeiterkontrollen ist das immer größer werdende Verlangen nach Transparenz, auch bei privaten Unternehmen. Einige Unternehmen haben in den vergangenen Jahren dafür sog „Compliance-Offices" eingerichtet. Vorrangiges Ziel dieser ist die Verhinderung und/oder Aufklärung von Straftaten. Aber auch die Einhaltung unternehmensinterner freiwilliger Richtlinien oder Vorgaben soll durch ausreichende Kontrolle gewährleistet werden. **„Compliance"** hat insb deshalb stark an Bedeutung gewonnen, weil gerade Vorstände bzw Geschäftsführer für die Einhaltung bestimmter Regelungen verantwortlich und meist haftbar sind. IdZ sind zB der Österreichische Corporate Governance Kodex (idF Kodexrevision 2018), Kap „IV. Vorstand" über die Verantwortung des Vorstandes, aber auch § 82 AktG bzw § 22 Abs 1 GmbHG, die die Errichtung eines unternehmensinternen Kontrollsystems verlangen, zu nennen. Hinzuweisen ist auch auf § 9 VStG, wonach verwaltungsstrafrechtlich für die Einhaltung verwaltungsrechtlicher Vorgaben verantwortlich ist, wer zur Vertretung nach außen berufen ist. Gerade diesbezüglich sind auch die rechtlichen Kontrollmöglichkeiten von Bedeutung. Erst wenn eine bestimmte **Kontrollmaßnahme** arbeitsrechtlich unzulässig ist, kann aus ihrer Unterlassung dann auch keine Haftung (zB für einen Vorstand) entstehen. Ansonsten wäre sie aber (auch) **unter Compliance-Gesichtspunkten zu implementieren.** Insofern haben arbeitsrechtliche Regelungen zur möglichen und zulässigen Kontrolle von AN auch auf diesem Gebiet Relevanz. Dabei darf aber nicht außer Acht gelassen werden, dass **umgekehrt auch** die **Einhaltung** von **Vorgaben des Datenschutzrechtes unter** diese **Compliance fällt.**

1.15 ZB können aus verwaltungs(straf-)rechtlicher Sicht „wirksame" Kontrollsysteme erforderlich sein. So sind nach der Judikatur des VwGH hinsichtlich des technischen AN-Schutzes sämtliche technischen Möglichkeiten auszuschöpfen, um die Einhaltung von AN-Schutzvorschriften kontrollieren zu können (zB VwGH 18. 8. 2015, Ro 2015/11/0003; vgl zur Problematik auch *Lesigang,* Überwachungspflichten des AG iS verwaltungsstrafrechtlicher Judikatur 83 ff). Hierbei kann es also zu **schwierigen Abwägungen** zwischen dem Schutz von Leib und Leben von AN sowie der Absicherung des AG vor verwaltungsstrafrechtlicher Verantwortlichkeit einerseits und datenschutzrechtlichen Ansprüchen der AN andererseits kommen.

1.16 Aber auch das gesellschaftliche Bedürfnis nach immer mehr „Sicherheit", das auch von staatlichen Stellen vorgelebt wird (man denke nur an die – globale – Zurückdrängung von bürgerlichen Freiheitsrechten zugunsten Maßnahmen gegen eine diffuse Gefahr des Terrorismus und idZ zB an die – ehemalige – europäische Vorratsdatenspeicherung) und von einer wachsenden „Sicherheitsindustrie" gerne bedient wird (idZ sei die Ausuferung von Videoüberwachung erwähnt), bleibt nicht ohne Auswirkung auf das Arbeitsleben (wenn zB nicht nur der Kunde, sondern auch der AN zunehmend im Blickfeld der Videokamera steht).

1.17 Hauptzweck der arbeitsrechtlichen Normen ist der Schutz von AN-Rechten, gegenständlich idR **Persönlichkeitsrechten,** worunter vermehrt auch der Schutz vor übermäßiger Kontrolle verstanden wird (vgl das **Schlagwort** vom **„gläsernen AN"**). Zusätzlich sollen in diesem Handbuch die für den AN-Datenschutz relevanten Ableitungen aus dem all-

gemeinen Datenschutzrecht aufgezeigt werden. Angesichts der dargestellten Entwicklungen sind diese beiden Rechtsbereiche (nämlich **Arbeitsrecht und Datenschutzrecht**) zunehmend **gefordert,** die – der **Mitarbeiterkontrolle gegenläufigen** – entsprechenden **Rechte** der **AN** zu **gewährleisten,** insb um **Rechtsstaatlichkeit und Grundrechtsschutz auch** am **Arbeitsplatz** zu erfahren, was in einer demokratischen Gesellschaft auch eine **politische Grundforderung** sein muss.

1.18 Der Großteil der Bevölkerung steht in einem Arbeitsverhältnis und ist auf ein Erwerbseinkommen angewiesen. Aus der wirtschaftlichen Unterlegenheit und der persönlichen Abhängigkeit ergibt sich, dass AN während eines aufrechten Arbeitsverhältnisses bei rechtswidriger Kontrolle bzw rechtswidriger Datenverwendung selten gegen den AG vorgehen werden. IdZ sind deshalb auch die **kollektiven Schutzmechanismen** der bestehenden Rechtslage im Betriebsverfassungsrecht **herauszuarbeiten,** es soll aber darüber hinaus auch Fragen entsprechender (neuer) **Sanktionen und Konsequenzen** (zB möglicher **Verwertungsverbote** rechtswidrig erlangter Beweismittel) nachgegangen werden.

II. Aufbau des Praxishandbuches

1.19 Das Handbuch soll in erster Linie einen Beitrag dazu liefern, dass die Grenzen zwischen zulässigen und unzulässigen praxisrelevanten Kontrollmaßnahmen klarer und nachvollziehbar aufgezeigt werden können. Viele Regelungen zur Mitarbeiterkontrolle oder dem AN-Datenschutz sind Generalklauseln (zB §§ 16, 1157 ABGB, § 96 Abs 1 Z 3 ArbVG, § 1 DSG 2000) oder lassen Raum für Interpretation und Argumentation (zB § 12 Abs 4 Z 2 DSG 2018). Deshalb ist es sinnvoll, nach einer **übersichtlichen Darstellung** der anwendbaren **Regelungen** des **Arbeits- und Datenschutzrechts** im **Allgemeinen Teil** zu den jeweiligen **praxisrelevanten und aktuellen Kontrollthematiken** im **Besonderen Teil** vor diesem rechtlichen Hintergrund verschiedene praktische Fallgruppen zu diskutieren, um zu rechtskonformen, aber auch **praxisgerechten Lösungen** zu kommen. So kann auf verschiedene Probleme im Speziellen eingegangen werden. ZB werden an Kontrollen des Gesundheitszustandes von AN andere rechtliche Anforderungen als an eine Videoüberwachung von AN zu stellen sein.

1.20 Auch sind moderne Technologien, wie etwa die GPS-Ortung oder eine digitale Videoüberwachung, wiederum viel stärker mit Datenschutzrecht verwoben als herkömmliche Tor- oder Taschenkontrollen.

1.21 In vielen Fällen läuft die Prüfung der Zulässigkeit von Kontrollmaßnahmen auf eine Interessenabwägung zwischen berechtigten Zwecken des AG einerseits und beeinträchtigten Persönlichkeitsrechten der AN andererseits hinaus. Im Besonderen Teil sollen dabei Kriterien für eine solche Interessenabwägung herausgearbeitet werden. **Verschiedene Kontrollarten** und **Kontrollmethoden** werden diesbezüglich zu **unterschiedlichen Ergebnissen** dieser **Interessenabwägung** führen. Gleichzeitig dürfen dabei die spezifischen Gehalte und Schutzrichtungen der verschiedenen anwendbaren Normen aber nicht unter den Tisch fallen; die Diskussion der einzelnen Fallgruppen soll auch aufzeigen, dass es die diesbezüglich komplexe Rechtslage nicht zulässt, die verschiedenen Normen einfach in einem „Mischtatbestand" einer einheitlichen Interessenabwägung für alles und jedes aufgehen zu lassen (vgl entsprechend *Rebhahn,* Mitarbeiterkontrolle 26 f).

Das würde nämlich auch die Gefahr mit sich bringen, dass einfach aktuelle (und „tech- **1.22**
nikgetriebene") gesellschaftspolitische Strömungen unreflektiert zur vermeintlichen Lösung komplizierter Lebenssachverhalte am Arbeitsplatz benützt werden, ohne sich sorgsam (und oft auch mühsam) mit der **diffizilen Ausmessung gegenläufiger Rechtspositionen** auseinanderzusetzen, was allein aber zu ausgewogenen und tragfähigen Lösungen führt. Diese Lösungen sollen letztlich dazu führen, dass AN nicht nur als reine (messbare) Ressource angesehen werden, die am besten keine eigene Persönlichkeit mehr aufweisen. Nämlich abgesehen davon, dass dadurch viel kreatives Potenzial im Betrieb zugunsten einer „Normung" von AN verloren ginge, verlöre **Arbeit** dadurch auch ihre **sinnstiftende Funktion** für den Menschen, was auch von **eminenter gesellschaftspolitischer Bedeutung** ist.

So soll dieses Handbuch letztlich auch dem hehren Zweck dienen, das Bewusstsein um **1.23**
diese Zusammenhänge nicht auf dem Altar der Technikgläubigkeit und kühlen „Nützlichkeit" zu opfern und das Augenmerk statt auf eine „Technikzentrierung" auf eine **„Humanzentrierung"** zu richten.

9783214020675
Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle | 2
Josef Grünanger, Wolfgang Goricnik
MANZ Verlag Wien

2. Kapitel
Allgemeines

Wolfgang Goricnik/Josef Grünanger/Jens Winter

I. Einführung

Anders als in einigen anderen Mitgliedstaaten der EU gibt es in Österreich **kein** eigenes **Gesetz zum Arbeitnehmerdatenschutz,** sondern einige wenige einschlägige Normen in verschiedenen Gesetzen.[1] **2.1**

Allerdings wurden gesetzliche **Regelungen** zur **Nutzung von Informations- und Kommunikationstechnologie** und **entsprechende Kontrollmaßnahmen** für den **öffentlichen Dienst** beschlossen.[2] In den §§ 79c–79i BDG wurden Regelungen zum Umgang mit IKT-Einrichtungen festgeschrieben (dazu im Detail Rz 6.71 ff). Bemerkenswert ist, dass nach § 79e Abs 1 BDG die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren – anders als im Arbeitsrecht der Privatwirtschaft –, unzulässig ist. Ob und inwiefern daraus für privatrechtliche Arbeitsverhältnisse Rückschlüsse gezogen werden können, wird in Rz 6.86 ausgeführt. **2.2**

Folgende Szenarien der Mitarbeiterüberwachung können beobachtet werden: **Kontrolle des Arbeitsergebnisses,** Kontrolle **der Leistung** und/oder **des Verhaltens** der Mitarbeiter während und außerhalb der Arbeitszeit, Kontrolle **der Benützung** von **technikunterstützten Betriebsmitteln** (Telefon, Internet, E-Mail) des AG,[3] aber auch schon die Kontrolle **der Benützung** von **AN-eigenen Betriebsmitteln** (zB Smartphones, Stichwort „BYOD"). **2.3**

Rechtlich differenziert betrachtet werden muss die **Art** des **Beschäftigungsverhältnisses.** Freie DN sind im Gegensatz zu AN nicht in die betriebliche Organisation eingegliedert. In Bezug auf Arbeitszeit, Arbeitsort und Arbeitsinhalt sind freie DN weitgehend nicht fremdbestimmt.[4] Bei freien DN fehlt somit das Element der Fremdbestimmung, das bei AN manche Kontrollmaßnahmen rechtfertigen kann. **Außerhalb** eines **regulären Arbeitsverhältnisses** sind sohin **viele** dieser **Kontrollmaßnahmen unzulässig.**[5] **2.4**

II. Rechtsgrundlagen

Es gibt in Österreich kein Arbeitnehmerdatenschutzgesetz, wohl aber **einzelne einschlägige Normen,** die dem Arbeitnehmerdatenschutz unmittelbar oder mittelbar dienen. **2.5**

1 Zur Rechtslage in anderen Staaten vgl zB *Colucci,* The Impact 73 ff.
2 Vgl dazu schon *Hartmann,* jusIT 2010, 48.
3 *Rebhahn,* Mitarbeiterkontrolle 13.
4 Vgl zB *Rebhahn* in ZellKomm[3] § 1151 ABGB Rz 55 ff; *Schrammel* in *Klang*[3] § 1151 ABGB Rz 60 ff.
5 Dazu näher *Goricnik,* Datenschutzrechtliche Aspekte der Stellung der CrowdworkerInnen, in *Lutz/Risak* 250 f.

Nach ihrem Schutzcharakter unterscheiden diese Normen bzgl ihres Anwendungsbereichs zwischen **Individual**- und **Kollektivschutz.** Individualschutz schützt die Interessen einzelner Personen und damit auch einzelne Mitarbeiter in ihrem Arbeitsverhältnis. Normen betreffend den Kollektivschutz schützen erstens nur AN iSd ArbVG und sind zweitens nur bei Maßnahmen mit kollektivem Charakter anzuwenden. Regelungen zum (iwS) datenschutzrechtlichen Individualschutz speziell im Arbeitsverhältnis finden sich kaum in der österreichischen Rechtsordnung, zu nennen sind § 10 AVRAG[6] und § 12 Abs 4 Z 2 DSG 2018. Allgemein zu nennen sind § 16 ABGB und § 1 DSG 2000, ferner § 1328a ABGB, welcher rechtswidrige und schuldhafte Eingriffe in die Privatsphäre schadenersatzrechtlich sanktioniert. Diese Norm ist trotz der Subsidiaritätsklausel des Abs 2 auch für das Arbeitsverhältnis anwendbar, weil sich im Arbeitsrecht keine besondere Bestimmung dieser Art findet.[7] Normen des Kollektivschutzes finden sich in den § 96 Abs 1 Z 3, § 96a Abs 1 Z 1 und 2 und § 97 ArbVG. Bei **Maßnahmen mit kollektivem Bezug** sind **zusätzlich** auch die **individualrechtlichen Bestimmungen** zu beachten. Die Verletzung von (nationalen) individualrechtlichen Bestimmungen kann also nie durch die rechtmäßige Beachtung und Anwendung der kollektiven Bestimmungen geheilt bzw gerechtfertigt werden.[8] Ob diese apodiktische Aussage durch die unionsrechtliche Öffnungsklausel des Art 88 Abs 1 DSGVO unter bestimmten Umständen zu relativieren ist, wird in Rz 2.86f exemplarisch erörtert.

A. Individualrechtliche Bestimmungen

1. § 16 ABGB – Persönlichkeitsrechte im Privatrecht

2.6 Diese als **Generalklausel** formulierte Bestimmung soll die Persönlichkeitsrechte des Einzelnen schützen. Konkretisiert wird diese Norm durch die Wertungen der verfassungsmäßig garantierten Rechte, aber auch der einfachgesetzlich normierten besonderen Persönlichkeitsrechte.[9] Auf diese Weise sind die Grundrechte mittelbar auch zwischen Privaten anzuwenden. Viele Autoren bezeichnen diese Bestimmung deshalb als **„Einfallspforte" der Grundrechte in** das **Privatrecht.**[10] Die hL von der **mittelbaren Drittwirkung** der **Grundrechte** besagt nämlich, dass die Grundrechte im Privatrecht besonders zur Konkretisierung von Generalklauseln herangezogen werden können. In diesem Zusammenhang erfüllt § 16 ABGB eine wichtige Funktion: Die Bestimmung lässt die grundrechtlichen Wertungen in den privatrechtlichen Persönlichkeitsschutz einfließen und wirkt so als eine **Schnittstelle zwischen** dem **Öffentlichen Recht und** dem **Privatrecht.**[11]

---

6 Da diese Bestimmung (mit Ausnahme des persönlichen Geltungsbereiches) inhaltlich § 96 Abs 1 Z 3 ArbVG gleichzusetzen und auch so auszulegen ist, wird sie im Weiteren bei den „kollektivrechtlichen Bestimmungen" näher miterörtert.

7 Vgl *Rebhahn,* Mitarbeiterkontrolle 15.

8 ZB *Strasser/Jabornegg,* ArbVG § 96 Anm 17; *Reissner* in ZellKomm[3] § 96 ArbVG Rz 26.

9 *Aicher* in *Rummel/Lukas,* ABGB[4] § 16 Rz 1; *Schauer* in *Kletečka/Schauer,* ABGB-ON[1.02] § 16 Rz 11.

10 ZB *Binder,* Detektiveinsatz und Arbeitnehmerkontrolle 15; *Brodil,* ZAS 2004, 156; *Brodil,* Individualarbeitsrechtliche Fragen 72.

11 *Schauer* in *Kletečka/Schauer,* ABGB-ON[1.02] § 16 Rz 15 mwN.