GRENZENLOSE FREIHEIT?

Datenschutz und Überwachung im Außen- und Mobildienst

IG EXTERNAL

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

www.gpa-djp.at

Unser Service für Sie:

- **Rechtsberatung und Rechtsschutz** in arbeitsrechtlichen Angelegenheiten
- **Beratung** zu Arbeitsrecht, Arbeitszeit, Abfertigung Neu, Kollektivvertrag, Einstufung, Überstunden, Karenz und Mutterschutz, Weiterbildung uvm.
- Mehr **Information** durch die Mitgliederzeitschrift **KOMPETENZ**
- Umfassendes **Service** durch die Mitglieds-**CARD**, auch im Bereich Freizeit, Sport, Kultur und Urlaub

Mitglied sein bringt's!

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

VORWORT

Außendienst, Mobildienst, Arbeit außerhalb des Betriebes: Die kundennahe berufliche Tätigkeit hat viele Besonderheiten. Unzählige Kilometer unterwegs zwischen den Arbeitseinsätzen, unregelmäßige Arbeitsrhythmen und oft erschwerte Arbeitsbedingungen zählen dazu. Aber besonders ein Umstand macht diese mobile Arbeit seit jeher für viele Menschen sehr attraktiv: Meist auf sich allein gestellt, allein verantwortlich, muss und kann man sich die Arbeit etwas autonomer gestalten, als das im Betriebsverband möglich ist. Kein Vorgesetzter, der auf die Uhr sieht, wenn man kommt oder geht, kein Stempeln der Arbeitszeiten. Eine kleine Pause zwischen zwei Terminen, damit der Stresspegel herunterkommt, ein kurzes Zusatzplauscherl mit einer Kundin, ein selbst gewählter kleiner Umweg, um dem Stau zu entgehen.

Solche kleine Freiheiten sind lange Zeit Motivation und Ausgleich für erschwerte Arbeitsbedingungen gewesen. Grenzenlos waren diese Freiheiten zwar nie. Aber gibt es diese Freiheiten überhaupt noch in Zeiten der ständigen elektronischen Vernetzung jedes Mitarbeiters und jeder Mitarbeiterin mit Mobiltelefon, Laptop oder Tablet? Gibt es überhaupt noch Freiräume in Zeiten der lückenlosen Verfolgung und Aufzeichnung aller Wege und Aufenthaltsorte mittels GPS? Wo enden die angenehmen Seiten elektronischer Hilfen aus der Zentrale und wo beginnen Kontrolle und Überwachung lästig oder gar erdrückend zu wirken?

Die Interessengemeinschaft für Außen- und Mobildienst IG EXTERNAL hat sich in Theorie und Praxis und in Zusammenarbeit mit der Abteilung Arbeit und Technik der GPA-djp diesen Fragen eingehend gewidmet. Im Sommer 2012 wurde eine Online-Umfrage zum Thema „Technologie als Unterstützung und/oder Kontrollmaßnahme?" durchgeführt, an der sich mehr als 300 Personen beteiligt haben. In der vorliegenden Broschüre legt die GPA-djp Informationen und Werkzeuge vor, die der kollektiven Regelung der ArbeitnehmerInnenrechte und des Datenschutzes im Außen- und Mobildienst dienen.

Ziel der Bemühungen ist es, mittels fairer Regelungen sinnvolle Anwendungen mobiler elektronischer Technik mit der Abwehr allzu drastischer Kontrollen und Überwachungen zu verbinden und damit Freiräume und Freiheiten im Außen- und Mobildienst zu wahren. Bei der Umsetzung dieses Ziels sind Wissen, Kompetenz und Mut aller Beteiligten und Betroffenen gefragt, der Bediensteten, der Betriebsräte, der Vorgesetzten und nicht zuletzt – ein erstes Bewährungsfeld – der nach der Novelle des Datenschutzgesetzes jetzt einzuführenden Datenschutzbeauftragten. Die Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier wird mit Rat und Nachdruck zum Gelingen der Übung beitragen.

Wolfgang Katzian
Vorsitzender der GPA-djp

Gerhard Prochaska
Vorsitzender IG EXTERNAL

Impressum:

Herausgeber: Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier
Alfred-Dallinger-Platz 1, 1030 Wien
Interessengemeinschaften **IG EXTERNAL**
Für den Inhalt verantwortlich: Dr. Gerald Musger, Interessengemeinschaften;
Mag.ª Clara Fritsch, Geschäftsbereich Grundlagen, Abteilung Arbeit und Technik
Layout: GPA-djp Marketing, Ulrike Pesendorfer
Fotos: GPA-djp, fotolia.com, iStockphoto
DVR: 0046655, ÖGB ZVR-Nr.: 576439352

Stand: August 2012

INHALT

Aktuelle Entwicklungen im Überblick

Sowohl die Gesetzeslage in Österreich als auch die auf EU-Ebene sind derzeit heiß diskutiert. Das Wichtigste in Kürze: in Österreich sind die Einführung eines freiwilligen betrieblichen Datenschutzbeauftragten (DSB), eine Lockerung der behördlichen Kontrollmechanismen sowie eine Erleichterung für Datentransfers innerhalb eines Konzerns im Gange. Auf EU-Ebene soll die gesamte Rechtsetzung im Datenschutz vereinheitlicht, ein Datenschutzbeauftragter für Großbetriebe eingerichtet, Konzernerleichterungen geschaffen und Sanktionen verschärft werden.

EU-Vorgaben wie die Vorratsdatenspeicherung oder das kürzlich vom EU-Parlament gekippte „Anti-Piraterie-abkommen" ACTA beeinflussen den betrieblichen Datenschutz ebenfalls. Insbesondere im Außen- und Mobildienst sind diese Entwicklungen von Relevanz, da hier der Datentransfer von Angestellten zur Firma unumgänglich ist und die täglichen Arbeitsverrichtungen fast lückenlos darstellt sind.

In ihrer Presseaussendung vom 18. Juli 2012 begrüßt die GPA-djp die Einführung des freiwilligen betrieblichen Datenschutzbeauftragten in Österreich und übt zugleich Kritik am Entfall der Vorab-Kontrolle für Videoüberwachung.

Die Einführung eines betrieblichen Datenschutzbeauftragten entspricht einer langjährigen Forderung der GPA-djp. Die konkrete Ausgestaltung dieser Funktion mit Weisungsungebundenheit, Kündigungsschutz, einer Mindestfunktionsperiode sowie ein klar umrissenes Aufgabengebiet und eine Kundmachungspflicht gegenüber der Datenschutzkommission stimmt mit den Forderungen der GPA-djp weitgehend überein. Mit der Installierung eines DSB werde auch der Verwaltungsaufwand reduziert, erklärte GPA-djp-Vorsitzender Wolfgang Katzian: „Hat ein Unternehmen keinen Datenschutzbeauftragten, der das erledigt, müssen nämlich alle Datenanwendungen an das Datenverarbeitungsregister gemeldet werden." Dass eine ausdrückliche Zustimmung der Betroffenen ArbeitnehmerInnen, eine Verwendung ihrer Daten rechtfertigt und zu einem Entfall der Vorab-Kontrolle führt, wird von der GPA-djp kritisiert. Die ungleichen Machtverhältnisse im Arbeitsleben bedeuten ein Abhängigkeitsverhältnis, daher kann man nicht von einer „freiwilligen Zustimmung" der ArbeitnehmerInnen ausgehen.

Die betriebliche Praxis in Österreich zeigt außerdem, dass Videokameras zu den beliebtesten Kontrollinstrumenten zählen. Hier eine behördliche Kontrolle zu unterbinden wäre kaum im Interesse der ArbeitnehmerInnen. Die GPA-djp regt daher an, es bei den geltenden Erleichterung bei der Videoüberwachung zu belassen (z.B. für Trafiken, Tankstellen, Banken) und die erst 2010 eingeführte Genehmigungspflicht bei der Aufbewahrung der Video-Daten länger als 72 Stunden beizubehalten, um Wildwuchs zu vermeiden.

Auch auf EU-Ebene rumort es beim Thema Datenschutz. Der von der Europäischen Kommission vorgelegte Entwurf einer Datenschutzverordnung, die im Gegensatz zur geltenden Richtlinie direkt zu nationalem Recht würde, wird vom ÖGB in vielen entscheidenden Punkten stark kritisiert. Zwar ist das Anliegen, eine einheitliche

Gesetzgebung schaffen zu wollen, zu würdigen, doch die liberalen Gestaltungsmöglichkeiten für Konzerne (es reicht ein DSB für alle Niederlassungen), die Privilegien für Klein- und Mittelbetriebe (sie müssen keinen verpflichtenden Datenschutzbeauftragten einführen) sowie einige andere Bestimmungen lassen befürchten, dass rechtliche Errungenschaften auf nationaler Ebene ausgehebelt werden oder zumindest unter Druck kommen.

Die Diskussions- und Entscheidungsprozesse auf nationaler und europäischer Ebene werden weitergehen, ebenso das Lobbying für die Anliegen der ArbeitnehmerInnen gegenüber der Kommission, dem Europäischen Parlament und den nationalen Regierungen.

(Details zu den konkrete Gesetzen bzw. deren Entwürfen finden sich im rechtlichen Artikel und der Linksammlung in dieser Broschüre.)

Mobile Technologie: Unterstützung und Kontrollmaßnahme

Ergebnisse der Umfrage unter Außen- und Mobildienstbeschäftigten

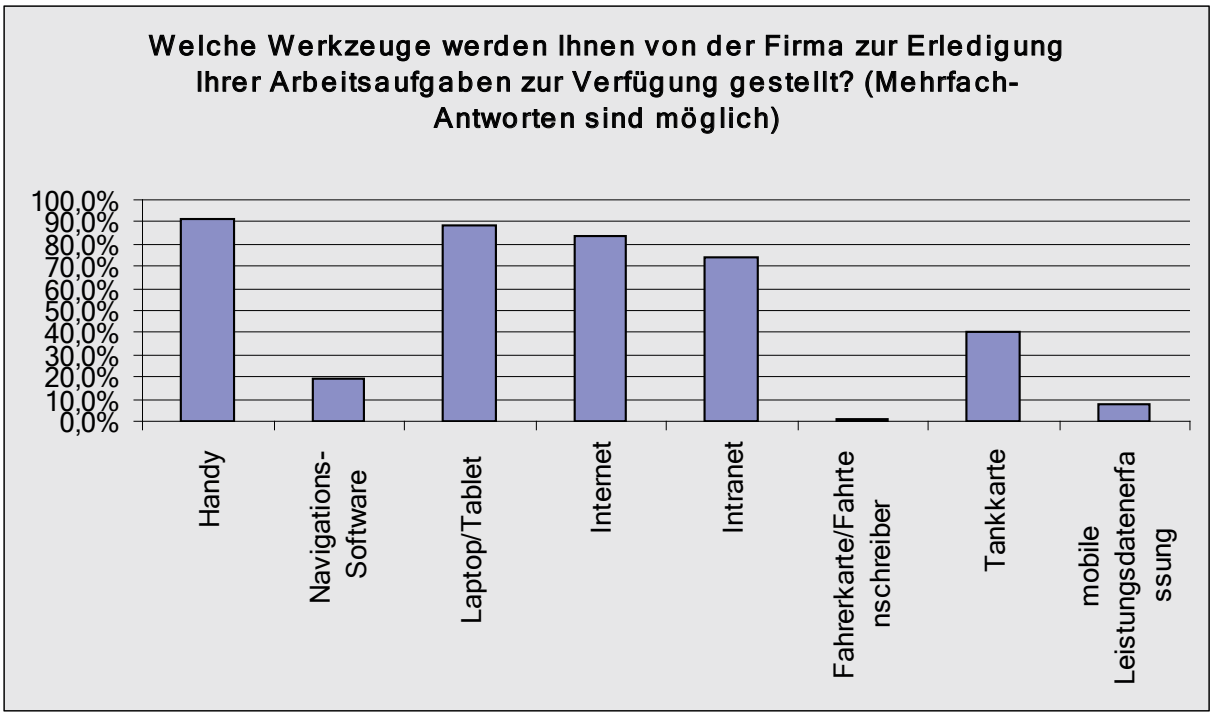
Mobile Technologien spielen im Außen- und Mobildienst eine immer wichtigere Rolle: als unabdingbare Arbeitsinstrumente, zur Aufzeichnung der Arbeitszeiten und Erfassung von Informationen, zur Kommunikation mit der Zentrale, mit KollegInnen, Vorgesetzten und KundInnen. Was als Hilfe und Unterstützung angepriesen wird, hat nicht selten eine Kehrseite: Um diese Fragen und Probleme gut beleuchten und dementsprechende Antworten und Instrumente entwickeln zu können, hat die Interessengemeinschaft IG EXTERNAL in Zusammenarbeit mit der GPA-djp-Abteilung Arbeit und Technik im Juni und Juli 2012 eine Umfrage durchgeführt, die sowohl online als auch über herkömmliche Fragebögen abgewickelt wurde. Hier präsentieren wir die wichtigsten Ergebnisse.

Von über 3000 Adressaten sind uns 306 ausgefüllte Frageboden zugegangen. 27% kamen aus den Bereichen der Finanz- und Versicherungsdienstleistungen, 22% vom technischen Kundendienst, 20% von den sozialen und medizinischen Mobildiensten, 31% teilen sich alle anderen Branchen und Bereiche. Das Gender-Verhältnis bei den Antworten war 80% männlich und 20% weiblich. Nur 6% kamen von Personen unter 30 Jahren, 62% gaben ein Alter zwischen 30 und 50 an, 32% waren älter als 50.

Damit sind die Ergebnisse nicht streng repräsentativ, was die Gesamtheit des Außen- und Mobildienstes betrifft, geben aber dennoch ein ausgewogenes Gesamtbild.

Im Folgenden werden die wichtigsten Ergebnisse entlang der gestellten Fragen zusammengefasst.

- **Welche Werkzeuge werden Ihnen von der Firma zur Erledigung Ihrer Arbeitsaufgaben zur Verfügung gestellt?**



Dass 92% ein Mobiltelefon der Firma haben, überrascht nicht. 88% mit Firmenlaptop, 84% mit Internet bzw. 74% mit Intranetzugang zeigt, wie eng MitarbeiterInnen im Außendienst datenmäßig bereits mit der Zentrale verbunden sind. Interessant auch, dass fast 41% eine Firmentankkarte haben.

- **Welches dieser Werkzeuge ist für Sie persönlich am wichtigsten?**

Für 52% ist das Mobiltelefon das wichtigste Instrument (auch als Smartphone, Blackberrry, iPhone etc. genannt), für 42% ist es der Laptop. Einem kleinen Teil waren beide Werkzeuge gleich wichtig. Internet und Intranet wurden zu 14% genannt, oft in Kombination mit einer „Hardware" wie Laptop, Tablet oder Smartphone.

- **Bitte nennen Sie drei Vorteile, die dieses wichtigste Werkzeug für Sie hat!**

Diese offene Frage wurde sehr ausführlich beantwortet. Es zeigen sich viele Vorteile der Vereinfachung (alles in einem Gerät), Flexibilität (Arbeit an unterschiedlichen Orten und zu selbst gewählten Zeiten, Möglichkeit der Arbeit zu Hause, Dienstpläne), der Datengenauigkeit und Fehlerarmut (Austausch mit Daten aus dem Zentralrechner, Kunden-, Termindaten, Rückfragen), der Schnelligkeit (rasche Verarbeitung der Daten, Rückkopplung, Rechnung), der Sicherheit und Logistik (bargeldloses Inkasso, Materialnachlieferung), erhöhte Kompetenz den Kunden gegenüber (Informationen, Präsentationen, Kalkulationen online), aber auch der Abgrenzung und autonomen Arbeitsgestaltung (An-/Abschalten wann ich will, aber auch Erreichbarkeit, wenn ich will) und teilweise auch der Zusatznutzen erlaubter privater Verwendung.

- **Welche Nachteile hat dieses wichtigste Werkzeug ihrer Meinung nach?**

Die Liste der genannten Nachteile ist etwas kürzer (16% haben überhaupt keinen Nachteil angegeben), aber bei den Nennungen ebenso genau und detailliert. Viele unterschiedliche Aspekte werden angeschnitten, die auf Diskussions- und Handlungsbedarf gewerkschaftlicher und betriebsrätlicher Arbeit verweisen.

Technische und ergonomische Probleme: kleiner Bildschirm, kleine Tastatur (Handy), zu langsam, zu groß, schwache Akkus, Gewicht, Attachments nicht lesbar.

Technische Einschränkungen: verfügbare Netze, Verbindungsprobleme, limitierter Internetzugang, schwache Software, veraltete Geräte, WLAN-Abhängigkeit.

Gesundheitliche Risiken: schlecht für die Augen, schlechte Sitzpositionen, Strahlenbelastung beim Handy, Kopfschmerzen, Stressfaktor: man macht keine Pausen mehr, Verspannungen.

Verlust-, Pannen- und Sicherheitsrisiken: Datenfehler, Datenausfall, Leitungsunterbrechung, Intransparenz der EDV, Abhängigkeit von einem Gerät, bei Verlust des Geräts „verschwindet" das Wissen, Ablenkung vom Fahren auch bei Freisprecheinrichtung, mangelnder Datenschutz, Virenbefall.

Organisatorische Probleme: für gemeinsame/arbeitsteilige Tätigkeit mehrerer MitarbeiterInnen nicht geeignet, kurzfristige Dienst(zeit)änderungen, eMail-Flut zu groß, Innendienst delegiert Arbeiten nach außen, durch technische Vorgaben kaum individuelle Lösungen möglich, Einzelkämpfertum wird gefördert.

Kontrolle durch Arbeitgeber: Standort-peilung, minutengenaue Kontrolle der Kundengespräche, Unsicherheit, „welche Kontrollsoftware da eingebaut ist", Kostencheck, Vorratsdatenspeicherung, Kon-trolle, wer mit wem wo wie lange telefoniert hat, Leistungs- und Verhaltenskontrolle, Kontrolle stellt Vertrauen in Frage, gläserne MitarbeiterInnen.

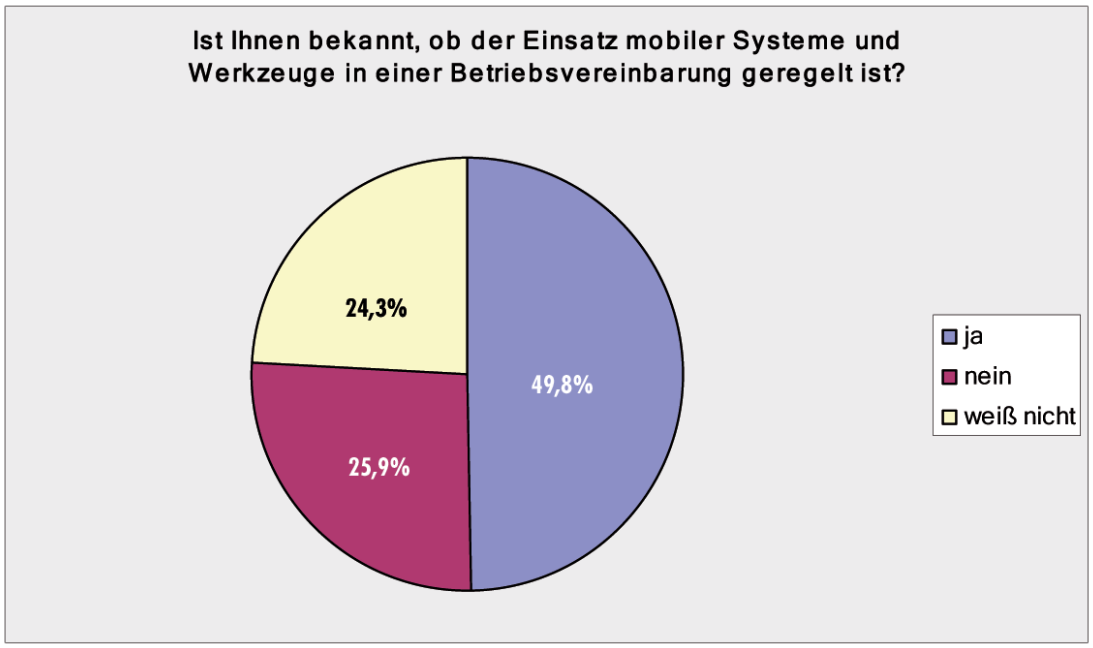
Abgrenzung zwischen Arbeit und Freizeit schwierig: Jederzeitige Erreichbarkeit, auch im Urlaub oder Krankenstand, Freizeit sowieso, Arbeitszeitüberschreitungen, ver-ringerte Privatsphäre.

Abgrenzung zwischen Kundengespräch und technischer Erreichbarkeit: Entpersönlichung des Kundenkontakts (kühlt ab), Störung des Kundengesprächs durch Anrufe, zu schnelle Kommunikation.

Der „innere" Druck: immer nachschauen…, Datenkontrolle, Gefahr, immer verfügbar zu sein, schnell reagieren zu müssen, Verleitung, Arbeit mit nach Hause zu nehmen, eigene Neugier, immer aktuell informiert zu sein…, Reduktion der Denk- und Ruhepausen, fehlende Selbstbeherrschung.

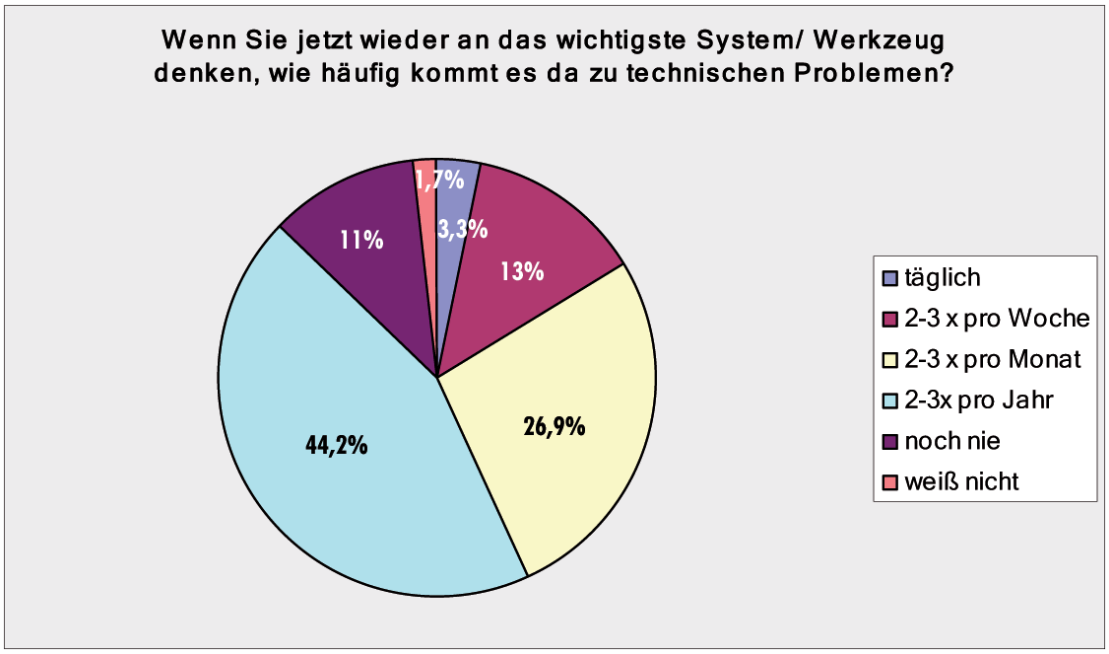
Gesteigerte Erwartung von Kunden, Vorgesetzten, KollegInnen: Lenkzeit wird durch Freisprecheinrichtung zur Arbeitszeit, Erwartung rascher Reaktion auf Mail bzw. Rückruf, Erwartung immer und überall erreichbar zu sein.

- **Ist Ihnen bekannt, ob der Einsatz mobiler Systeme und Werkzeuge in einer Betriebsvereinbarung geregelt ist?**



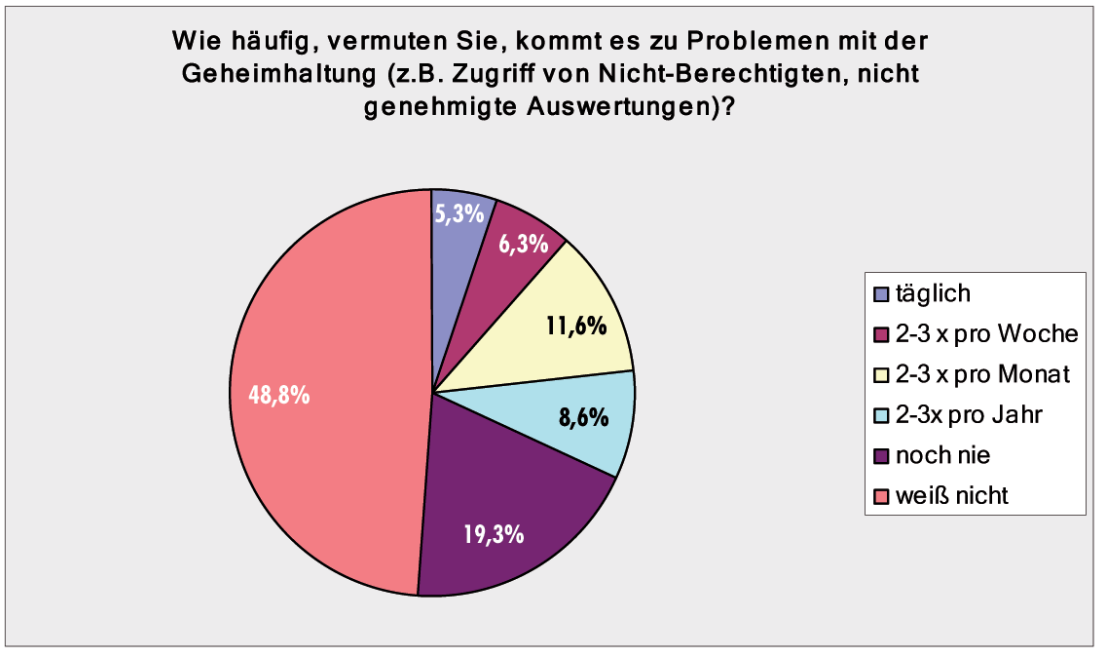
Dass immerhin die Hälfte der Befragten diese Frage positiv beantwortete, verweist sowohl auf die verantwortliche Haltung vieler Betriebsräte als auch darauf, dass inzwischen auch viele Firmenleitungen mit diesen Fragen sorgfältig umgehen.

- **Wenn Sie jetzt wieder an das wichtigste System/Werkzeug denken, wie häufig kommt es da zu technischen Problemen?**



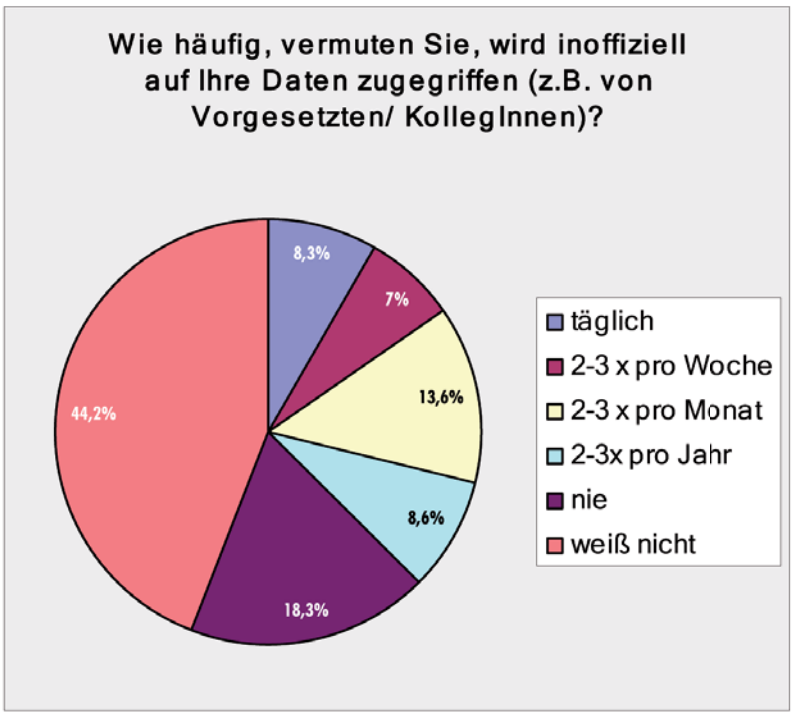
Die Häufigkeit bzw. sogar Regelmäßigkeit auftretender technischer Probleme mit der mobilen Technik ist erschreckend hoch. Nur bei 11% ist es noch nie zu Problemen gekommen.

- **Wie häufig, vermuten Sie, kommt es zu Problemen mit der Geheimhaltung (zB Zugriff von Nicht-Berechtigten, nicht genehmigte Auswertungen)?**



Hier ist die Dunkelziffer sehr hoch. Aber bedenklich genug scheint, dass bei mehr als einem Drittel angegeben wird, es komme täglich oder mehrmals wöchentlich zu nicht erlaubten Datenzugriffen oder Auswertungen und somit zu einer Verletzung des Datenschutzes.

- **Wie häufig, vermuten Sie, wird inoffiziell auf Ihre Daten zugegriffen (zB von Vorgesetzten/ KollegInnen)?**



Die Vermutungen von missbräuchlichem Datenzugriff durch Vorgesetzte oder KollegInnen liegen sogar noch höher; nur von 18% der Befragten wird diesem Personenkreis eine „saubere Weste" attestiert. 15% traut Vorgesetzten oder KollegInnen täglichen bzw. mehrfach wöchentlichen Missbrauch zu.

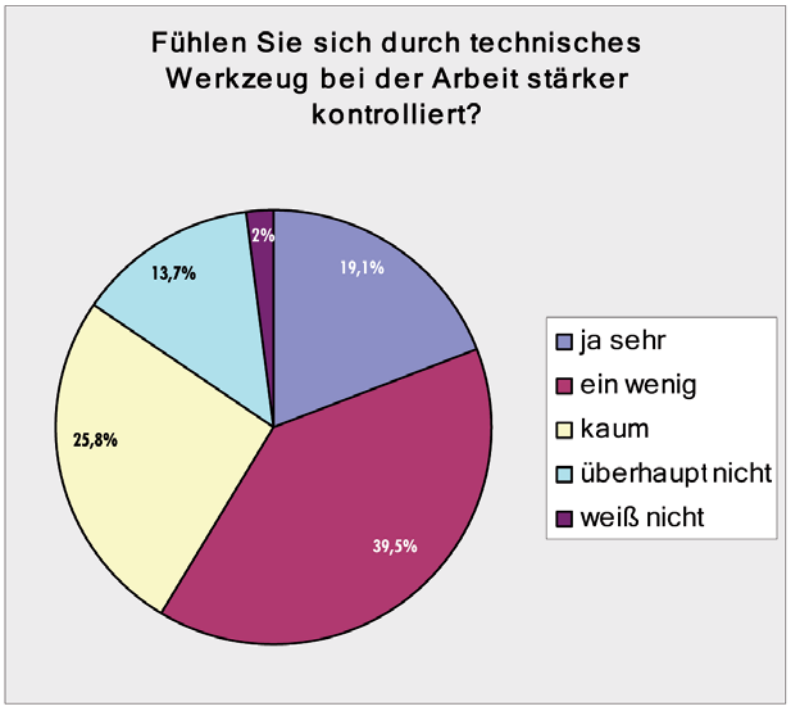
- **Fühlen Sie sich durch technisches Werkzeug in ihrer Freiheit, Ihre Arbeit zu gestalten, eingeschränkt?**
  Hier werden dem Gerät selbst nur geringe Beeinträchtigungen zugeschrieben: Weniger als 8% fühlen sich „sehr eingeschränkt", etwa 30% „ein wenig", jedoch 62% „kaum" oder „überhaupt nicht".

- **Gibt es in Ihrem Betrieb einen innerbetrieblichen Datenschutzbeauftragten?**
  Ein Drittel der Befragten hat einen innerbetrieblichen Datenschutzbeauftragten.

- **Mit wem können Sie auftretende Probleme besprechen?**
  Zwei Drittel ziehen dabei KollegInnen, Betriebsräte oder SystemadministratorInnen zu Rate, knapp die Hälfte Vorgesetzte.

- **Wer hat sich des Problems angenommen?**
  Mit 61% sind SystemadministratorInnen die Problemlöser Nummer eins. Mit 39% bzw. 33% folgen Betriebsräte und KollegInnen.

- **Fühlen Sie sich durch technisches Werkzeug bei der Arbeit stärker kontrolliert?**



19% der Befragten fühlen sich „sehr", 39% immerhin „ein wenig" durch technisches Werkzeug kontrolliert. Ebenso viele sagen dazu „kaum" oder „überhaupt nicht". Bei diesem subjektiven Empfinden geben nur 2% keine klare Antwort.

- **Könnten Sie bitte einen Fall näher beschreiben, bei dem es zu Problemen mit den aufgezeichneten Daten gekommen ist?**

  Einige Beispiele aus den Antworten:
  „GPS - Datenauswertungen in Dienstwagen werden zur Stundenüberprüfung herangezogen und KollegInnen müssen sich rechtfertigen. Druck besteht schon, da Bewusstsein es könnte aufgezeigt werden."

  „Ja, interne Informationen über eMailverkehr auf kleinem Verteiler gelangte zu weiteren Personen."

  „Es gab bereits illegale Auswertungen eines Vorgesetzten bei der Leistungsdatenerfassung. Nicht zulässige Leistungs-/Verhaltenskontrollen."

  „Mobilnetzgespräche und Daten wurden ausgewertet und damit unterstellt, dass man die Betriebsmittel zu sehr privat verwendet!"

  „eMailversand wurde kontrolliert und mir Sanktionen angedroht."

  „Anrufprotokoll, wie schnell wir im Außendienst vom Handy abheben"

  „Wir erfahren irgendwie, wer wann online ist bzw. welche Programme wann gestartet sind. Dabei muss auffallen, dass wir sehr oft an Wochenenden bzw. in der Nacht arbeiten. In unseren Tätigkeitsberichten dürfen wir diese Arbeitszeiten nicht eintragen, weil dann arbeitsrechtliche Bestimmungen missachtet werden. Besteht die Welt aus Lug und Trug?"

  „Anhand des Speicherdatums verschiedener Files wurde die Arbeitszeit nachvollzogen."

  „Chef hat Daten eingesehen."

- **Wie wichtig ist Ihnen persönlich der ArbeitnehmerInnen-Datenschutz (nach dem Schulnotensystem)?**
  Hier ist die Antwort eindeutig und unmissverständlich: 94% sagen "sehr wichtig" oder „wichtig"!

- **In welchem Bereich finden Sie ihn besonders wichtig?**
  Als häufigste Präzisierung wird hier genannt: alle Bereiche. Bei näherer Differenzierung werden die sensiblen Bereiche „persönliche Daten", „Gesundheitsdaten", „Arbeitszeitdaten", Ortungsdaten (GPS), kurz alle „die Persönlichkeitssphäre betreffenden Daten" hervorgehoben. Vom technischen Standpunkt aus werden besonders e-Mails und Telefondaten genannt. Explizit als „vertraulich" oder „privat" gekennzeichnete Daten sollten besonderen Schutz genießen.

Rechtliche Grundprinzipien des betrieblichen Datenschutzes

Generell gilt, dass jeder Mensch ein Recht auf die Achtung seiner Privatsphäre hat und auf den Schutz seiner/ihrer personenbezogenen Daten. In diese oberste Priorität kann unter bestimmten Umständen eingegriffen werden werden. Diese Umstände regelt das Datenschutzgesetz 2000 (DSG). Aus dem Text des DSG ergeben sich Grundsätze, die für jede Art der Datenverwendung[1] gültig sind. Die einzelnen Bestimmungen im Gesetzestext werden für die praktische Auslegung zusammengefasst und in folgende Grundprinzipien „übersetzt":

1. Grundsatz der Zweckmäßigkeit

Der Zweck jeder Datenverwendung muss genau festgelegt werden. Die Verarbeitung personenbezogener Daten muss mit dem vorher definierten Zweck der Datenermittlung übereinstimmen. Datensammlungen ohne genaue Angaben darüber, um welche Daten es sich handelt und warum sie gebraucht werden, für zukünftige oder nur ganz allgemein begründete Pläne, stehen im krassen Widerspruch zur Zweckbindung.

Zitat aus dem Gesetzestext: Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden (§6 Abs 1 Z 2). Daten dürfen nur verwendet werden, sofern sie für den Zweck der Datenanwendung wesentlich sind, und über diesen Zweck nicht hinausgehen (§6 Abs 1 Z 3).

2. Grundsatz der Datensparsamkeit

Mehrere Formulierungen weisen darauf hin, dass Datenverarbeitungen möglichst eingeschränkt, möglichst sparsam sein müssen. „Sachlich richtig" meint beispielsweise, dass nicht irgendwelche Begründungen für Datensammlungen vorgegeben werden dürfen. „Auf dem neuesten Stand" weist darauf hin, dass Daten aktuell sein müssen. Auch die Vorschrift zur Aufbewahrungsdauer zeigt, dass Daten immer eingeschränkt zur Verfügung stehen sollen – sie dürfen nur so lange gespeichert werden, so lange es dafür einen guten Grund gibt. Man kann sich daran orientieren, dass bei der Verwendung personenbezogener Daten immer ein „Minimalprinzip" eingehalten werden muss, dh es muss geklärt werden, ob die Vorgehensweise tatsächlich das am wenigsten in die Privatsphäre der Betroffenen[2] eingreifende Verfahren ist, um das gewünschte Ziel zu erreichen. Der Eingriff in die Privatsphäre muss auf ein Minimum beschränkt sein.

Kurz gesagt: Daten müssen sparsam verwendet werden. Dieses Prinzip der Datensparsamkeit soll den Umfang der erfassten Daten auf ein sinnvolles Maß beschränken und Datenermittlungen auf Verdacht, im vorauseilenden Gehorsam oder unendlich lange Aufbewahrungszeiten verhindern.

Zitate aus dem Gesetzestext: Der Eingriff in das Grundrecht [auf Datenschutz darf] jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen werden (§1 Abs 2). Daten dürfen nur in der Art und Weise verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, falls notwendig, auf den neuesten Stand gebracht sind (§6 Abs 1 Z 4). Daten dürfen nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt

1 Wenn im Datenschutz von „Verwendung" die Rede ist, dann zählen dazu sämtlich Vorgänge, die mit personenbezogenen Daten erfolgen; also das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten von Daten (einzige Ausnahme: Übermitteln).

2 Wenn im Datenschutz von „Betroffenen" die Rede ist, sind damit immer diejenigen gemeint, deren personenbezogene Daten verwendet werden (also im Zusammenhang mit ArbeitnehmerInnen-Datenschutz der/die ArbeitnehmerIn).

wurden, erforderlich ist (§ 6 Abs 1 Z 5).

Die Zulässigkeit (…) setzt voraus, dass Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten Mitteln erfolgen (…) (§ 7 Abs. 3 DSG).

3. Grundsatz der Rechtmäßigkeit

Sämtliche Datenschutzbestimmungen und Gesetze sowie sittliche Grundsätze müssen befolgt werden. Der/die Betroffene darf über die Umstände des Datengebrauchs seiner/ihrer Daten nicht getäuscht werden.

Besteht eine gesetzliche Vorgabe, darf in die Privatsphäre eingegriffen werden. Wenn also die Pflicht des/der Arbeitgebers/in besteht, Sozialversicherungsbeiträge abzuführen, dann ist das kein Eingriff in die Privatsphäre. Gibt es aber keine gesetzliche Vorschrift, dass bestimmte Daten an bestimmte Behörden oder Organisationen (zB Fördergeber) weitergeleitet werden müssen, so braucht es eine vertragliche Verpflichtung für eine solche Datenverwendung. Um feststellen zu können, auf Basis welcher Verträge der Auftraggeber[3] handelt, müssen diese Verträge den Betroffenen zugänglich gemacht werden. BetriebsrätInnen könnten sich also die Verträge, die angeblich den Grund für Datenermittlungen beinhalten, zeigen lassen.

Es können also auch bestehende, rechtlich gültige Verträge dazu führen, dass Daten verwendet werden dürfen und das keinen Eingriff in die Privatsphäre darstellt. Allerdings immer nur unter den angeführten Grundprinzipien und unter Wahrung der Betroffenenrechte.

Das Argument, auf das sich ArbeitgeberInnen und ihre RechtsanwältInnen aber am häufigsten stützen, ist dass laut DSG auch sogenannte berechtigte Interessen dazu führen können, dass personenbezogene Daten einfach verwendet werden dürfen. Dazu muss aber der/die ArbeitgeberIn erst einmal glaubhaft machen können, dass überhaupt berechtigte Interessen bestehen. Sollte ein solcher Fall vor Gericht verhandelt werden (was bislang bei privatrechtlichen Arbeitsverhältnissen in Österreich noch nicht der Fall war) dann wird es zu entscheiden gelten, ob die Interessen der Betroffenen am Schutz ihrer Daten überwiegen oder die Interessen der ArbeitgeberInnen, diese Daten zu verwenden.

Zitate aus dem Gesetzestext: Daten dürfen nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden (§6 Abs 1 Z 1). Datenverwendungen sind gerechtfertigt, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht (§8 Abs 1 Z 1), überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten bestehen (§ 8 Abs 1 Z 4) oder in Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und einem Betroffenen geschehen (§8 Abs 3 Z 4 DSG).

4. Grundsatz der Transparenz:

Den Betroffenen stehen bestimmte Informationen zu – innerhalb einer Frist von acht Wochen ist eine (einmal jährlich kostenlose und ansonsten mit einem Pauschalbetrag von EUR 18,89 abzugeltende) Auskunft über die Verwendung ihrer personenbezogenen Daten zu erteilen.

Die Auskunft muss Folgendes abdecken:

- verarbeitete Daten

3 Wenn im Datenschutz vom „Auftraggeber" die Rede ist, ist damit immer derjenige gemeint, der die personenbezogene Daten verwenden möchte (also im Zusammenhang mit ArbeitnehmerInnen-Datenschutz der/die ArbeitgeberIn).

- deren Herkunft
- Zweck oder rechtliche Grundlage für die Verwendung
- allfällige Empfänger oder Empfängerkreise

Die Betroffenenrechte müssen vom Auftraggeber der Datenverarbeitung gewährleistet werden. Der/die ArbeitgeberIn hat also dafür zu sorgen, dass beispielsweise das Geburtsdatum oder das Entgelt der Beschäftigten korrekt ermittelt und gespeichert wird. Ist dies nicht der Fall, können die Betroffenen Richtigstellung oder Löschung beantragen.

Dieser Transparenzgrundsatz findet sich auch darin wieder, dass sämtliche Datenanwendungen in einem öffentlich zugänglichen Register gemeldet werden müssen (Ausnahme: Standard- und Musterverordnungen; zB die SA002 für die Personalverwaltung in privatrechtlichen Dienstverhältnissen). Dieses Datenverarbeitungsregister (DVR) kann von jedermann eingesehen werden und gibt Auskunft darüber, welche Datenarten und welche Systeme verwendet werden, nicht jedoch über die einzelnen personenbezogenen Daten selbst. (Diese Vorgehensweise im Sinne der Transparenz wird mitunter auch unter dem Stichwort „Publizitätsprinzip" abgehandelt.)

Zitat aus dem Gesetzestext: Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten. (§1 Abs 3 DSG)

Der internationale Datentransfer

Jedes EU-Land hat eine eigene Regelung zum ArbeitnehmerInnen-Datenschutz. Manche haben dazu ein eigenes Gesetz (Finnland), manche haben verpflichtende innerbetriebliche Datenschutzbeauftragte (Deutschland), manche haben zu bestimmten Datenverwendungen im Arbeitsleben eine gesetzliche Vorgabe (Italien zur Videoüberwachung) – die Bandbreite ist groß. Dadurch, dass im europäischen Datenschutz nationale rechtliche Grundlagen eine Rechtfertigung für den Eingriff in die Privatsphäre darstellen, ist es sehr unterschiedlich, was in den einzelnen Staaten erlaubt ist und was nicht. Jede Verordnung kann nämlich eine rechtmäßige Grundlage für die Verwendung personenbezogener Daten sein. Nicht zu vergessen, dass die Arbeitsbeziehungen zwischen ArbeitgeberInnen und ArbeitnehmerInnen EU-weit sehr unterschiedlich geregelt sind.

Dieser „Rechts-Dschungel" führt dazu, dass es sehr stark vom konkreten Einzelfall abhängt, davon welche Gesetze außer dem DSG noch einzuhalten sind, welche rechtlichen Vorgaben zusätzlich gelten, welche berechtigten Interessen mitspielen, welche rechtlich bindenden Verträge vorliegen, etc. in welcher Form der ArbeitnehmerInnen-Datenschutz gestaltet wird. Über das Arbeitsverfassungsgesetz (§§96, 96a und 97) kann sich ein österreichischer Betriebsrat fast immer in datenschutzrelevante betriebliche Regelungen verpflichtend einbringen.

Das österreichische Datenschutzgesetz beruht – wie die Datenschutzregelungen aller anderen EU-Staaten – auf einer EU-Richtlinie aus dem Jahre 1995. Diese Richtlinie enthält Vorgaben, die in jedem Mitgliedsland in nationalstaatliches Recht umgesetzt werden mussten. Es sind also die oben beschriebenen Prinzipien in jedem EU-Land vorhanden und die EU geht davon aus, dass EU-weit ein (zumindest einigermaßen) einheitliches Datenschutz-Niveau herrscht. Deshalb gibt es für Datentransfer innerhalb der EU keine weiteren gesetzlichen Beschränkungen aus dem DSG[4] – vorausgesetzt dass die Grundprinzipien eingehalten werden.

Nun schreibt das DSG aber vor, dass in bestimmten Fällen, Datenverwendungen genehmigt werden müssen:

- Verwendung sensibler Daten
- Verwendung strafrechtlich relevanter Daten
- Überlassen oder Übermitteln an Dritt-Staaten (also Nicht-EU-Staaten)
- Informationsverbundsystem (wenn mehrere rechtlich eigenständige Auftraggeber Daten gemeinsam ermitteln und auch gemeinsam verwenden, also wenn zB alle rechtlich eigenständigen Unternehmensteile eine gemeinsame Projektdatenbank befüllen und auch einsehen und bearbeiten können.)

Ist also eines dieser Dinge der Fall, muss die Datenverwendung von der nationalen Datenschutzbehörde, der Österreichischen Datenschutzkommission (DSK), geprüft und genehmigt werden. Im transnationalen Datenverkehr hat man es folglich relativ schnell mit diesen Voraussetzungen zu tun und es muss die DSK eingeschalten werden.

Nun gibt es in Österreich ergänzend zum DSG das Arbeitsverfassungsgesetz (ArbVG) und das sieht vor, dass Systeme, in denen personenbezogene Daten automatisiert verarbeitet werden, in Betriebsvereinbarungen geregelt werden müssen. Folglich kann sich der Betriebsrat (BR) einmischen, welche Daten hier tatsächlich gemäß den Datenschutz-Prinzipien übermittelt werden dürfen. Erfahrungsgemäß bestehen Auffassungsunterschiede darüber, was eine Konzernleitung für zweckmäßig hält und was BetriebsrätInnen und Belegschaft für zweckmäßig halten, was laut Konzernleitung das gelindeste Mittel ist und was nach Ansicht des Betriebsrates/der Betriebsrätin noch sparsamer wäre.

Eine besondere Bevorzugung von Konzernen kennt das DSG – noch – nicht. Die meisten Konzerne betreiben de facto Informationsverbundsysteme (zB bei Karriere-Datenbanken), deklarieren diese jedoch nicht und lassen sie folglich auch nicht genehmigen. Mit der geplanten Änderung zum Datenschutz im EU-Recht soll sich auch in diesem Bereich einiges ändern.

Geplante Änderungen der EU-Kommission

Im Jänner 2012 hat die EU-Kommission eine Neufassung der Datenschutz-Regelung vorgelegt. Die derzeit geltende Richtlinie stammt aus dem Jahr 1995 und ist folglich dringend auf einen aktuelleren Stand zu bringen. Eine neue Verordnung soll den Datenschutz innerhalb der EU einheitlich regeln. Darin geht es darum, wie die Binnenmarktfreiheit im Datentransfer und die Bürgerlichen Freiheiten, sprich der Schutz der Persönlichkeitsrechte, zu denen ja auch die Privatsphäre zählt, zu gestalten sind. Schon allein aus dieser Vorgabe, dass der

4 Einigen Ländern bestätigt die EU ein Datenschutzniveau, dass dem der EU gleichwertig ist und in diese Länder können daher ebenfalls – unter Beachtung der Grundprinzipien – Daten transferiert werden; derzeit sind das innerhalb von Europa Andorra und die Schweiz sowie die Inseln Guernsey, Jersey, Isle of Men und Färöer sowie die Länder Argentinien, Israel und für privatwirtschaftliche Unternehmen größtenteils auch Kanada; in den USA sind Firmen, die sich dem „Safe-Harbor-Regime" unterwerfen gleich gestellt. Transfers in alle anderen Nicht-EU-Länder müssen folglich genehmigt werden (Ausnahme: sogenannte „Standardvertragsklausen" werden verwendet).
Wenn im Datenschutz von „sensiblen Daten" die Rede ist, dann sind folgende personenbezogenen Daten gemeint: rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben – und sonst nichts.

freie Datentransfer mit den bürgerlichen Freiheiten gleichgesetzt wird, lässt sich ablesen, dass nicht mehr die individuellen Bürgerrechte und der Schutz der Privatsphäre im Vordergrund stehen sollen, sondern die wirtschaftlichen Interessen des freien Datenverkehrs.

Der Entwurf enthält jede Menge unausgegorene Bestimmungen – die sollen dann in weiterer Folge von der EU-Kommission konkretisiert werden. Dieser „Freibrief" betrifft unter anderem auch die nähere Ausgestaltung des betrieblichen Datenschutzbeauftragten (zB zu Ressourcen, Kriterien, Anforderungen, Zertifizierungen...). Damit würden sich Nationalstaaten und ihre Datenschutz-Behörden weitere Befugnisse aus der Hand nehmen lassen und die Kommission, ein bekannter Weise nicht demokratisch bestelltes Gremium, würde weitere Entscheidungs- und Gestaltungsbefugnisse bei sich konzentrieren.

Weiters wird es – geht es nach dem Willen der EU-Kommission – bei der Meldepflicht Verschlechterungen geben. Die Meldung soll nicht mehr an ein zentrales Register erfolgen, sondern es müssen nur mehr innerhalb des Betriebes Aufzeichnungen geführt werden.

In Betrieben mit 250 und mehr MitarbeiterInnen wird es eine/n Datenschutzbeauftragte/n geben, die/der die innerbetrieblichen Aufzeichnungen verwaltet. Betriebe mit weniger als 250 MitarbeiterInnen sind von dieser „Auflage" befreit.

Die Einführung eines verpflichtenden betrieblichen Datenschutzbeauftragten (DSB) ist prinzipiell zwar erfreulich, weniger erfreulich ist die konkrete Ausgestaltung dieser Funktion. Abgesehen davon, dass nur Großbetriebe diese Funktion einrichten müssten, soll sie auch nur in der „Hauptniederlassung" von Konzernen zwingend erforderlich sein. Wenn man also die österreichische Betriebslandschaft betrachtet, wäre das keine Funktion mit Breitenwirksamkeit. Man muss nämlich von den Großbetrieben mit mehr als 250 MitarbeiterInnen (das sind 2011 0,3% der Betriebe mit 39,8% der unselbständig Beschäftigten) noch diejenigen mit ausländischer Konzernzentrale abrechnen. Da bleiben nicht mehr viele Betriebe mit einer/einem verpflichtenden DSB übrig. Auch mangelt es der Funktion an näherer Definition. Es wäre unbedingt erforderlich, dass eine/ein betriebliche/r Datenschutzbeauftragte/r Weisungsfreiheit, Kündigungsschutz, vorgegebene Arbeitszeiten, eine adäquate standardisierte Ausbildung und eine passende Bezahlung erhält. Diesbezüglich müssten jedenfalls Mindeststandards im Rahmen der Verordnung vorgegeben werden.

Auf der Haben-Seite kann die ArbeitnehmerInnen-Interessenvertretung verbuchen, dass die Möglichkeit geschaffen wurde, nun auch vor Gericht die Interessen der ArbeitnehmerInnen zu vertreten. Bisher war der Datenschutz ja ausschließlich Individualrecht, nun werden auch Interessenvertretungen die Einhaltung der Persönlichkeitsrechte einklagen können (JuristInnen sprechen hier von „Parteistellung").

Derzeit sind die Verhandlungen und Klärungen zum Entwurf der EU-Kommission sowohl in der Ratsarbeitsgruppe als auch in den EU-Parlamentsausschüssen im Gange. Im Herbst 2012 wird der Ausschuss für Recht und bürgerliche Freiheiten (LIBE), der Hauptberichterstatter zu dem Gesetzesvorhaben, ein internationales Hearing zu dem Thema veranstalten. Ebenfalls für Herbst geplant ist eine Resolution vom Europäischen Gewerkschaftsbund (EGB) die bemängeln wird, dass in dem Entwurf ArbeitnehmerInnen-Datenschutz zu kurz kommt. Die GPA-djp wird sich weiterhin im EU-Parlament in den für den Datenschutz zuständigen Ausschüssen (LIBE und EMPL) dafür einsetzen, dass diese Verordnung abgeändert wird.

Innerbetrieblicher Datenschutz

Immer mehr Unternehmen möchten ihre Datenbestände vereinheitlichen und ihre elektronische Administration „vereinfachen". Ob es die internen Abläufe in sogenannten „work-flow"-Systemen sind, ob es Datenbanken zur Personal-, Termin- oder Ressourcenplanung und -verwaltung sind oder ob es sich um die Zeiterfassung handelt, die personenbezogenen Daten der ArbeitnehmerInnen werden darin aufgezeichnet und nach den Maßgaben der Unternehmensleitung weiterverwendet.

In Teilgesellschaften von weltweit agierenden Konzernen ist diese Tendenz noch stärker zu beobachten, weil man zentralisierten Zugang zu den Daten der Tochtergesellschaften haben möchte. Konzernweite Lohnverrechnung in Indien, Personalbemessung zentralisiert in der holländischen Konzernzentrale, allgemeines Kundenservice im us-amerikanischen Schwester-Konzern, und Ähnliches sind längst Realität. Unterstützt durch Informations- und Kommunikationstechnologien (IKT) sind der Verarbeitung von MitarbeiterInnen-Daten kaum Grenzen gesetzt. Da kann es schon mal vorkommen, dass der eine oder andere Datensatz irrtümlich oder absichtlich nicht dazu verwendet wird, wozu er ursprünglich vorgesehen war – Missbräuche passieren.

Datenschutzgesetz (DSG) und Arbeitsverfassungsgesetz (ArbVG) sind die wichtigsten gesetzlichen Grundlagen, um dem unnötigen und unkontrollierten Verarbeiten von MitarbeiterInnen-Daten etwas entgegenzusetzen. Der Gesetzgeber hat hier versucht, dem (weltweiten) Datentransfer Grenzen zu setzten.

Aus der Beratungspraxis wissen wir allerdings, dass Daten oft nicht dafür verwendet werden, wofür sie erhoben werden. Aus vorhandenen Daten werden falsche Schlüsse gezogen. Daten werden oft zwecklos gespeichert und verknüpft – einfach weil es technisch möglich ist. Ein elektronisches Gedächtnis vergisst aber nichts! Für die Löschung müssen Menschen sorgen. Daher ist es wichtig, innerbetriebliche Maßnahmen zu setzen, die die Datenerhebung, Datenweitergabe und Datenverarbeitung regeln.

Welche Daten darf der Arbeitgeber rechtmäßig verwenden?
Der Bundeskanzler hat in einer so genannten Standardverordnung (BGBl. II Nr. 201/2000 und Novelle BGBl. II Nr. 232/2003) genau festgelegt, welche personenbezogenen Daten vom Arbeitgeber festgehalten werden dürfen und an wen diese Daten weitergeleitet werden dürfen. Zum Beispiel dürfen die Arbeitszeitdaten nur an das Arbeitsinspektorat, Betriebsrat (BR), Sicherheitsvertrauenspersonen, Rechtsvertreter oder Gerichte weitergegeben werden. Die Höhe des Gewerkschaftsbeitrages darf – nach Bekanntgabe durch die Betroffenen – nur der zuständigen Bank, der angegebenen Gewerkschaft, Rechtsvertretern und Gerichten zugänglich sein. Das Geburtsdatum geht wiederum die Bank nichts an. Die Liste in der Standardanwendung zur Personalverwaltung für privatrechtliche Dienstverhältnisse (SA 002) ist sehr ausführlich und umfasst alle gängigen Daten für die Personalverwaltung. Üblicherweise kommt ein Unternehmen damit locker aus.

Es empfiehlt sich, regelmäßig zu überprüfen, ob die Daten auch ausschließlich für den ihnen zugedachten Zweck – nämlich ausschließlich die Personalverwaltung – verwendet werden. Diese Zweckbindung ist nämlich oberstes Prinzip im Datenschutz. Kein Zweck – keine Datenverwendung.

Welche Datenverwendungen muss der Arbeitgeber melden?
Möchte der Arbeitgeber/die Arbeitgeberin über die SA 002 hinausgehende Daten im Betrieb verwenden (zB eine Qualifikationsdatenbank, eine projektorientierte Zeiterfassung,…), muss eine Meldung an die Daten-

schutzkommission (DSK) erfolgen. Dazu muss eindeutig beschrieben werden, welche personenbezogenen Daten zu welchem Zweck verwendet werden, wer Zugang zu den Daten haben soll und welche Sicherheitsmaßnahmen ergriffen wurden. Eine Verletzung der Meldepflicht kann mit einer Verwaltungsstrafe von bis zu EUR 25.000,-- geahndet werden. Ein solcher Fall ist allerdings in Österreich bislang nicht bekannt.

Welche Daten der MitarbeiterInnen müssen vor ihrer Verwendung genehmigt werden?
Im Unterschied zur Meldepflicht, gibt es noch eine Genehmigungspflicht wenn besonders heikle personenbezogene Daten verarbeitet werden sollen. Das DSG schreibt vor, dass diese so genannten „sensiblen Daten" **vor ihrer Verwendung** durch den Auftraggeber, also im Arbeitsverhältnis den/die ArbeitgeberIn, explizit genehmigt werden müssen. Dieses Prozedere wird „Vorab-Genehmigungsverfahren" genannt.

Sensiblen Daten sind genau definiert. Sie umfassen Angaben über Religion, politische Überzeugung, „rassische" oder ethnische Zugehörigkeit, persönliche Sexualität und Gesundheitsdaten. Auch Daten über die Kreditwürdigkeit einer Person und Daten aus dem Strafregister definiert der Gesetzgeber als „besonders schützenswürdig" und somit genehmigungspflichtig bei der Datenschutzkommission.[5]

Außerdem müssen so genannte **„Informationsverbundsysteme"** genehmigt werden. Dabei handelt es sich um Datenverwendungen, die von mehreren Unternehmen beliefert und genutzt werden (zB verknüpfte Adress-Datenbanken, gemeinsames Datawarehouse,…).

Auch jede Installation von **Videokameras** muss der Datenschutzkommission gemeldet werden. Es sei denn, im Unternehmen werden ausschließlich analoge Kameras verwendet oder es wird nur verschlüsselt aufgezeichnet, wobei die Entschlüsselung nur unter der Genehmigung der Datenschutzkommission erfolgen darf[6].

Bei all diesen Datenverwendungen muss exakt angegeben werden welche Daten, zu welchem Zweck, mit welchen Empfängerkreisen, also Zugriffsberechtigungen gespeichert werden. Bei Übermittlung oder Überlassung an Dritte außerhalb des EU-Raumes (sogenannte Drittstaaten) muss ebenso Zweck, Dauer, Empfängerkreis angegeben und eigens von der Datenschutzkommission genehmigt werden.

Was kann der Betriebsrat / die Betriebsrätin tun?
Die §§ 96 und 96a Arbeitsverfassungsgesetz (ArbVG) sind für den innerbetrieblichen Datenschutz wichtig. Insbesondere die Ziffern zu:

- **Kontrollsystemen**, sofern sie die **Menschenwürde** berühren (zB sind nach einem Urteil des Obersten Gerichtshofs (OGH) biometrische Zeiterfassungssysteme mittels Fingerprint; wenn das **subjektive Empfinden** einer umfassenden Kontrolle durch den Arbeitgeber vorhanden ist.),

- **Personalfragebögen**, die über die Erfassung von Stammdaten, Qualifikation und Verwendungsgruppe hinaus gehen (zB einer regelmäßigen Abfrage zur Zufriedenheit mit der Arbeitssituation),

5 Da die Europäische Richtlinie zum Datenschutz in jedem Land unterschiedlich umgesetzt wurde, ist auch die Definition von sensiblen Daten verschieden. In Italien zum Beispiel zählen biometrische Daten auch zu dieser Kategorie. Diese Vielfalt erschwert den internationalen Datenverkehr, was ein Grund für die EU-Kommission war, an eine neue Verordnung zum Datenschutz auszuarbeiten. Derzeit wird über diesen (den ArbeitnehmerInnen-Datenschutz leider kaum berücksichtigenden) Entwurf im EU-Parlament und seinen Ausschüssen beraten.

6 Da dieses Verfahren aufwendig ist (es muss der Schlüssel hinterlegt werden), wird es laut Auskunft der Datenschutzkommission aber bislang nicht verwendet.

- **Personalbeurteilung** soweit sie durch die betriebliche Verwendung nicht gerechtfertig ist (zB Beurteilung von Teamfähigkeit, Flexibilität, etc. im MitarbeiterInnengespräch),

- **Systeme** zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der ArbeitnehmerInnen (zB **Personalverwaltungsprogramme**).

Anders als oft angenommen, kann die Zustimmung des Betriebsrates/ der Betriebsrätin nicht durch eine individuelle Zustimmung einzelner ArbeitnehmerInnen ersetzt werden. Bei all diesen zustimmungspflichtigen Punkten muss sich der Betriebsrat / die Betriebsrätin dafür einsetzen, dass diese Rechte nicht umgangen oder missachtet werden. Das Verhandeln von Betriebsvereinbarungen zu den angegebenen Themen ist meist ein längerer Prozess bei dem die Abteilung Arbeit und Technik gerne zur Seite steht. Oft müssen die relevanten Informationen erst zusammengetragen werden. Sind im Betrieb neue Systeme in Zusammenhang mit Datenschutz geplant (zB Umstellung auf ein neues Zeiterfassungssystem, Datentransfers zur Konzernmutter, etc.), muss der Betriebsrat / die Betriebsrätin in Zusammenarbeit mit der Geschäftführung folgende **Fragen klären**, bevor er/sie die Zustimmung zur Verwendung personenbezogener Daten der ArbeitnehmerInnen gibt:

- Welche personenbezogenen Daten sollen übermittelt werden? (taxative Aufzählung der einzelnen Daten)

- Wofür sollen die Daten verwendet werden? (Verwendungszweck pro Datum)

- In welchem System sollen die Daten gespeichert und verarbeitet werden? (Bezeichnung des Systems inkl. Version, Handbuch, Systembeschreibung)

- Welche personenbezogenen Auswertungen sollten gemacht werden? (taxative Aufzählung der geplanten Auswertungen, Verwendungszweck pro Auswertung)

- Sollen die Daten mit anderen Daten verknüpft werden? Wenn ja, mit welchen und zu welchem Zweck? (Geplante Verknüpfungen, Schnittstellen mit anderen Anwendungen bzw. Systemen? Verwendungszweck)

- Sind Übermittlungen der Daten an Dritte geplant? Wenn ja, welche und zu welchem Zweck? (Empfänger innerhalb und außerhalb des Konzerns, Verwendungszweck)

- Wann sollen die Daten gelöscht werden? (Speicherdauer muss gemäß dem Prinzip der Aktualität und Datensparsamkeit festlegt werden)

- Wer hat Zugriff auf welche personenbezogenen Daten? (Aufzählung der zugriffsberechtigten Personen bzw. Funktionen, Berechtigungsplan)

- Wer hat Zugriff auf die Auswertungen? (zB im Manager-Desktop von SAP, Aufzählung der Personen bzw. Funktionen mit Zugriff auf welche Auswertungen, Berechtigungsplan)

- Wer ist für den Datenschutz verantwortlich? (zB DatenschutzbeauftragteR, SystemadministratorIn, innerbetriebliche Datenschutzgruppe; gibt es ein Datenschutzkonzept?)

- Wie kann der Betriebsrat / die Betriebsrätin die Verwendung der personenbezogenen MitarbeiterInnendaten kontrollieren? (Mitbestimmungs- und Kontrollrechte nach dem ArbVG)

- Wie können die MitarbeiterInnen die Verwendung der über ihre Person gespeicherten Daten kontrollieren? (Betroffenenrechte nach dem DSG)

- Wurde eine Meldung an die Datenschutzkommission gemacht?

- Wurde die Datenanwendung - so erforderlich - genehmigt?

- Was soll bei unterschiedlichen Interpretationen der Betriebsvereinbarung oder bei Verdacht auf missbräuchliche Verwendung der personenbezogenen Daten geschehen?

Welche Rechte haben die Betroffenen?
Diejenigen, deren Daten verarbeitet werden, haben **Recht** auf:

- **Berichtigung** falscher Daten,

- **Löschung** und/oder Sperrung falscher Daten bzw. widerrechtlich erfasster Daten,

- **Widerruf** einmal gegebener Zustimmungen zur Datenverwendung,

- Vertraulichkeit und **Sicherheit** bei jeder Datenanwendung,

- **Information** über Zweck und Gegenstand der Datenanwendung sowie Empfänger der Daten ohne **unzumutbare Verzögerung oder Kosten** (auch wenn ein Datenverarbeiter behauptet, keine personenbezogenen Daten von Betroffenen zu haben, sollte das den Betroffenen mitgeteilt werden). Die **Herkunft** der Daten muss aus der Information ebenfalls hervorgehen. Die Information soll auch den logischen Aufbau der Datenanwendung - so sie automatisiert erfolgt - enthalten. Ferner muss die Auskunft in **verständlicher** Form gegeben werden

  Im DSG sind leider nur Individualrechte festgehalten. Der Betriebsrat / die Betriebsrätin kann sich also vor Gericht nicht auf seine/ihre Vertretungsfunktion der ArbeitnehmerInnen berufen, wenn er/sie in Sachen Datenschutz aktiv werden möchte. Gemäß DSG ist derzeit keine Parteistellung für die betriebliche Interessenvertretung vorgesehen. Die Betroffenen müssen selbst um ihre Rechte kämpfen. BetriebsrätInnen können sich aber auf die oben beschriebenen Zustimmungspflichten nach dem ArbVG berufen und für eine gute, die Privatsphäre der ArbeitnehmerInnen schützende **Betriebsvereinbarung** sorgen. Der Betriebsrat / die Betriebsrätin kann außerdem Bewusstseinsarbeit leisten und das **gemeinschaftliche Vorgehen der Betroffenen** fördern.

In Betrieben ohne Betriebsrat, ist die Verwendung von sensiblen Daten dann zulässig, wenn die Betroffenen zugestimmt haben. Im DSG ist nicht genau festgelegt, ob eine solche Zustimmung schriftlich, mündlich oder durch konkludente Handlung gegeben werden kann. Alle drei Möglichkeiten stehen offen.

Festgelegt ist, dass die **persönliche Zustimmung**

- frei,
- ohne Zwang,
- in Kenntnis der Sachlage und
- für den konkreten Fall abgegeben wird (§4 Z 14 DSG).

Eine solche individuelle Zustimmung darf also nicht allumfassend (das wäre nicht konkret), für alle Zeiten gültig (das wäre nicht auf den Fall bezogen) und auch nicht in Zusammenhang mit zB einer Bewerbung erfolgen (das wäre nicht frei und in der Regel ist auch die Kenntnis der Sachlage dann nicht gegeben).

Datenschutzgesetz und Arbeitsverfassungsgesetz müssen beide eingehalten werden; sie ergänzen einander, können aber nicht eines das andere ersetzen. Manche Arbeitgeber versuchen, sich durch individuelle Zustimmung der einzelnen ArbeitnehmerInnen von den anderen gesetzlichen Erfordernissen „freizukaufen", indem sie beispielsweise auf die Zustimmung des Betriebsrates/ der Betriebsrätin bei Kontrollmaßnahmen „verzichten"! Eine persönliche Einwilligung setzt allerdings keinesfalls die datenschutzrechtlichen Grundprinzipien nach dem DSG außer Kraft und entbindet auch nicht von den Zustimmungspflichten im ArbVG. DSG und ArbVG bestehen nebeneinander.

Welches Service bietet die GPA-djp an?

- Blog zum Thema ArbeitnehmerInnen-Datenschutz: http://arbeitundtechnik.gpa-djp.at/

- Informations-Broschüren zum Datenschutz
  - „Datenschutz ohne Kontrolle ist wie Suppe essen mit der Gabel – Praxis-Tipps und Infos zum ArbeitnehmerInnen-Datenschutz"
  - „Fahren Sie nach Indien! Ihre Daten sind schon dort – Informationen und Handlungshilfen zum grenzüberschreitenden Datenverkehr"
  - „Datenschutzgesetz aus Sicht der ArbeitnehmerInnen"
  - „Der Rächer der enterbten Daten"

- Referate/Workshops/Seminare zu Grundsätzen des innerbetrieblichen Datenschutzes und Kontrollsystemen

- Muster-Betriebsvereinbarungen zu IKT und Kontrollsystemen (zB eMail, Internet, SAP,…)

- Beratung zur betriebsspezifischen Gestaltung von BVs und zum innerbetrieblichen Datenschutz

Faustregeln im Umgang mit MitarbeiterInnen-Daten

Die Sicherheit für die MitarbeiterInnen ist umso höher je

- weniger personenbezogene Daten verwendet werden,

- mehr die ArbeitgeberInnen bei der Verwendung der Daten auf einen gut argumentierbaren Zweck beschränkt sind,

- höher die Verantwortung für die Datenverarbeitenden (also den/die ArbeitgeberIn) ist.

Checkliste: Merkmale einer guten Vereinbarung zum Datenschutz

Mitunter verwenden Konzerne keine Betriebsvereinbarungen im Sinne des ArbVG, um den Transfer ihrer MitarbeiterInnen-Daten zu regeln. Privacy Statements, Codes of Conduct, Binding Corporate Rules, Verhaltenskodizes, etc. können ebenso Vereinbarungen zum Datentransfer beinhalten. Um sicher zu gehen, dass solche Vereinbarungen auch den Datenschutzprinzipien entsprechen und die Interessen der ArbeitnehmerInnen berücksichtigen hilft die folgende Checkliste.

1. **Beschränkung der Zweckbestimmung** – Die Daten dürfen nur für einen bestimmten Zweck verwendet werden. Dieser ist festgelegt und darüber hinaus ist jede Datenanwendung untersagt.

2. **Aktualität und Verhältnismäßigkeit** – Die Daten müssen aktuell sein und sie müssen zu dem Zweck für den sie bestimmt sind auch erfüllen können. Eine umfangreiche Übermittlung von Daten, die gar nichts mit dem angegebenen Zweck zu tun hat, ist nicht erlaubt.

3. **Weitergabe an Dritte beschränken** – Die Daten dürfen nicht an Dritte weitergegeben werden, außer diese sind mittels Vertrag eindeutig verpflichtet dasselbe Datenschutzniveau zu bieten, wie der ursprüngliche Auftraggeber.

4. **Speicherzeit** – Es muss festgelegt werden, wie lange welche Daten gespeichert werden sollen. Das gilt insbesondere für Verträge mit Dritten oder Dienstleistern zur Datenverarbeitung.

5. **Transparenz** – Die betroffenen Personen haben das Recht, informiert zu werden, wer welche ihrer Daten zu welchem Zweck verwendet.

6. **Zugriff, Berichtigung, Widerspruch** – Die Betroffenen haben das Recht, auf Auskunft, auf das Löschen von widerrechtlich verarbeiteten Daten und im Falle des Falles die Richtigstellen von falschen oder unaktuellen Daten.

7. **Verständlichkeit** – die Vereinbarung muss so verfasst sein, dass sie allgemein verständlich ist.

8. **Sicherheit** – Technische und organisatorische Maßnahmen zur sicheren Aufbewahrung und Verwendung der personenbezogenen Daten müssen getroffen werden. Die Datenverarbeitenden dürfen nur auf Anweisung der Verantwortlichen die Daten verarbeiten.

9. **Unterstützung** – die Vereinbarung enthält Unterstützung und Hilfestellung für die Betroffenen, was u.a. mittels eines klaren Instanzenweges bei Missständen und Beschwerden gewährleistet werden kann. Die Institutionen (zB ein Schiedsgericht) müssen neutral sein (d.h. nicht abhängig von den handelnden Personen bzw. paritätisch besetzt), Kontrollbefugnisse haben und einfach zugänglich sein (dh. möglichst nicht auf Kosten derjenigen arbeiten, die eine Beschwerde einreichen).

10. **Befolgung** – Die Vereinbarung wird von den handelnden Personen eingehalten, was durch regelmäßige externe Überprüfung erfolgen kann (zB spezialisierte Audits, Zertifizierung, etc.) oder auch mittels klarer Sanktionsmechanismen gefördert werden kann (zB Entschädigung der Betroffenen bei nachgewiesenem

Missbrauch, wobei eine Schädigung nicht allein bei materiellem Schaden oder Verlust gegeben ist sondern auch psychische und moralische Schäden betrifft). Eine rein auf freiwilliger Basis eingeführte Vereinbarung hat aller Voraussicht nach wenig Aussicht auf Erfolg.

11. **Bewusstsein und Überprüfung** - Voraussetzung für eine hohe Befolgungsrate ist, dass die Betroffenen von der Vereinbarung wissen und sie auch inhaltlich kennen. Das kann z.B. über regelmäßige Schulungen, Wissensabfragen u.ä. gefördert werden.

12. Bei **sensiblen Daten** müssen die Betroffenen persönlich der Verwendung zustimmen.

13. Beim **Direktmarketing** muss der/die Betroffene jederzeit die Zustimmung widerrufen können.

Generell gilt die Regel:

- Je mehr der/die EmpfängerIn der Daten in deren Verwendung beschränkt ist, desto mehr Sicherheit haben die Betroffenen.

- Je höher die Verantwortung für alle Vorgänge im Zusammenhang mit dem Datentransfer für die AuftraggeberInnen ist, desto mehr Sicherheit haben die Betroffenen.

Hinweise zum Vorgehen bei Dateneinsicht und Schutz vor Datenmissbrauch

Schutz vor Daten-Missbrauch

In verschiedensten Systemen werden personenbezogene Daten von MitarbeiterInnen verarbeitet. Diese Vielfalt an Daten bringt es mit sich, dass eine Vielfalt an Auslegungsmöglichkeiten entsteht. Ein Missbrauchsverdacht steht schneller im Raum, als man denkt. Führungskräfte und auch MitarbeiterInnen widerstehen der Versuchung nicht immer, dass sie sich ihren Verdacht mit Hilfe der ihnen zu Verfügung stehenden Datenmengen bestätigen (seltener widerlegen) lassen – und das auf nicht ganz korrekte Weise.

Da wird Einsicht in Datenbestände genommen, die mit ihrem eigentlichen Arbeitsbereich nicht wirklich etwas zu tun haben. Um herauszufinden, ob jemand mit vielen Überstunden „unabkömmlich" ist oder einfach dem „Anwesenheits-Kult" frönt, könnte man doch schnell die Daten aus der Zeiterfassung mit den Internet-Aktivitäten abgleichen.

Um festzustellen, ob MitarbeiterInnen ihre Emails zeitgerecht erledigen, könnte man deren Accounts näher unter die Lupe nehmen – und dabei auf private Aktivitäten stoßen.

Damit solche „Verdachtsüberprüfungen" nicht zu umfassender Bespitzelung ausufern, muss hier mit den ArbeitgeberInnen eine zweckmäßige Vorgehensweise vereinbart werden.

Der Vorteil einer solchen fix vereinbarten Vorgehensweise liegt darin, dass alle MitarbeiterInnen und alle Vorgesetzten dann gleich behandelt werden und sich nicht dem Vorwurf der Ungerechtigkeit aussetzen müssen. Außerdem ist den Betroffenen somit im Vorhinein klar, welche Maßnahmen in welcher Abfolge getroffen werden und es kommt zu keinen „bösen Überraschungen".

Diese Abmachung darüber was im Falle des Falles zu geschehen hat, sollte möglichst vor einem konkreten Verdachtsfall geschlossen werden. In der Konfliktsituation selber, ist es erfahrungsgemäß nur mehr schwer möglich. Ideal ist es, einen eigenen Absatz in der jeweiligen Betriebsvereinbarung einzufügen.

Vorgehen bei Dateneinsicht

Personen, die des Missbrauchs verdächtigt werden, wird ihr „Vergehen" zunächst einmal erklärt. Dies ist erforderlich um (im technischen Bereich häufig auftretende) Missverständnisse aus dem Weg zu räumen. Den Betroffenen soll die Möglichkeit zur Bereinigung des Problems eingeräumt werden (zB den entsprechenden zu umfangreichen Ordner löschen) bzw. die Gelegenheit zum ausgesprochenen Verdacht Stellung zu nehmen (zB ein Virus wurde in Abwesenheit aus dem Internet eingeschleppt). Dieser erste Schritt nach einem auffälligen Datenverwendungsverhalten sollte ausschließlich zwischen SystemadministratorIn/ ControllerIn und dem/der Betroffenen erfolgen.

Ist dadurch das Problem bzw. das Fehlverhalten nicht zu beseitigen, wendet sich der/die SystemadministratorIn/ ControllerIn an den/die direkte/n Vorgesetzte/n, wobei eine engere Kontrolle des/der Betroffenen vereinbart wird. Ziel dieser Phase ist ein direktes Gespräch mit dem/der Vorgesetzten, zu dem auf Wunsch der/des Beschuldigten auch der/die BetriebsrätIn hinzugezogen werden kann.

Kann der Missbrauchsverdacht danach noch immer nicht entkräftet bzw. geklärt werden, ist die Stelle, die das Fehlverhalten vermutet (zB SystemadministratorIn, Personalabteilung,…) berechtigt, umgehend im Beisein des/der betroffenen MitarbeiterIn und des Betriebsrates, eine Dateneinsicht vorzunehmen. Dabei werden nun Accounts der/des Betroffenen offengelegt und ausgewertet, um die Missbrauchsvorfälle genau untersuchen zu können.

Bestätigt sich der Verdacht (zB Download von umfangreichen Filmen für den Privatgebrauch) wird es Disziplinarmaßnahmen geben. Allfällige Sanktionen müssen die mit BetriebsrätInnen beraten werden und in Zusammenhang mit dem Missbrauch stehen (zB Sperre des Internets).

Die Überprüfung und Einsichtnahme in Protokolle und Daten sollte auch auf Antrag des Betriebsrates ermöglicht werden, um das Verhalten von Vorgesetzten in den Datenanwendungen überprüfen zu können. Auch Vorgesetzte, die unrechtmäßige Arbeitsaufträge erteilen, machen sich der missbräuchlichen Datenverwendung schuldig.

Jede Einsichtsnahme muss schriftlich festgehalten werden. Sowohl der Grund des Einsicht als auch Anwesende, Zeitraum, betroffene Systeme und Datensätze sowie die vorgenommenen Tätigkeiten (zB löschen eines Ordners, Auswertung einer Arbeitszeiterfassung) sind zu protokollieren.

Das dient dazu, die Einsichtnahme nachvollziehbar machen zu können (zB bei Abwesenheit der Beschuldigten), mutwillig konstruierte Beschuldigungen feststellen zu können und auch der Beweissicherung. Dadurch dass ein Grund für den Verdacht angegeben wird, ist die Zweckbestimmung festgelegt und die Dateneinsicht darf sich dann auch nur auf diesen Zweck beziehen (zB wird jemand des Diebstahls bezichtigt, ist es nicht zweckmäßig, sich dessen Verkaufsergebnisse der letzten vier Jahre anzusehen). Für diese Protokolle sind – wie für alle anderen Datenverwendungen auch – Löschfristen zu vereinbaren.

Die Formulierung einer entsprechenden Betriebsvereinbarung könnte wie folgt lauten:

„Grundsätzlich wird die Protokollierung von Daten aus technischen Gründen maschinen- und damit auch personenbezogen vorgenommen. Der direkte Personenbezug wird aber nur unter bestimmten Bedingungen einer bestimmten Personengruppe zugänglich gemacht.

Stufe 1: Die Kontrolle erfolgt allerdings im Sinne einer stufenweisen Kontrollverdichtung vorerst nur durch die IT-Abteilung und ohne konkreten Personenbezug. Der betroffene Personenkreis wird informiert und zur Verhaltensänderung aufgefordert.

Stufe 2: Im Fall des Weiterbestehens einer Gefahr für die betriebliche IKT-Infrastruktur ist die/der einzelne Betroffene zu informieren.

Stufe 3: Erst bei fortgesetzter pflichtwidriger und System gefährdender Nutzung kann die Offenlegung der personenbezogenen Daten gegenüber der vorgesetzten Person unter Hinzuziehen des Betriebsrates erfolgen.

Stufe 4: Der Dienstgeber wird bei einem konkret festgestellten Missbrauch die allfälligen disziplinarischen Maßnahmen mit dem Betriebsrat vereinbaren.

Anmerkung: Auch Vorgesetzte, die unrechtmäßige Arbeitsaufträge erteilen, machen sich der missbräuchlichen Datenverwendung schuldig.

Der Prozess der Einsichtnahme ist zu protokollieren, ebenso wie begründete Verdachtsmomente schriftlich festzuhalten sind. Wird jemand zu unrecht verdächtigt, sind die Protokolle sofort zu löschen, erhärten sich Verdachtsmomente, sind die Protokolle maximal drei Jahre aufzubewahren (lt. § 14 Abs 5 DSG).

Ausgenommen von den ersten beiden Stufen der Kontrollverdichtung sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit. Darüber hinaus für all diejenigen Fälle, in denen ein begründeter Verdacht eines Verstoßes gegen strafrechtliche Bestimmungen vorliegt, der durch rasches Eingreifen vermieden werden kann."

Ausführlich nachgelesen werden kann dieses Thema in einem rechtswissenschaftlichen Artikel, den zwei Mitglieder der Österreichischen Datenschutzkommission geschrieben haben. In dem Artikel wird ein Konzept für den innerbetrieblichen Umgang mit datenrechtlichem Fehlverhalten entwickelt: die stufenweise Kontrollverdichtung (Waltraud Kotschy und Sebastian Reimer (2004): „Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht" Zeitschrift für Arbeits- und Sozialrecht (ZAS) 2004/5, 167. Manz'sche Verlags- und Universitätsbuchhandlung. Wien).

Mustervereinbarung mobile Ortungssysteme

Vorbemerkung: Mustervereinbarungen und Leitfäden können Orientierung geben, sind jedoch nur dann nützlich, wenn sie auf die speziellen betrieblichen Umstände zugeschnitten sind. Wird ein Betriebsvereinbarungsmuster nicht „maßgeschneidert", gehen schnell wichtige Gestaltungsmöglichkeiten verloren. Aus diesem Grund sind die Regelungen der nachfolgenden Betriebsvereinbarung als Eckpunkte zu verstehen. Sie sollen als Anregungen dienen, um daraus eine zu den Verhältnissen im eigenen Betrieb möglichst optimal passende Vereinbarung zu entwickeln.

Die GPA-djp unterstützt und berät Sie gerne auf diesem Weg!

Hinweis: Die in der Muster-Betriebsvereinbarung grau hinterlegten Passagen sind als Kommentare zu verstehen und stellen keinen normativen Betriebsvereinbarungstext dar.

Betriebsvereinbarung für den Einsatz des Ortungssystems X

Technologien mit denen Ortung durchgeführt werden kann, sind zB Mobilfunknetze, GPS, WLAN oder RFID.

gemäß § 96 Abs 1 Z 3 ArbVG iVm § 96a ArbVG

zwischen der Geschäftsführung der Firma.....

und dem Betriebsrat der Firma....

Inhaltsverzeichnis:

1. Geltungsbereich
Diese Betriebsvereinbarung gilt: für alle ArbeitnehmerInnen sowie arbeitnehmerähnlichen Personen (zB auch für Leiharbeitskräfte, Lehrlinge, etc), die das System X zur Verfügung gestellt bekommen.

2. Rechtsgrundlagen
Die rechtliche Basis bilden insbesondere die Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG) im Besonderen die §§ 91, 92, 96/96a und 97 sowie die Bestimmungen des Datenschutzgesetzes 2000 (DSG 2000).

3. Zielsetzung
Die gegenständliche BV dient dem Schutz der Persönlichkeitsrechte der Betroffenen. Es kommt das System X mit folgenden Merkmalen technische Infrastruktur, Geräte, Software, Systemkomponenten zum Einsatz. Das System X wird nicht zum Leistungsvergleich und/oder zur Verhaltenskontrolle der MitarbeiterInnen herangezogen. Es wird übereinstimmend festgehalten, dass keine Bewegungsprofile erstellt werden.

Das System X dient einer administrativ effizienteren und transparenteren Ressourcenplanung. Die Einsätze können so rascher koordiniert und an den jeweiligen Standort sowie die Qualifikationen der ArbeitnehmerInnen angepasst werden.

ODER:

Der Einsatz von Software X hat zum Ziel, die Transparenz der betrieblichen Prozesse zu erhöhen, indem der Ort, der Beginn und die Fertigmeldung von Dienstleistungen sowie deren wesentliche Aspekte elektronisch erfasst werden.

4. Grundsatz
Die Daten werden ausschließlich während der Arbeitszeit ermittelt und ausschließlich für die hier vereinbarten Zwecke verwendet.

Der Einsatz des Systems X führt nicht zu Personaleinsparungen.

5. Systemanwendung
Eine permanente automatische Übertragung der Positionsdaten wird nicht durchgeführt. Die Weitergabe von Positionsdaten wird erst von dem/der MitarbeiterIn frei geschalten.

ODER:

Die Datenübertragung erfolgt automatisch im Stundenintervall.

Diese Information über die Häufigkeit der Datenübertragung ist insofern wichtig für die ArbeitnehmerInnen, als dadurch mehr Transparenz für sie gegeben ist. Permanente Übertragung und Speicherung der Positionsdaten an die Zentrale wäre (zumindest in den Branchen, wo es nicht um Leben und Tod geht) eine überschießende Maßnahme.

Der/Die MitarbeiterIn hat die Möglichkeit, die automatische oder von der Zentrale abgerufene Übertragung der Standortsignale zu unterbrechen.

Sollte ein/e MitarbeiterIn seitens der Zentrale gezielt geortet werden, so ist dies dem/der Betroffenen anzuzeigen. zB mittels einer Signallampe im Fahrzeug

Es wird den ArbeitnehmerInnen frei gestellt, ob sie einen außerplanmäßigen Auftrag hinzunehmen oder nicht.

6. Gesundheit und Sicherheit am Arbeitsplatz

Bei der Verwendung von Bordcomputern: Sollte für das Lesen des Bildschirms eine eigene/zusätzliche Brille erforderlich sein, so wird diese vom Arbeitgeber bezahlt. Bei Bedarf ist eine jährliche Kontrolle durch einen Augenarzt ist zu gewährleisten.

Komplexe Telematiksysteme können in brenzligen Situationen (zB Verwicklung in einen Unfall) durch ihr Verhalten (zB permanentes Piepsen) zu Stress und dadurch vergrößerter Gefahr führen.

In Gefahrensituationen hat der/die ArbeitnehmerIn die Möglichkeit, das Gerät auszuschalten.

7. Arbeitszeit-Pausenberechnung

Sollte das Ortungssystem mit einem System gekoppelt sein, das Statusmeldungen des Kfzs speichert, kann das Verhalten der FahrerInnen minutiös nach verfolgt werden. Daher:

Die Statusdaten des Fahrzeugs zB Geschwindigkeit, Benzinverbrauch, Zündung an/aus werden nicht als Berechnungsbasis für Pausen und geleistete Arbeitszeit herangezogen. Die Pausen- und Arbeitszeitregelungen werden entsprechend den generellen betrieblichen Regelungen beibehalten.

Sollten Daten über die Arbeitszeit- und Pausen über das mobile Terminal oder über eine eigene Chipkartenlösung erfasst werden, so sind diese Daten von den Statusmeldungen des Fahrzeugs getrennt zu behandeln – am besten in einer Betriebsvereinbarung zur Arbeitszeiterfassung.

Das An- und Abmelden darf nur zur Disposition von ArbeitnehmerInnen nach Entfernung und Qualifikation verwendet werden – nicht zur Überprüfung der Arbeitszeit, da diese nicht ident ist mit der Beanspruchung des Fahrzeugs. Stichwort: abgestelltes Fahrzeug vor Bahnschranken, im Stau, etc.

Auch die gesetzlich vorgeschriebenen Inhalte des Fahrtenbuches werden nicht über die Status-meldungen des Fahrzeugs berechnet.

Einsätze werden nur nach persönlicher Rückfrage bei den MitarbeiterInnen geändert.

Sollten Zweifel hinsichtlich der Richtigkeit der erfassten Arbeitszeiten bestehen, verpflichtet sich der/die ArbeitgeberIn, die Aufzeichnungen gemeinsam mit dem/der ArbeitnehmerIn zu überprüfen. Einseitige Eingaben oder Änderungen durch MitarbeiterInnen der Personalverwaltung sind gesondert gekennzeichnet.

8. Erreichbarkeit

Grundsätzlich müssen MitarbeiterInnen im Sinne einer aktiven Kundenorientierung nicht permanent erreichbar sein. MitarbeiterInnen müssen sich in regelmäßigen Abständen kann noch näher definiert werden in der Zentrale melden – sowie es ihre Arbeitszeiten erlauben.

Meldet sich ein/e MitarbeiterIn nicht innerhalb von X Stunden in der Zentrale, kann er/sie aus Sicherheitsgründen kontaktiert werden. Frist ist an die Arbeitsbedingungen anzupassenden und sollte keinesfalls unter zwei Stunden liegen.

Die MitarbeiterInnen sind nicht gezwungen, sich in auftragsfreien Zeiten im Fahrzeug aufzuhalten.

MitarbeiterInnen sind außerhalb der vertraglichen Arbeitszeit nicht verpflichtet, das Gerät einzuschalten.

9. Datenverwendung

9.1. Auswertungen, Listen und Reports

In Software X werden folgende personen- und tätigkeitsbezogenen Daten verwendet:

- Personalstammdaten: Name, Personalnummer, Firmenhandy
- Falls die Einsätze nach Qualifikation unterschiedlich geplant werden: Qualifikation
- Organisatorische Zuordnung
- Route
- Informationen zum Einsatz: Ort, Vertragsdaten, Art der ausgeführten Tätigkeit die Möglichkeiten sollten hier möglichst standardisiert sein, sodass alle dieselben Vorgaben haben und nicht allzu einschränkend sein; zB zwei vorgegebene Kästchen zum eingeben: Störungsbehebung/Wartung Dauer der Tätigkeit
- Arbeitszeitdaten lt. Einsatzplanung
- Status: verfügbar ja/nein
- geplante Aufträge

Eine taxative Auflistung von personenbezogenen Listen und Reports ist jedenfalls zu erstellen – die Liste kann auch im Anhang 1 sein, zB in Form eines Excel-sheets.

Die Daten werden ausschließlich für die in dieser Vereinbarung angegebenen Zwecke eingesetzt.

Bei Konzernen empfiehlt es sich die personenbezogenen Einsatzdaten auf nationaler Ebene zu belassen. Daher:

Eine Verknüpfung von personenbezogenen Daten mit Daten anderer Konzerntöchter ist nicht gestattet.

Wenn regelmäßige Auswertungen geplant sind, müssen diese abschließend in der BV bzw. im Anhang aufgelistet werden (beliebt bei der GF und zu hinterfragen vom BR ist zB die Auswertung „un-/produktiver" Stunden). Sollten Ad-hoc-Auswertungen gewünscht sein (dh einmalige Auswertungen nach frei zusammengestellten Auswertungskriterien), sind diese nicht zulässig, wenn sie den Rückschluss auf Einzelne ermöglichen. Einer rein statistischen Auswertung steht nichts entgegen, solange der Grundsatz der Anonymität eingehalten ist. Daher bei Ad-hoc-Auswertungen:

Bei Auswertungen, die über im Rahmen der BV konkret vereinbarte hinausgehen, werden Personengruppen bestehend aus mindestens 10 MitarbeiterInnen zusammengefasst, sodass kein Personenbezug mehr besteht.

Die Weitergabe von Auswertungen ist nur in zusammengefasster Form, also ohne Personenbezug auf Anfrage an die jeweils direkten Vorgesetzten möglich.

Bei einem Verdacht auf Fehlverhalten von MitarbeiterInnen, ist dieser schriftlich zu begründen und nur mit Zustimmung des Betriebsrates können allfällige Auswertungen veranlasst werden. Der Betroffene ist über die Auswertungen und deren Ergebnisse umgehend zu informieren.

Dateneingabe, Datenpflege und Wartung der Daten ist immer Arbeitszeit.

9.2. Löschung

Die Ortungsdaten werden nach einer Woche gelöscht. Daten, die für die Überprüfung eines Auftrags oder die Erfüllung gesetzlicher Vorgaben erforderlich sind, werden für X Monate gespeichert. Nach dieser Frist werden die personenbezogenen Daten gelöscht und nur mehr aufsummierte Daten gespeichert. Die gesamten Daten werden nach X Jahren gelöscht.

ODER bei Betrieben in denen die Fahrzeuge nicht fix FahrerInnen zugeordnet sind:

Die Liste mit Zuordnungen von Fahrern zu den Fahrzeugen wird ausschließlich in der Einsatzleitung für einen Monat aufgehoben und dann gelöscht.

9.3. Routenplanung

Bei konkreten Routenvorgaben ist es den FahrerInnen möglich, nach Rücksprache mit der Zentrale, die Route abzuändern. Sollten Planungsdaten benötigt werden, so werden dafür nur anonymisierte Daten verwendet.

Aus den Fahrtenbuchaufzeichnungen der MitarbeiterInnen errechnen sich die gefahrenen Kilometer und werden zum Zweck der Kilometergeldabrechnung übermittelt. Die für das Fahrtenbuch relevanten Daten sind im **Anhang 2** angeführt.

9.4. Privatnutzung

Sollten die Fahrzeuge auch zur Privatnutzung zur Verfügung stehen und das Ortungssystem auch während dieser Zeit Daten aufzeichnen, müssen diese Aufzeichnungen:

a) einen sinnvollen Zweck erfüllen (zB zusammenfassende Darstellung der gefahrenen Kilometer, Ortung des Fahrzeuges zur privaten Orientierung) und

b) dürfen dem Arbeitgeber dadurch keine personenbezogenen Daten über die Privatsphäre der ArbeitnehmerInnen zur Verfügung gestellt werden.

Daher:

Das Versenden und Empfangen von Positionsbestimmungen ist in einem Ausmaß gestattet, das keine zusätzlichen Kosten verursacht und den Geschäftsablauf nicht stört.

Eine Verwendung der Daten, die bei der privaten Nutzung von Fahrzeugen entstehen, durch den/die ArbeitgeberIn ist nicht gestattet. Die aufgrund der Privatnutzung entstehenden Daten werden ausschließlich im Rahmen gesetzlicher Verpflichtungen an zuständige Behörden weitergeleitet.

9.5. Zugriffsberechtigungen

Alle zugriffsberechtigten Personen haben durch ihre Unterschrift zu bestätigen, dass sie über die verwendeten personenbezogenen Daten, das Bestehen der gegenständlichen Betriebsvereinbarung und die daraus resultierenden Datenschutzbestimmungen informiert wurden. Diese Bestätigungen liegen auch dem Betriebsrat vor.

Eine genaue Auflistung der Berechtigungen ist am besten im Anhang 3 zu ergänzen.

10. Rechte und Pflichten

10.1. Informationspflicht des Dienstgebers

Alle MitarbeiterInnen müssen bei Beginn des Dienstverhältnisses über die Verwendung des Systems X und die darin enthaltenen personenbezogenen Daten informiert werden. In regelmäßigen Abständen werden diese Informationen aktualisiert.

ODER:

MitarbeiterInnen sind über die Verwendung ihrer Daten zu informieren (§ 24 DSG). Die Information umfasst insbesondere Angaben darüber, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden, woher die Daten stammen und an wen sie weitergeleitet werden (§ 1 Abs 3 DSG).

Die bestehende Betriebsvereinbarung ist zu erläutern.

Da es sich bei Ortungssystemen um Systeme handelt, die personenbezogene Daten verarbeiten, ist diese Verwendung im Datenverarbeitungsregister anzugeben, welches von der Datenschutz-kommission im Bundeskanzleramt geführt wird.

10.2. Rechte der ArbeitnehmerInnen

Jede/r ArbeitnehmerIn hat das Recht auf Auskunft über die zu seiner/ihrer Person verarbeiteten Daten (§ 26 DSG). Ferner besteht das Recht auf Richtigstellung unrichtiger Daten bzw. auf Löschung jener Daten, die unberechtigt ermittelt wurden (§ 1 Abs 3 DSG) oder deren Verwendung nicht mehr erforderlich ist (§ 27 DSG).

Auskunft gebende Person ist X. Name oder Funktion der verantwortlichen MitarbeiterIn; zB Personalabteilung, Rechtsabteilung, Datenschutzbeauftragte/r.

10.3. Rechte des Betriebsrats

Die Geschäftsleitung stellt dem Betriebsrat eine Übersicht über Zugriffskompetenzen und Zugriffs-rechte, ein Verzeichnis von Art, Standort und Verknüpfung der sich im Einsatz befindlichen Geräte zur Verfügung. Der Betriebsrat kann jederzeit die Übereinstimmung des vereinbarten System-zustandes mit dem tatsächlichen Systemzustand überprüfen.

Werden bestimmt Daten externen Dienstleistern überlassen (zB Personalverrechnung wurde outgesourct), sollte der BR Zugang zu den zugrunde liegenden Verträgen haben:

Sofern zwischen Unternehmen und Dritten Verträge existieren, die Datenübermittlung von oder zum Unternehmen betreffen, hat der Betriebsrat ein Einsichtsrecht in diese Verträge. Existieren keine Verträge, ist dem Betriebsrat eine Übersicht über die Datenübertragungen zu übermitteln.

Zur Klärung technischer Fragen hat der Betriebsrat das Recht, externe ExpertInnen hinzuzuziehen, die vom Unternehmen zu bezahlen sind. .

Bei geplanten Systemänderungen ist der Dienstgeber/die Dienstgeberin verpflichtet, den Betriebs-rat umfassend und vom Beginn der Planung an, zu informieren.

Oder eine etwas eingeschränktere Bestimmung:

Ist im Rahmen eines Systemwechsels oder einer Systemadaptierung eine erweiterte Verwendung personenbezogener Daten vorgesehen, ist diese zwischen Arbeitgeber und Betriebsrat zu vereinbaren.

Je nach Umfang der Änderung ist eine entsprechende Nachschulung anzubieten.

11. Qualifizierung

Alle von dieser Betriebsvereinbarung betroffenen Beschäftigten sind auf Kosten des Arbeitgebers/der Arbeitgeberin umfassend zu schulen. Die Schulung ist zeitnah zum erstmaligen Einsatz des Systems und im Rahmen der bezahlten Arbeitszeit durchzuführen. Bei der Schulung wird die Herstellerfirma hinzugezogen und bestehende Kontrollmöglichkeiten sowie Datenschutzaspekte werden explizit erörtert.

Betriebsratsmitglieder sind berechtigt, im Rahmen der bezahlten Arbeitszeit und auf Kosten des Arbeitgebers/der Arbeitgeberin an den Schulungen teilzunehmen.

12. Evaluierung und Konfliktlösung

Evaluierung und Konfliktlösung sind Aufgabe einer internen Kommission. Diese interne Kommission besteht aus fünf Mitgliedern (Anhang 4). Jede Vertragspartei entsendet zwei Kommissionsmitglieder. Darüber hinaus gehört ihr in beratender Funktion der/die betriebliche Datenschutz-beauftragte an.

Konkrete Anregungen zur Festlegung von Aufgaben, Entscheidungsbefugnissen und Sitzungs-häufigkeit von interner Kommission und Datenschutzbeauftragtem/-r können in der GPA-djp nach-gefragt werden.

13. Inkrafttreten und Geltungsdauer

Diese Betriebsvereinbarung tritt mit XX.XX.XXXX in Kraft, gilt unbefristet und ist jederzeit ohne Nachwirkung kündbar.

Alternativ kann sich – je nach betrieblichen Gegebenheiten - auch die Vereinbarung einer befris-teten Geltungsdauer empfehlen: Diese Betriebsvereinbarung tritt am XX.XX.XXXX in Kraft und wird zunächst auf die Dauer von X Monaten, somit bis XX.XX.XXXX, befristet abgeschlossen. X Monate vor Ablauf der Befristung prüft die interne Kommission gemäß Punkt 12 die Betriebsverein-barung auf Praktikabilität und erstattet ggf. Modifizierungsvorschläge. Allfällige Änderungen und Ergänzungen dieser Betriebsvereinbarung bedürfen des Einvernehmens zwischen den Vertragspar-teien sowie der Schriftform. Nach positivem Abschluss der Evaluierung gilt die Betriebsvereinba-rung unbefristet weiter.

14. Anhang

Anhang 1: Abschließende Aufzählung der regelmäßig durchgeführten Auswertungen /Listen/Reports, Häufigkeit der Durchführung
Anhang 2: Daten des Fahrtenbuches
Anhang 3: Zugriffsberechtigungen
Anhang 4: Mitglieder der internen Kommission

Zeichnungsbevollmächtigte:

für die Unternehmensleitung | für den Betriebsrat

..... | .....

Datum:.....

Mustervereinbarung mobile Leistungslohnverrechnung

Vorbemerkung: Mustervereinbarungen und Leitfäden können Orientierung geben, sind jedoch nur dann nützlich, wenn sie auf die speziellen betrieblichen Umstände zugeschnitten sind. Wird ein Betriebsvereinbarungsmuster nicht „maßgeschneidert", gehen schnell wichtige Gestaltungs-möglichkeiten verloren. Aus diesem Grund sind die Regelungen der nachfolgenden Betriebsvereinbarung als Eckpunkte zu verstehen. Sie sollen als Anregungen dienen, um daraus eine zu den Verhältnissen im eigenen Betrieb möglichst optimal passende Vereinbarung zu entwickeln.

Die GPA-djp unterstützt und berät Sie gerne auf diesem Weg!

Hinweis: Die in der Muster-Betriebsvereinbarung grau hinterlegten Passagen sind als Kommentare zu verstehen und stellen keinen normativen Betriebsvereinbarungstext dar.

Muster - Betriebsvereinbarung

für den Einsatz von mobiler Leistungserfassung mittels.....

Der Name des Systems muss hier angeführt werden, da nur so festgestellt werden kann, über welche technischen Möglichkeiten das System verfügt. Gängige Produkte sind zB Blackberrys und auf diesen werden dann eigene Software zur Leistungserfassung installiert.

gemäß § 96 Abs 1 Z 3 ArbVG iVm § 96a ArbVG

zwischen der Geschäftsführung der Firma.....

und dem Betriebsrat der Firma....

Inhaltsverzeichnis:

1. Geltungsbereich

Diese Betriebsvereinbarung gilt: für alle ArbeitnehmerInnen sowie die bei der Firma X beschäftigten arbeitnehmerähnlichen Personen (insbesondere freie DienstnehmerInnen und Leiharbeitskräfte), die seitens der Fa. X mobile Endgeräte zur Verfügung gestellt bekommen.

2. Rechtsgrundlagen

Die rechtliche Basis bilden insbesondere die Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG) im Besonderen die §§ 91, 92, 96, 96a und 97 sowie die Bestimmungen des Datenschutz-gesetzes 2000 (DSG 2000).

3. Zielsetzung

Die BV dienst dem Schutz der Persönlichkeitsrechte der MitarbeiterInnen.

Das System X wird nicht zum Leistungsvergleich, zur Leistungsbeurteilung und/oder zur

Verhaltenskontrolle der MitarbeiterInnen herangezogen.

ODER:

Das System dient der Leistungserfassung und darf weder zur Verhaltenskontrolle noch zur Steigerung des Arbeits- und Leistungsdrucks der ArbeitnehmerInnen verwendet werden.

Die Daten aus dem X Name des mobilen Geräts zB Blackberry werden für

- die effiziente Abwicklung von betrieblichen Abläufen
- für die Disposition der Einsatzkräfte
- zur Leistungsverrechnung gegenüber den AuftraggeberInnen und den KundInnen
- effizienten Datenübertragung zwischen ArbeitnehmerInnen und ArbeitgeberIn

verwendet.

Über die in der BV getroffenen Auswertungen und Kontrollen hinausgehende Datenverwendungen sind nicht zulässig. Allfällige Leistungs- und Verhaltenskontrolle der Beschäftigten ist auf die hier vereinbarten Kontrollen beschränkt.

ODER:

Das Unternehmen X betreibt das System X Name des mobilen Geräts zB Blackberry mit dem Ziel einer effizienten Datenübermittlung zwischen ArbeitnehmerIn und ArbeitgeberIn, sowie einer effizienten Planung und Leistungsverrechung in der KlientInnenbetreuung.

4. Grundsatz

Es gilt der Grundsatz der Datensparsamkeit. Die Daten werden ausschließlich für die hier vereinbarten Zwecke verwendet.

5. Systembeschreibung

5.1. Beschreibung des Systems

Technische Infrastruktur, Geräte, Software, Systemkomponenten, Schnittstellen.

Diese Systembeschreibung kann im Anhang (Anhang 1) oder im firmeneigenen Intranet abgelegt werden. Die Systembeschreibungen sind allen MitarbeiterInnen zugänglich zu machen.

Die Daten werden manuell von den MitarbeiterInnen synchronisiert.

ODER:

Die Datenübertragung erfolgt grundsätzlich automatisch im Stundenintervall.

Bei einem technischen Ausfall gilt die schriftliche Aufzeichnung der/des MitarbeiterIn.

5.2. Haftung

Die Haftung der MitarbeiterInnen für Beschädigungen und Abhandenkommen der firmeneigenen Geräte und deren Zubehör ist auf Vorsatz und grobe Fahrlässigkeit beschränkt.

Bei Verlust und/oder Diebstahl des mobilen Einsatzgerätes bzw. des Zubehörs ist der/die ArbeitgeberIn unverzüglich zu benachrichtigen.

5.3. Kosten

Der/die BetriebsinhaberIn übernimmt die Anschaffungskosten für das Gerät, die Wartungskosten für den laufenden Betrieb sowie anfallende Reparaturkosten.

5.4. Systemanwendung

Jede/r ArbeitnehmerIn erhält ein mobiles Einsatzgerät mit dem entsprechenden Zubehör.

Der Empfang ist schriftlich zu bestätigen. Zu jedem Einsatz sind die jeweiligen Leistungen sowie Leistungszeiten von den MitarbeiterInnen zu dokumentieren. Leistungszeiten sowie Leistungen sind von allen MitarbeiterInnen verpflichtend tagesaktuell zu führen. Ein konkreter aktueller Leistungskatalog ist im Anhang (**Anhang 2**) beizufügen.

5.5. Arbeitszeit

Dateneingabe, Datenpflege, Wartung der Daten ist immer Arbeitszeit.

ODER:

Pro Arbeitstag wird automatisch eine halbe Stunde zugebucht, die aufgrund der Datenbearbeitung erfahrungsgemäß entsteht.

Einsätze werden nicht ohne Mitsprache der Betroffenen einseitig geändert.

ODER:

Die MitarbeiterInnen haben die Möglichkeit, Aufträge nicht anzunehmen, sofern sie keine Möglichkeit sehen, die Arbeit in angemessener Zeit durchzuführen.

Diese Information (angenommen/nicht angenommen) wird in weiterer Folge zur besseren Planung und Optimierung der Routen ausgewertet.

ODER:

Werden Einsätze einseitig von der Zentrale aus angeordnet, sind die dadurch entstehenden Mehr- und/oder Überstunden entsprechend zu verrechnen.

Am Monatsende werden die Einsatzzeiten jeder Mitarbeiterin/ jedes Mitarbeiters in einer Übersicht dargestellt und die Möglichkeit zur Berichtigung gegeben. Änderungen bzw. Korrekturen der Monatsübersicht sind ausschließlich im Einvernehmen mit den MitarbeiterInnen vorzunehmen.

5.6. Erreichbarkeit

Grundsätzlich müssen MitarbeiterInnen im Sinne einer aktiven KundInnenorientierung nicht permanent über das Handy erreichbar sein. MitarbeiterInnen müssen sich in regelmäßigen Abständen in der Zentrale melden/ die Mobilbox abhören – sowie es ihre Arbeitszeiten erlauben.

Kann noch näher definiert werden, zB drei Mal im Laufe eines vollen Arbeitstages

Meldet sich ein/e MitarbeiterIn nicht innerhalb von X Stunden in der Zentrale, kann er/sie aus Sicherheitsgründen kontaktiert werden.

Frist ist an die Arbeitsbedingungen anzupassen und sollte keinesfalls unter drei Stunden liegen.

MitarbeiterInnen sind außerhalb der vertraglichen Arbeitszeit oder Rufbereitschaftszeit nicht verpflichtet, das mobile Endgerät einzuschalten.

6. Datenverwendung

6.1. Auswertungen, Listen und Reports

Es werden folgende personen- und tätigkeitsbezogenen Daten verwendet:

- Personalstammdaten: Name, Personalnummer, Organisatorische Zuordnung
- Firmenhandynummer
- Informationen zum Einsatzort: Ort, Art der ausgeführten Tätigkeit (zB Dauer der Störungs-behebung/ Wartung, Leistungserbringung laut Katalog)
- Arbeitszeitdaten lt. Einsatzplanung,
- Status: verfügbar ja/nein
- Geplante Aufträge/Jobs: Name der Kundin/des Kunden, Ort, Art des Einsatzes

Eine taxative Auflistung von personenbezogenen Listen und Reports ist jedenfalls zu erstellen – ev. in Form eines Excel-sheets (Anhang 3). Bei Konzernen empfiehlt es sich, die personenbezogenen Einsatzdaten auf nationaler Ebene zu belassen. Daher:

Eine Verknüpfung von personenbezogenen Daten mit Daten anderer Konzerntöchter ist nicht gestattet. Auswertungen werden ausschließlich in der Zentrale Abteilung X, zB Personalverwaltung durchgeführt.

Es werden ausschließlich die im **Anhang 3** aufgelisteten Auswertungen durchgeführt.

Regelmäßige Auswertungen müssen abschließend in der BV aufgelistet werden (beliebt ist zB die Auswertung „un-/produktiver" Stunden, was vermieden werden sollte).

Vorgesetzte können folgende Auswertungen jederzeit anfordern. Eine solche Anforderung wird vermerkt.

Ad-hoc-Auswertungen müssen ebenfalls in einer eigenen Liste im Anhang (Anhang 4) festgelegt werden. Sie sind allerdings nicht zulässig, wenn sie den Rückschluss auf Einzelne ermöglichen. Einer rein statistischen Auswertung steht nichts entgegen, solange der Grundsatz der Anonymität eingehalten ist. Daher bei Ad-hoc-Auswertungen:

Bei Ad-hoc-Auswertungen werden Personengruppen bestehend aus mindestens 10 MitarbeiterInnen zusammengefasst, sodass kein Personenbezug mehr besteht.

6.2. Löschung

Die anfallenden Daten aus der Auftragsbearbeitung stehen nur für eine nachträgliche Überprüfung eines Auftrags oder die Erfüllung gesetzlicher Vorgaben zur Verfügung. Sie werden für X Monate gespeichert.

Die Speicherung personenbezogener Daten richtet sich nach den gesetzlichen Notwendigkeiten und den betrieblichen Abläufen – sie sollte so kurz wie nur irgend möglich gehalten werden. Empfehlenswert sind zB ein Quartal Speicherdauer um Reklamationen der KundInnen bearbeiten zu können.

Nach dieser Frist werden die personenbezogenen Daten gelöscht und nur mehr aufsummierte Daten gespeichert. Diese werden nach X Jahren gelöscht.

6.3. Privatnutzung

Das Versenden und Empfangen privater Nachrichten sowie das Führen von privaten Telefonaten ist in einem Ausmaß gestattet, das keine hohen zusätzlichen Kosten verursacht und den Geschäft-sablauf nicht stört.

ODER:

Für die private Verwendung ist die Vorwahl X zu verwenden und die hier anlaufenden Kosten werden getrennt abgerechnet. Die Rechnung sowie allfällige Einzelgesprächsnachweise werden vom Telefonanbieter direkt an die betroffene Person gesandt. Gespräche, die unter dieser Vorwahl geführt werden, dürfen vom/von der ArbeitgeberIn nicht datentechnisch verarbeitet werden.

Dh es dürfen keine Gesprächsprotokolle, Verbindungsdaten, und Ähnliches zur Geschäftsführung gelangen.

Die Verbindungsdaten über eingehende Mails werden elektronisch protokolliert. Das Protokoll dient ausschließlich zur Analyse und Korrektur technischer Fehler und zur Gewährleistung der Sicherheit des unternehmensinternen Netzes. Zugriff auf diese Daten hat ausschließlich die Netzwerk-administration. Das Protokoll wird regelmäßig X mal pro Monat archiviert. Bei diesem Archivierungsvorgang wird die vorletzte Kopie automatisch gelöscht.

Der/die ArbeitgeberIn erhält vom Netzwerkbetreiber keine Einzelgesprächsnachweise, sondern nur Gesamtkostenabrechnungen. Sollte es zu auffälligen Abrechnungen kommen, können in Absprache mit dem Betriebsrat Einzelgesprächsnachweise gefordert werden.

6.4. Zugriffsberechtigungen

Alle zugriffsberechtigten Personen haben durch ihre Unterschrift zu bestätigen über die verwendeten Daten, das Bestehen der gegenständlichen Betriebsvereinbarung und die daraus resultierenden Datenschutzbestimmungen informiert worden zu sein. Diese Bestätigungen sind dem Betriebsrat in Kopie zu übermitteln.

Eine genaue Auflistung der Berechtigungen ist am besten im Anhang (Anhang 5) zu ergänzen.

7. Rechte und Pflichten

7.1. Informationspflicht des Dienstgebers/der Dienstgeberin

Alle MitarbeiterInnen müssen bei Beginn des Dienstverhältnisses über die Verwendung des mobilen Endgerätes informiert werden. MitarbeiterInnen sind gemäß § 24 Datenschutzgesetz (DSG) in geeigneter, also verständlicher Weise über die Verwendung ihrer Daten zu informieren. Die bestehende Betriebsvereinbarung ist zu erläutern.

7.2. Rechte der ArbeitnehmerInnen

Jede/r ArbeitnehmerIn hat das Recht auf Auskunft über die zu seiner/ihrer Person verarbeiteten Daten gemäß § 26 DSG. Ferner besteht das Recht auf Richtigstellung unrichtiger Daten bzw. auf Löschung jener Daten, die unberechtigt ermittelt wurden (nach § 1 Abs 3 DSG) oder deren Verwendung nicht mehr erforderlich ist (§ 27 DSG). Sollten Zweifel hinsichtlich der Richtigkeit der erfassten Arbeitszeiten bestehen, verpflichtet sich der/die ArbeitgeberIn die Aufzeichnungen gemeinsam mit dem/der ArbeitnehmerIn zu überprüfen. Eingaben durch MitarbeiterInnen der befugten Abteilung zB Personalverwaltung sind gesondert gekennzeichnet.

7.3. Rechte des Betriebsrats

Die Geschäftsleitung stellt dem Betriebsrat eine Übersicht über Zugriffskompetenzen und Zugriffs-rechte, ein Verzeichnis von Art, Standort und Verknüpfung der verwendeten Geräte zur Verfügung. Der Betriebsrat kann jederzeit die Übereinstimmung des vereinbarten Systemzustandes mit dem tatsächlichen Systemzustand überprüfen.

Im Falle von externen Dienstleistern, an die bestimmte Daten überlassen werden, sollte der Betriebsrat Zugang zu den zugrunde liegenden Verträgen haben. Daher absichern:

Sofern zwischen Unternehmen und Dritten Verträge existieren, die Datenübermittlung von oder zum Unternehmen betreffen, hat der Betriebsrat ein Einsichtsrecht in diese Verträge. Existieren keine Verträge, ist dem Betriebsrat eine geeignete Übersicht über die Datenübertragungen zu ü-bermitteln. Zur Klärung technischer Fragen hat der Betriebsrat das Recht, externe ExpertInnen hinzu zu ziehen, die vom Unternehmen zu bezahlen sind.

Bei geplanten Systemänderungen ist der/die DienstgeberIn verpflichtet, den Betriebsrat sowie betrieblicheN DatenschutzbeauftragteN (siehe Punkt 7.4.) und interne Schlichtungsstelle (siehe Punkt 7.4.) rechtzeitig und umfassend vom Beginn der Planung an, zu informieren.

Oder eine etwas eingeschränktere Bestimmung:

Ist im Rahmen eines Systemwechsels oder einer Systemadaptierung eine erweiterte Verwendung personenbezogener Daten vorgesehen, ist diese zwischen ArbeitgeberIn und Betriebsrat zu vereinbaren.

7.4. Bestellung eines/r Datenschutzbeauftragten

Geschäftsführung und Betriebsrat bestellen gemeinsam eine/n betriebliche/n Datenschutzbeauftragte/n (DSB), die/der zu datenschutzrelevanten Themen berät und Mitglied der allfällig einberufenen betrieblichen Schlichtungsstelle ist.

Die Aufgaben sowie die arbeitsrechtliche Absicherung des/der DSB können in der Betriebsvereinbarung zusätzlich konkretisiert werden; zB ist AnsprechpartnerIn für alle Beschäftigten und unterstützt sie beratend beim Schutz ihrer personenbezogenen Daten, besucht regelmäßig Fortbildungen, um auf dem neuesten Stand zu sein, ist AnsprechpartnerIn für datenschutzrelevante Fragen in rechtlicher, technischer und administrativer Hinsicht, etc. Details über die genauen Rechte und Pflichten eines/r Datenschutzbeauftragten, können bei der GPA-djp nachgefragt werden.

7.5. Qualifizierung

Alle von dieser Betriebsvereinbarung betroffenen Beschäftigten sind umfassend auf Kosten des/der ArbeitgeberIn zu schulen. Die Schulung ist zeitnah zum erstmaligen Einsatz des Systems und im Rahmen der bezahlten Arbeitszeit durchzuführen. Betriebsratsmitglieder sind berechtigt, auf Kosten des/der ArbeitgeberIn an den Schulungen teilzunehmen. In Absprache mit dem Betriebsrat werden die MitarbeiterInnen einmal pro Jahr über ihre Erfahrungen mit dem System der mobilen Leistungserfassung befragt, um Ansatzpunkte für eine mögliche Verbesserung des Systems und damit der Benutzerfreundlichkeit zu erhalten.

8. Inkrafttreten

Diese Betriebsvereinbarung tritt mit XX.XX.XXXX in Kraft, gilt unbefristet und ist jederzeit ohne Nachwirkung kündbar.

Alternativ kann sich – je nach betrieblichen Gegebenheiten - auch die Vereinbarung einer befristeten Geltungsdauer empfehlen: Diese Betriebsvereinbarung tritt am XX.XX.XXXX in Kraft und wird zunächst auf die Dauer von X Monaten, somit bis XX.XX.XXXX, befristet abgeschlossen. X Monate vor Ablauf der Befristung prüft die interne Kommission (je 2 Beauftragte der Geschäftsführung und des Betriebsrates), unter Beiziehung des/r betrieblichen Datenschutzbeauftragten, die Betriebsvereinbarung auf Praktikabilität und erstattet ggf.

Modifizierungsvorschläge. Allfällige Änderungen und Ergänzungen dieser Betriebsvereinbarung bedürfen des Einvernehmens zwischen den Vertragsparteien sowie der Schrift-form. Nach positivem Abschluss der Evaluierung gilt die Betriebsvereinbarung unbefristet weiter.

9. Konfliktlösung und Evaluierung

Evaluierung und Konfliktlösung sind Aufgabe einer internen Kommission. Diese interne Kommission besteht aus fünf Mitgliedern. Jede Vertragspartei entsendet zwei Kommissionsmitglieder. Darüber hinaus gehört ihr in beratender Funktion der/die betriebliche Datenschutzbeauftragte an.

Konkrete Anregungen zur Festlegung von Aufgaben, Entscheidungsbefugnissen und Sitzungshäufigkeit von interner Kommission und Datenschutzbeauftragtem/r können in der GPA-djp nachgefragt werden. Eine Formulierung könnte sein:

X Monate vor Ablauf der Befristung prüft die interne Kommission die Betriebsvereinbarung auf Praktikabilität und macht gegebenenfalls Modifizierungsvorschläge. Es wird beginnend mit XX.XX.XXXX die vorliegende Betriebsvereinbarung X Mal jährlich in einem gemeinsamen Gespräch zwischen Geschäftsführung und Betriebsrat beraten. Dabei wird ihre Aktualität bezüglich der Bedürfnisse der ArbeitnehmerInnen und der Entwicklung des Gesamtunternehmens analysiert.

Kommt es zu Unklarheiten über eingetragene oder einzutragende Daten, werden die Betroffenen zunächst von den zuständigen MitarbeiterInnen in der IT und/oder Personalverwaltung darauf aufmerksam gemacht. Sollte es so zu keiner Klärung kommen, werden der/die direkte Vorgesetzte und der Betriebsrat über das Problem informiert und ein gemeinsames Treffen angeregt. Bei Problemen, die auch auf diesem Wege nicht gelöst werden können, ist eine interne Kommission einzuberufen.

10. Anhang

Anhang 1: Beschreibung System
Anhang 2: Systemanwendung - Leistungskatalog
Anhang 3: Taxative Auflistung von personenbezogenen Listen und Reports (Excel-Sheet)
Anhang 4: Ad-hoc-Auswertungen
Anhang 5: Berechtigungen

Zeichnungsbevollmächtigte:

für die Unternehmensleitung für den Betriebsrat

……. ……

Datum:……

Links zum Datenschutz

Überwachungs- und Kontrollmaßnahmen gegenüber MitarbeiterInnen sind weltweit im Vormarsch. Die technischen Möglichkeiten sind scheinbar unbegrenzt und die einzelnen Systeme werden immer leistungsstärker und immer häufiger miteinander verknüpft. Sei es eine weltweite Vernetzung der Personalverrechnungs- und Leistungsbeurteilungssysteme bei internationalen Konzernen, eine elektronische Zeiterfassung kombiniert mit Standortbestimmung und Leistungserfassung bei Transport- und Logistikunternehmen oder eine Videoüberwachung im Betrieb – immer werden die persönlichen Daten der MitarbeiterInnen aufgezeichnet.

Das österreichische Arbeitsverfassungsgesetz und das Datenschutzgesetz setzen diesen Vorgängen Grenzen. Der/die Betriebsrat/-rätin hat Mitspracherecht, sobald die personenbezogenen Daten der MitarbeiterInnen betroffen sind.

Die Linksammlung bietet wichtige Informationen im Zusammenhang mit dem Schutz von MitarbeiterInnen-Daten.

Österreich:
Die GPA-djp, Abteilung Arbeit und Technik, bietet ihren Mitgliedern eine umfangreiche Sammlung an Muster-Betriebsvereinbarungen zu den gebräuchlichsten technischen Systemen
http://www.gpa-djp.at/servlet/ContentServer?pagename=GPA/Page/Index&n=GPA_9.3

und Broschüren zum betrieblichen Datenschutz an
http://www.gpa-djp.at/servlet/ContentServer?pagename=GPA/Page/Index&n=GPA_9.2

Aktuelle Informationen aus der betrieblichen Praxis und Rechtsentwicklung im ArbeitnehmerInnen-Datenschutz, Beispiele aus den Betrieben und praxisnahe Anregungen bietet der Blog:
http://arbeitundtechnik.gpa-djp.at/

Die **Datenschutzkommission** findet man unter der Adresse: http://www.dsk.gv.at/
Die Seite bietet grundsätzliche Informationen zu Aufgaben und Kompetenzen der Kommission, Entscheidungen der Kommission, Formulare für die Meldung und Genehmigung von Datenanwendungen, sowie den im Zwei-Jahres-Abstand erscheinenden Datenschutzbericht. Auch die aktuellen Versionen der **Standard- und Musterverordnung** sind hier einsehbar. Das **Datenverarbeitungsregister** wird von der Datenschutzkommission geführt und ist somit auch über diese Homepage erreichbar. Seit 2010 ist die **Online-Meldung** im DVR gesetzlich vorgegeben und in Planung, doch gibt es dazu – noch – keinen Link.
Das **Datenschutzgesetz**: http://www.dsk.gv.at/dsg2000d.htm

„Das Österreichische Informationssicherheitshandbuch" 2007 vom Bundeskanzleramt erstellt, enthält alle wesentlichen Schritte, die erforderlich sind um ein innerbetriebliches Sicherheitsmanagement zu betreiben. Zielgruppen sind sowohl die Privatwirtschaft als auch mittlere und größere Organisationen (für die öffentliche Verwaltung ist es per Ministerratsbeschluss vom Juli 2007 explizit empfohlen):
http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=23263

Europa:
News, Richtlinien, Rechtssprechung, nationale Kontaktadressen, etc. und auch ein anschauliches Video der **EU-Kommission**: http://ec.europa.eu/justice/data-protection/index_de.htm

Der Entwurf der neuen **EU-Datenschutz-Verordnung** der EU-Kommission ist in ihrer Version vom Jänner 2012 hier zu begutachten:
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

Die kritische **Stellungnahme des Österreichischen Gewerkschaftsbundes** dazu ist hier zu lesen:
http://arbeitundtechnik.gpa-djp.at/2012/03/13/eu-datenschutzverordnung-reloaded/

Stellungnahme des **Europäischen Wirtschafts- und Sozialausschusses** (EWSA):
http://www.gpa-djp.at/servlet/NcMain?pagename=GPA/Page/Index&n=GPA_6.a&cid=1337928848291

Die **Standardvertragsklauseln**; darin wird von der EU-Kommission festgelegt, unter welchen vertraglichen Bedingungen personenbezogene Daten aus dem EU-Raum in Drittstaaten überlassen und übermittelt werden dürfen.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF

Die **Artikel 29 Datenschutzgruppe**, bestehend aus leitenden Mitgliedern der nationalen Datenschutzbehörden, hat die bestehende EU-Richtlinie bezüglich einiger Themen konkretisiert und interpretiert. Dabei sind zahlreiche wertvolle Arbeitspapiere und Stellungnahmen entstanden, die zwar nicht rechtlich bindend sind, aber hilfreich für die Argumentation. (Die gesamten Dokumente finden sich unter:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm)

Die für den ArbeitnehmerInnen-Datenschutz wichtigsten sind:
Stellungnahme zur Verarbeitung personenbezogener Daten von Beschäftigten (2001)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48de.pdf

Empfehlung zu Beurteilungsdaten von Beschäftigten (2001):
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp42de.pdf

Arbeitsdokument zur Überwachung und Kontrolle der elektronischen Kommunikation von Beschäftigten (2002):
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_de.pdf

Stellungnahme zu verbindlichen unternehmensinternen Regelungen (2005):
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_de.pdf

Häufig gestellte Fragen zu den Standardvertragsklauseln (2012):
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf

Eine alte, aber die einzige international vergleichende Studie zu gesetzlichen Datenschutzvorgaben innerhalb der EU von Frank Hendrickx (2002): **"Protection of workers' personal data in the European Union"**:
http://ec.europa.eu/employment_social/labour_law/docs/dataprotection_hendrickx_combinedstudies_en.pdf
Für den internationalen Vergleich ist diese englisch sprachige Werk gut geeignet.

Weltweit:
Die **us-amerikanischen Safe-Harbor-**Bestimmungen des Handelsministeriums sowie die jeweils aktuellen Firmen, die sich Safe- Harbor unterworfen haben, findet man unter:
http://www.export.gov/safeharbor/

Der Code der **Internationalen Arbeitsorganisation** (ILO) zum Schutz von ArbeitnehmerInnen-Daten. Auch wenn der Vorschlag der ILO aus dem Jahr 1997 stammt, enthält diese englisch sprachige Publikation nach wie vor aktuelle Tipps:
http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf

INTERESSENGEMEINSCHAFTEN

- sind offene und junge Strukturen
- ermöglichen beruflichen Erfahrungsaustausch
- intensivieren die Verknüpfung von Gesellschaft und Gewerkschaft
- demokratisieren die Gewerkschaft
- sind ein neues Element gewerkschaftlicher Kultur
- organisieren Menschen nach ihrer beruflichen Situation
- wählen ihre VertreterInnen in Direktwahlen auf Bundes- und Regionalebene
- entsenden Delegierte in die höchsten GPA-djp-Gremien
- bringen Anregungen für Kollektivvertragsverhandlungen
- geben Anstoß für neue Betätigungsfelder von Gewerkschaften
- sind ein Spiegelbild gesellschaftlicher Veränderungen

INTERESSENGEMEINSCHAFTEN BIETEN

- den eingetragenen Mitgliedern ein Informationsnetz (Newsletter elektronisch bzw. per Post), um wichtige berufsbezogene Neuerungen, Hinweise und Probleme direkt zu vermitteln und umgekehrt deren Fragen und Wünsche aufzugreifen
- den Mitgliedern und den BetriebsrätInnen spezielle Dienstleistungen und Informationsmaterialien an
- mit ihren Informationen an Eingetragene, die noch nicht Gewerkschaftsmitglieder sind, eine gute Vorarbeit, die Kompetenzen und den Mehrwert der Gewerkschaft für die Mitgliederwerbung zu nutzen
- mit der Website www.gpa-djp.at/interesse eine Informations- und Austauschplattform für berufsspezifische Interessen und Fragen.

IG EXTERNAL

- ist die Interessengemeinschaft aller außerhalb des Betriebes tätiger ArbeitnehmerInnen (Außendienst, Mobildienste, Dienstreise, Montage und Entsendung) und widmet sich den damit verbundenen spezifischen Fragestellungen

- bietet unter anderem die folgenden spezifischen Produkte:

  - Airbags – Ratgeber für die Arbeit außerhalb des Betriebes
  - Broschüre »Die Vielfalt der Berufe außerhalb des Betriebes«
  - Sammelmappe zur steuerlichen Geltendmachung von Autokosten
  - Checkliste Dienstfahrzeuge
  - setzt sich für ein faires kostendeckendes Kilometergeld sowie für angemessene Regelungen bei Dienstfahrzeugen ein
  - gibt Anregungen, wie Außen- und Mobildienst in den Kollektivverträgen besser berücksichtigt werden kann: Broschüre »Wir machen die Kollektivverträge gemeinsam mobil«
  - Eintragung und Informationen unter **www.gpa-djp.at/external**

NOTIZEN

NOTIZEN

JETZT Mitglied werden!

Familienname ..... Vorname ..... ❒ Frau ❒ Herr

Geburtsdatum | | | | | | | | | Titel..... Geburtsname.....

Straße/Haus-Nr. ..... PLZ/Wohnort.....

Telefonisch erreichbar..... eMail.....

❒ Angestellte/r ❒ Lehrling ❒ Werkvertrag ❒ geringfügig beschäftigt ❒ Freier Dienstvertrag ❒ Selbstständig (Gewerbeschein)
❒ Zeitarbeitskraft ❒ SchülerIn ❒ StudentIn ❒ dzt. ohne Beschäftigung ❒ Zweitmitgliedschaft ❒ FacharbeiterIn

Derzeitige Tätigkeit ..... ❒ Ich war bereits Mitglied der Gewerkschaft von/bis.....

Beschäftigt bei Firma (bzw. Schule/Universität)..... Dienstort .....

Anschrift .....

Branche .....

Nur ankreuzen wenn ein Betriebsabzug gewünscht wird:

❒ **Betriebsabzug** – da in meinem Betrieb ein Betriebsabzug möglich ist, erkläre ich mich einverstanden, dass mein Gewerkschaftsbeitrag durch den Arbeitgeber (Dienstgeber) von meinem Gehalt/Lohn, meiner Lehrlingsentschädigung abgezogen wird. Ich ermächtige den Arbeitgeber, alle im Zusammenhang mit der Betragseinhebung erforderlichen personenbezogenen Daten im Sinne des DSG § 18 (1) bzw. § 7 (1) an die GPA-djp zu übermitteln.

Die Beitragszahlung erfolgt mit SEPA Lastschrift-Mandat (Bankeinzug)

❒ Ich ermächtige die GPA-djp, Zahlungen von meinem Konto mittels SEPA-Lastschrift einzuziehen. Ich kann innerhalb von 8 Wochen, beginnend mit dem Belastungsdatum, eine Rückerstattung verlangen.

Höhe des monatlichen Beitrages: **EUR** | | | | | |

❒ monatlich ❒ alle 2 Monate ❒ jedes Quartal ❒ 1/2 jährlich ❒ jährlich (Schüler-/StudentInnen, Zweitmitgliedschaft)

IBAN | | | | | | | | | | | | | | | | | | | | | |

BIC | | | | | | | | |

Ihre Angaben werden **streng vertraulich** behandelt und unterliegen dem **Datenschutz**. Nach Zusendung Ihrer Anmeldebestätigung haben Sie unter Verwendung Ihrer Mitgliedsnummer die Möglichkeit, sämtliche für Sie wichtigen Informationen wie Kollektivvertrag, Informationen zu aktuellen Themen, Aktivitäten unserer Interessengemeinschaft, etc., einzuholen. Unsere Internetadresse: **www.gpa-djp.at**

Der monatliche Mitgliedsbeitrag beträgt 1% des Bruttogehaltes, bis zu einem Maximalbeitrag (siehe www.gpa-djp.at/mitgliedsbeitrag), der jährlich angepasst wird. Der Mitgliedsbeitrag ist steuerlich absetzbar. Meine Finanzamtsbestätigung finde ich ab Ende Jänner zum Download unter **www.gpa-djp.at**. Ihre Angaben werden streng vertraulich behandelt.

| | | | | | |

Beitrittsmonat/-jahr

.....

Datum/Unterschrift

(Diese Unterschrift gilt auch als Berechtigung für eine evtl. oben angekreuzte SEPA-Lastschrift.)

WerberIn-Mitgliedsnummer: .....

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

1030 Wien, Alfred-Dallinger-Platz 1, Service-Hotline: +43 (0)5 0301-301, Fax: +43 (0)5 0301-300
eMail: service@gpa-djp.at, DVR 0046655, ZVR 576439352, CID: AT48ZZZ00000006541

mitmachen – mitreden – mitbestimmen

IG INTERESSEN GEMEINSCHAFTEN GPA-djp

Interessengemeinschaften der GPA-djp bringen Menschen mit ähnlichen Berufsmerkmalen zusammen. Zum Austauschen von Erfahrungen und Wissen, zum Diskutieren von Problemen, zum Suchen kompetenter Lösungen, zum Durchsetzen gemeinsamer beruflicher Interessen.

Mit Ihrer persönlichen Eintragung in eine oder mehrere berufliche Interessengemeinschaften

>> erhalten Sie mittels Newsletter (elektronisch oder brieflich) regelmäßig Informationen über Anliegen, Aktivitäten und Einladungen für Ihre Berufsgruppe;

>> können Sie Ihre beruflichen Interessen auf direktem Weg in die Kollektivvertragsverhandlungen Ihres Branchenbereichs einbringen;

>> erschließen Sie sich Mitwirkungsmöglichkeiten an Projekten, Bildungsveranstaltungen, Kampagnen, Internet-Foren und anderen für Ihre Berufsgruppe maßgeschneiderten Veranstaltungen, auch auf regionaler Ebene;

>> nehmen Sie von der Interessengemeinschaft entwickelte berufsspezifische Dienstleistungen und Produkte in Anspruch (Fachberatung auf regionaler Ebene, Bücher, Broschüren und andere Materialien);

>> beteiligen Sie sich an demokratischen Direktwahlen Ihrer beruflichen Vertretung auf Bundesebene sowie regionaler Ebene und nehmen dadurch Einfluss auf die gewerkschaftliche Meinungsbildung und Entscheidung.

www.gpa-djp.at/interesse

Interessengemeinschaften

Ihr Zusatznutzen ohne Extrakosten

IG PROFESSIONAL für GeschäftsführerInnen, TeamleiterInnen, KonstrukteurInnen, DirektorInnen, TechnikerInnen, WissenschaftlerInnen, Meister-Innen, freiberufliche ManagerInnen, AbteilungsleiterInnen, ProjektleiterInnen, ÄrztInnen, SpezialistInnen auf anderen Gebieten - kurz für FachexpertInnen und Führungskräfte

IG FLEX für WerkvertragnehmerInnen, freie DienstvertragnehmerInnen und GewerbescheininhaberInnen ohne eigeneAngestellten

IG SOCIAL für Alten-, Kranken-, BehindertenbetreuerInnen, SozialarbeiterInnen, aber auch Angestellte in sozialen Berufen

IG IT für IT-SpezialistInnen, MitarbeiterInnen bei EDV-Projekten, im Internet und neuen Medien sowie in der Telekommunikation

IG EDUCATION für ErwachsenenbildnerInnen, (freie) TrainerInnen, LehrerInnen an Fachhochschulen und Privatuniversitäten, Menschen in Beratungsberufen

IG EXTERNAL für AußendienstmitarbeiterInnen, ServicetechnikerInnen, mobile KrankenpflegerInnen, BaustellenleiterInnen, LeiterInnen internationaler Forschungsprojekte, ForstaufseherInnen oder KundenbetreuerInnen von Ver-sicherungen

IG MIGRATION für Menschen, die in Österreich ohne österreichische Staatsbürgerschaft leben bzw. diese erst während ihres Aufenthaltes erwerben, MitarbeiterInnen in Beratungsstellen, in Initiativen von MigrantInnen, ÖsterreicherInnen, die in einem fremden Land leben sowie Menschen, denen dieses Thema wichtig ist

IG POINT-OF-SALE für Menschen in Verkauf und Beratung (zB VerkäuferInnen, BankkundenbetreuerInnen, KundenbetreuerInnen, ...)

Ich möchte mich in folgende Interessengemeinschaften eintragen:

❒ IG PROFESSIONAL ❒ IG FLEX ❒ IG SOCIAL ❒ IG EDUCATION ❒ IG MIGRATION

❒ IG EXTERNAL ❒ IG IT ❒ IG POINT-OF-SALE

Dieses Service ist für mich kostenlos.

❒ Frau ❒ Herr Titel .....

Familienname ..... Vorname .....

Straße/Haus-Nr. ..... PLZ/Wohnort .....

Berufsbezeichnung. ..... Betrieb .....

Telefonisch erreichbar ..... eMail .....

.....
Datum/Unterschrift

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

Ihre Kontaktadressen der GPA-djp

Service-Hotline: 05 03 01-301

Gewerkschaft der Privatangestellten,
Druck, Journalismus, Papier
1030 Wien, Alfred-Dallinger-Platz 1
service@gpa-djp.at

Regionalgeschäftsstelle **Wien**
1030 Wien, Alfred-Dallinger-Platz 1

Regionalgeschäftsstelle **Niederösterreich**
3100 St. Pölten, Gewerkschaftsplatz 1

Regionalgeschäftsstelle **Burgenland**
7000 Eisenstadt, Wiener Straße 7

Regionalgeschäftsstelle **Steiermark**
8020 Graz, Karl-Morre-Straße 32

Regionalgeschäftsstelle **Kärnten**
9020 Klagenfurt, Bahnhofstraße 44/4

Regionalgeschäftsstelle **Oberösterreich**
4020 Linz, Volksgartenstraße 40

Regionalgeschäftsstelle **Salzburg**
5020 Salzburg, Markus-Sittikus-Straße 10

Regionalgeschäftsstelle **Tirol**
6020 Innsbruck, Südtiroler Platz 14-16

Regionalgeschäftsstelle **Vorarlberg**
6901 Bregenz, Reutegasse 11

www.gpa-djp.at

Für alle, die **mehr wollen!**

GPA djp
GEWERKSCHAFT DER PRIVATANGESTELLTEN
DRUCK – JOURNALISMUS – PAPIER

1030 Wien, Alfred-Dallinger-Platz 1, Telefon 05 0301-301, Fax 05 0301-300
www.gpa-djp.at - eMail: service@gpa-djp.at, DVR: 0046655, ÖGB ZVR-Nr.: 576439352