Artikel 26

Überwachung der Arbeitnehmer

[1] Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden.

[2] Sind Überwachungs- oder Kontrollsysteme aus anderen Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden.

1. Allgemeines

Mit dem Artikel 26 ArGV 3 wird der bereits in Artikel 328 OR statuierte Persönlichkeitsschutz der Arbeitnehmerinnen und Arbeitnehmer im öffentlichen Arbeitsrecht verankert. Unabhängig davon muss jederzeit sichergestellt sein, dass nicht gegen die Datenschutzgesetzgebung (Datenschutzgesetz, DSG, SR 235.1; Datenschutzverordnung, DSV, SR 235.11) und das Strafgesetzbuch (StGB, SR 311.0) verstossen wird. Diese Rechtsgrundlagen dienen dem Schutz der Persönlichkeit und sichern die Grundrechte von Personen; auch wenn es um die Bearbeitung von Personen-Daten geht. Die Arbeitnehmenden sind so öffentlich-rechtlich gegen die Verhaltensüberwachung geschützt. Es ist somit auch nicht zulässig, durch eine privatrechtliche Abmachung – beispielsweise durch ein Abkommen zwischen Arbeitgeber und Arbeitnehmenden oder deren Organisationen – von diesen Bestimmungen abzuweichen.

Die Einrichtung eines technischen Überwachungs- oder Kontrollsystems ist nur dann zulässig, wenn es aus anderen Gründen, z. B. für die Sicherheits-, Qualitäts- oder Leistungsüberwachung notwendig ist. Dabei muss der Persönlichkeits- und Gesundheitsschutz der Arbeitnehmenden so weit wie möglich gewahrt bleiben.

Die Ahndung betriebsinterner Straftaten ist grundsätzlich nicht Sache des Betriebes, sondern ausschliesslich der Polizei. Setzt sich ein Arbeitgeber darüber hinweg, sind in unzulässiger Weise erhobene Überwachungsdaten in einem Strafverfahren meistens nicht verwendbar.

Überwachungsanlagen können bei betroffenen Arbeitnehmenden erfahrungsgemäss unangenehme Gefühle bis hin zu gesundheitlichen Beeinträchtigungen auslösen. Hinzu kommt, dass damit auch das allgemeine Betriebsklima schlechter wird. Es liegt deshalb im Interesse aller Beteiligten, dass bei unumgänglichem Einsatz eines technischen Überwachungs- und Kontrollsystems dieses möglichst zurückhaltend eingesetzt wird.

Eine Möglichkeit besteht darin, die Überwachungs- und Kontrollsysteme nur im Abwesenheit der Arbeitnehmenden in Betrieb einzusetzen (z. B. Diebstahlüberwachungsanlagen, Einsatz nur, wenn notwendig etc.).

Verhalten und Leistung hängen oft stark voneinander ab. Entsprechend ist eine scharfe Abgrenzung zwischen (erlaubter) Leistungs- oder Sicherheits- und (unerlaubter) Verhaltensüberwachung in vielen Fällen nur schwer oder gar nicht möglich. In solchen Fällen muss ein Betrieb sein überwiegendes Interesse (Sicherheit vs. Persönlichkeits- & Gesundheitsschutz) und die Verhältnismässigkeit (nur so viele Personendaten erfassen wie absolut notwendig) seines geplanten Kontroll- und Überwachungssystems prüfen und schriftlich begründen (→ SECO-Checkliste «Technische Überwachung am Arbeitsplatz»). Diese Begründung ist dem zuständigen kantonalen Arbeitsinspektorat auf Verlangen vorzulegen.

Beispiele erlaubter Überwachung zwecks Optimierung der Leistung:

- das automatische Registrieren der Anzahl oder Qualität produzierter Teile;
- das Registrieren der Anzahl entgegengenommener Anrufe in einem Callcenter;
- die Fahrstreckenaufzeichnung von Firmenfahrzeugen zur ökonomischen Wegoptimierung durch Disponenten.

Bei der Leistungserfassung ist die Verhältnismässigkeit zu wahren.

Um zu wissen, ob die Einrichtung eines Überwachungs- oder Kontrollsystems im Hinblick auf Art. 26 ArGV 3 zulässig ist oder nicht, muss zuerst abgeklärt werden, ob alle drei nachstehenden Bedingungen erfüllt sind:

a) Vorliegen eines klar überwiegenden anderen Interesses (z. B. Sicherheit des Personals, des Betriebs oder Produktionsoptimierung);
b) Verhältnismässigkeit zwischen dem Interesse des Arbeitgebers an einer Überwachung von für den Betrieb existentiell wichtigen Bereichen und dem Interesse der Arbeitnehmenden, nicht überwacht zu werden;
c) Mitwirkung der Arbeitnehmenden bezüglich Planung, Einrichtung und Einsatzzeiten der Überwachungs- und Kontrollsysteme sowie bzgl. Speicherdauer der erfassten Daten.

2. Absatz 1

Mit Überwachungs- und Kontrollsystemen sind alle technischen Systeme (optisch, akustisch, elektronisch etc.) gemeint, mit welchen durch technische Mittel Daten über das Verhalten von Arbeitnehmerinnen und Arbeitnehmern erfasst werden können.
Die Verhaltensüberwachung der Arbeitnehmenden beinhaltet jegliche Überwachung, die eine ständige (ununterbrochene) oder nicht ständige (kurzzeitig periodische oder stichprobenmässige) Kontrolle bestimmter Aktivitäten der Arbeitnehmenden in detaillierter Form ermöglicht.
Beispiele:

- Videokameras (in Arbeitsräumen oder Fahrzeugkabinen, Webcams etc.), die undeklariert aufnehmen können, was Mitarbeitende machen und wie sie dies tun;
- Mikrophone oder Telefone, mit welchen Gespräche der Arbeitnehmenden abgehört, aufgenommen oder deren Stimmen analysiert werden können;
- Satellitengestützte und andere Ortungssysteme, mit welchen die Position von Personen ständig verfolgt und aufgezeichnet werden kann;
- Informatikmittel, welche die computer- oder mobiltelefongestützten Aktivitäten von Arbeitnehmenden im Betrieb oder in deren Homeoffice überwachen (E-Mail, Spyware, Activity Tracker, App- oder Weblogs, Maus- oder Tastaturlogs etc.);
- Sensoren, die biometrische oder physiologische Daten von Arbeitnehmenden erfassen und auswerten (Gesichtserkennung, Stimmanalyse, Kopf-, Augen-, Pupillen-, Bewegungs- oder Muskelaktivität, Körpertemperatur, Atem- oder Herzfrequenz, Schweissemission etc.);
- Informatikmittel, die Instrumente der künstlichen Intelligenz (neuronale Netzwerke, Expertensysteme) für automatisierte Analysen und Auswertungen von mitarbeiterbasierten Daten verwenden (Seh-, Bewegungs-, Sprech- oder Kommunikationsmuster, psychologische Befunde etc.).

Nicht als technische Überwachungs- und Kontrollsysteme zur Verhaltensüberwachung gelten namentlich:

- Einrichtungen wie z. B. elektronische Badges für die Zutrittsregelung und Zeiterfassung in einem Betrieb;
- Technische Systeme zur Qualitätskontrolle, mit welchen z. B. die auf einer Anlage hergestellten Teile erfasst und verfolgt werden.

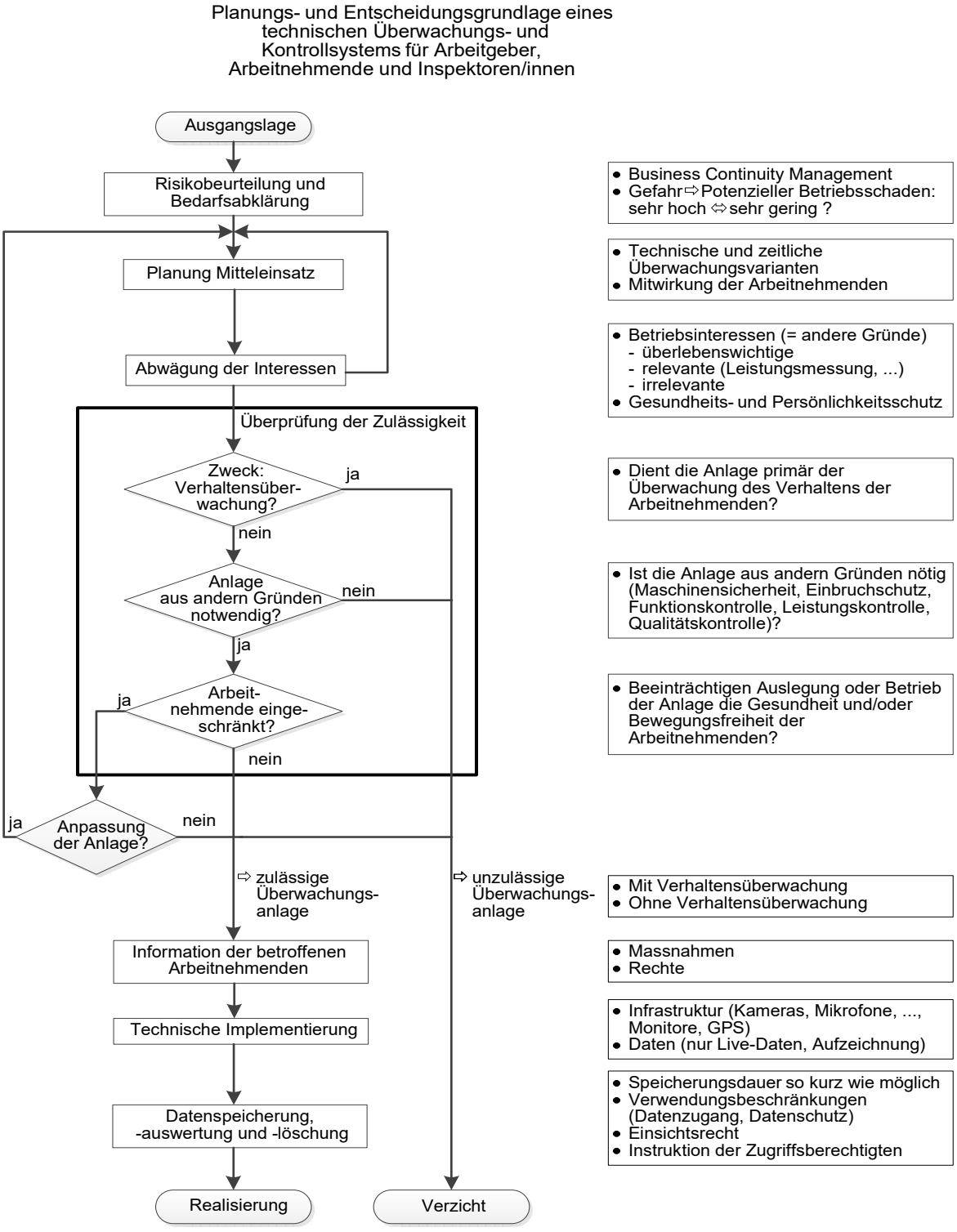

Abbildung 326-1: Empfohlene Planungs- und Entscheidungsgrundlage für ein neues Überwachungs- und Kontrollsystem.

3. Absatz 2

Technische Überwachungs- und Kontrollsysteme dürfen – sofern sie keine Verhaltensüberwachung des Personals ermöglichen – überall auf dem Firmengelände eingerichtet werden, wo es für den Betrieb wichtig ist und sich Personal nur selten und kurzzeitig aufhält. Zum Beispiel:

- ausserhalb der Gebäude, bei Parkplätzen und in Tiefgaragen;
- bei Zugängen, Eingängen, Durchgängen und Ausgängen;
- bei gefährlichen Maschinen und Anlagen;
- in Tresorräumen;
- bei gefährlichen Installationen im Freien;
- bei Lagern von gefährlichen Gütern.

Es muss von Fall zu Fall separat beurteilt und entschieden werden, ob ein technisches Überwachungs- und Kontrollsystem tatsächlich dem zu Beginn definierten Ziel dient.

3.1 Überwiegendes Interesse

Eine Interessensabwägung (Betriebsinteresse versus Persönlichkeitsschutz der Arbeitnehmenden) muss in jedem Einzelfall durchgeführt werden.
Als Betriebsinteresse ist insbesondere die Sicherheit der Arbeitnehmenden und von Dritten, die Sicherung von für den Betrieb überlebenswichtigen Betriebsgütern, die Datensicherheit und die Einhaltung von gesetzlichen Vorgaben anzuführen (z. B. Casinos, die obligatorisch mit Video-Überwachung ausgerüstet sein müssen gemäss dem 2. Abschnitt «Kameraüberwachung» der Spielbankenverordnung EJPD (SR 935.511.1)).
Wird bei der Interessensabwägung das Betriebsinteresse höher als der Persönlichkeitsschutz des Arbeitnehmenden eingestuft, handelt es sich um ein sogenannt überwiegendes Interesse.
Je wichtiger ein zu überwachendes Gut des Betriebes für seine Existenz ist, desto eher kann eine Überwachung der Arbeitnehmenden, die Zugang zu oder Umgang mit diesem Gut haben, in Kauf genommen werden.

Beispiele für ein überwiegendes Betriebsinteresse:

- Videoüberwachung eines Tresorraums in einer Bank/einem Schmuckgeschäft;
- Videoüberwachung in Goldschmiedewerkstätten/Kunstgalerien;
- GPS, das den Aufenthaltsort z. B. eines Fahrzeuges präzise ermittelt (Chauffeure mit Personen- oder Gütertransporten (z. B. Bargeld, Gefahrstoffe, Verderbliches), sowie Dienstleister (z. B. Taxi, Pannendienste, Servicemonteure etc.).

3.2 Verhältnismässigkeit (Interessen und Mittel)

Vor einer direkten Überwachung durch technische Mittel ist durch den Betrieb jedoch abzuklären, ob die Sicherheit dieses Guts nicht auf eine andere Weise sichergestellt werden kann, welche eine Überwachung der Arbeitnehmenden ausschliesst (Verhältnismässigkeit des Mitteleinsatzes).

Dabei sind verschiedene technische und zeitliche Überwachungs- und Kontrollvarianten zu prüfen – dies soweit möglich unter Vermeidung einer Videoüberwachung oder anderen vergleichbar stark in die Persönlichkeitssphäre eingreifenden technischen Mitteln.
Nachdem festgestellt wurde, dass ein legitimes Interesse an einer Überwachung besteht, stellt sich bei der Auswahl der Mittel folgende Frage: Wahrt das Überwachungs- und Kontrollsystem die Gesundheit und den Persönlichkeitsschutz der Arbeitnehmenden? Wenn nein, muss nach einem anderen Mittel gesucht werden, das diese Voraussetzung erfüllt

Der Grundsatz der Verhältnismässigkeit ist dann eingehalten, wenn

- das Betriebsinteresse an einer Überwachung wichtiger ist als das Interesse der Arbeitnehmenden am Schutz ihrer Persönlichkeit;
- das Überwachungs- und Kontrollsystem so gestaltet und eingesetzt wird, dass eine Gefährdung der Persönlichkeit des Arbeitnehmenden in höchstmöglichem Masse begrenzt wird.

Damit ein Betrieb, der Kontroll- und Überwachungssysteme einsetzen will, nachweisen kann, dass diese die Gesundheit und den Persönlichkeitsschutz der Arbeitnehmenden nicht beeinträchtigen, erstellt er mit Vorteil ein Konzept über die Funktionsweise sowie die Art und den Zeitpunkt von Aufzeichnungen dieser Systeme.

Beispiele für einen adäquaten Mitteleinsatz:

- Eine Personenlokalisierung oder Zutrittsregelung zu gewissen Teilen des Betriebes mittels Badges, Biometrie etc. ist einer Videoüberwachung der Arbeitnehmenden vorzuziehen. Bei den WC ist eine Türschliess-Überwachungsanlage jedoch unzulässig.
- Bei EDV-Systemen und -netzwerken sind zahlreiche Überwachungs- und Kontrollmöglichkeiten vorhanden. Die Benutzerinnen und Benutzer sind vorgängig darüber in Kenntnis zu setzen, in welcher Form eine allfällige Überwachung von rein geschäftsrelevanten Daten erfolgt. Die Nutzung des Internets ist betriebsintern zu regeln.
- Telefonanlagen, mit denen Gespräche zur Leistungskontrolle bei Telefonverkäufen oder zu Schulungszwecken mitgehört und/oder aufgezeichnet werden können, sind zulässig, wenn die Personen, deren Gespräche mitgehört oder aufgezeichnet werden, damit einverstanden sind und jeweils unmittelbar darüber in Kenntnis gesetzt werden, z. B. durch ein optisches oder akustisches Signal. Die Aufzeichnung von telefonischen Gesprächen unterliegt strengen Voraussetzungen (siehe im Abschnitt 3.3);
- Dienen Kontroll- und Überwachungsanlagen dem Schutz vor Kundendiebstählen, sind Mitarbeitende über betriebene technische Kontroll- und Überwachungsanlagen zu informieren (siehe Ziffer 3.4 Information und Anhörung der Arbeitnehmenden). Die Videokameras sind so zu positionieren und einzustellen, dass Mitarbeitende praktisch nicht miterfasst und aufgezeichnet werden. Die Positionen und Bildausschnitte sollen mit dem Personal besprochen werden, damit dieses den überwachten Bereich kennt. In den Abbildungen 326-2 und 326-3

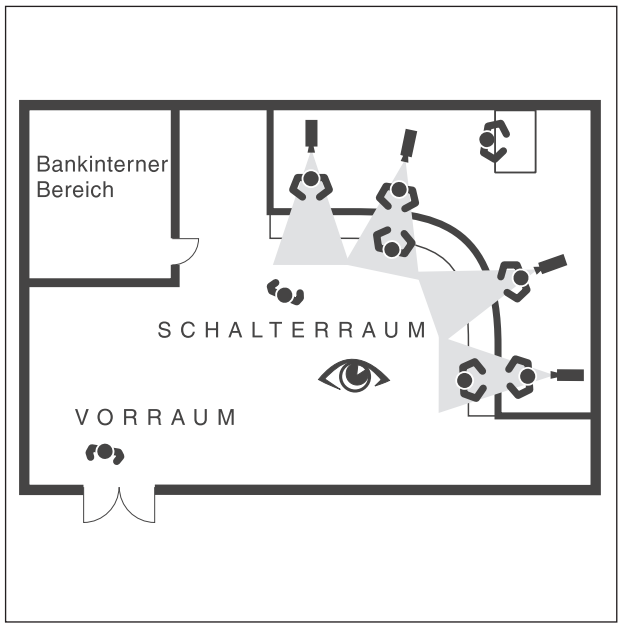

Abbildung 326-2: Anordnung von Kameras und deren Überwachungsbereich in einer «offenen» Bankschalterhalle ohne Abtrennung zwischen Kunden und Personal (Grundriss)

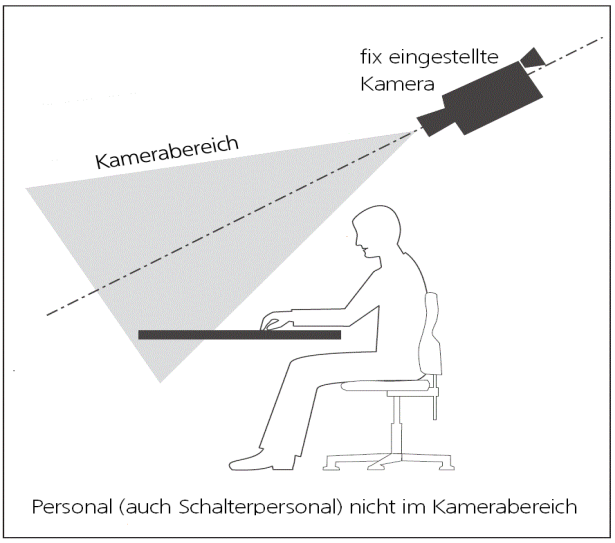

Abbildung 326-3: Überwachung einer «offenen» Bankschalterhalle (Schnitt)

sind die Anordnung von Kameras und deren Überwachungsbereich in einer Bankschalterhalle dargestellt, bei der Kundschaft und Personal nicht durch Sicherheitsglas voneinander abgetrennt sind. Das Bankpersonal hält sich dabei nur ausnahmsweise im Kamerabereich auf.

- Dienen Videoüberwachungsanlagen bei komplexen Produktionsanlagen primär für die Produktionssteuerung und/oder der Sicherheitsüberwachung, so gilt es, die Kameraposition und den Bildausschnitt fixer und beweglicher Kameras so zu wählen, dass ausschliesslich der Produktionsprozess und das Personal höchstens ausnahmsweise erfasst werden. Wäre aus Sicherheitsgründen die Überwachung der Arbeitnehmenden selbst nötig, z. B. um sie in einer Steuerzentrale in gefährlichen Situationen zu schützen, sind alternative Möglichkeiten zu prüfen, beispielsweise das regelmässige Quittieren einer Meldung.

Die Zeitdauer des eingeschalteten Kontroll- und Überwachungsvorgangs in Bereichen mit Arbeitnehmenden ist auf ein Minimum zu beschränken (siehe auch Ziffer 3.3 Datenschutz und Schutz der Persönlichkeit), indem dieser z. B. auf kritische Phasen reduziert wird oder indem für die Arbeitnehmenden die Möglichkeit besteht, ihn selber zu ihrem Schutz einzuschalten (z. B. Kameras mit Mikrophonen, welche Mitarbeitende bei Gefahr von Gewalt in einem Tankstellenshop, Verkaufsgeschäft oder Restaurant einschalten).

3.3 Datenschutz und Schutz der Persönlichkeit

Das Erheben, Bearbeiten und Speichern von Personendaten müssen gemäss der Datenschutzgesetzgebung (siehe Ziffer 1 Allgemeines) erfolgen.
Das Bearbeiten von Personendaten unterliegt dem Grundsatz von Treu und Glauben. Das bedeutet in diesem Zusammenhang, dass ein Bearbeiten der Personendaten für die betroffenen Personen stets auf transparente Art und Weise zu erfolgen hat. Die betroffenen Personen müssen vorgängig ausführlich über Art, Ziel und Zweck der Bearbeitung informiert werden.
Das Prinzip der Verhältnismässigkeit ist stets zu berücksichtigen. Es dürfen demzufolge nur sachdienliche oder nützliche Personendaten bearbeitet werden. Diese müssen nach einer möglichst kurzen, im Voraus festgelegten Zeitspanne, gelöscht werden. Der Zugang zu den Datensammlungen (bearbeitete Personendaten) ist betriebsintern zu regeln. Er muss auf die Personen beschränkt werden, welche zur Auswertung befugt sind. Es ist unzulässig, nach erfolgter Kontrolle die Daten aus Sicherheitsgründen zu archivieren.
Die Verwendung der ICT (Information and Communication Technology), die Datenerfassung und deren Auswertung ist betriebsintern zu regeln.
Es ist auch ein betriebsinternes Reglement zu erstellen, welches den Arbeitnehmenden transparent darüber Aufschluss gibt, welche Rechte und Pflichten ihnen beim Einsatz von Überwachungs- und Kontrollsystemen zustehen (z.B. Telefonie, Internet-Telefonie und Informatik) und wie die betriebsinterne Kontrolle und Überwachung erfolgt.

- Nutzung der betriebsinternen Telefonie: Die Aufzeichnung von telefonischen Gesprächen unterliegt strengen Voraussetzungen. Ein Verbot von Privatgesprächen darf nicht via das Abhören von Gesprächen kontrolliert werden, sondern indem beispielsweise Aussenverbindungen durch eine Zentrale vermittelt werden oder nur von bestimmten Anschlüssen aus möglich sind. Besteht ein solches Verbot, muss den Arbeitnehmenden die Möglichkeit gegeben werden, private Gespräche von einem unbeaufsichtigten betriebsinternen Anschluss aus zu führen. Der Arbeitgeber kann verlangen, dass längere private Telefongespräche während den Pausen und mit einem privaten Mobiltelefon zu erfolgen haben. Sofern das Führen privater Telefongespräche nicht generell untersagt ist, dürfen die von Arbeitnehmenden dabei angewählten Anschlüsse nicht aufgezeichnet werden. Allenfalls dürfen die ersten Ziffern der Teilnehmernummern aufgezeichnet werden,

und dies nur aus betrieblichen Gründen (z.B. um Rechnung zu stellen). Die Arbeitnehmenden müssen vorgängig darüber informiert sein.

- Nutzung der Informatik: Die Arbeitnehmenden müssen transparent darüber unterrichtet sein, welche Nutzungsregeln sie im Bereich der Informatik zu befolgen haben und in welchen Bereichen der Arbeitgeber Überwachungs- und Kontrollsysteme einsetzen darf. Die Arbeitnehmenden müssen insbesondere über die internen Regeln zur Nutzung des Internets und des E-Mailverkehrs (Account) in Kenntnis gesetzt werden. Dazu gehören auch die Verhaltensmassnahmen des Arbeitgebers bei Zugriff auf die E-Mails von abwesenden Arbeitnehmenden (Krankheit, Ferien usw.).

Es bleibt daran zu erinnern, dass Aufzeichnungen des akustischen und visuellen Hintergrunds (z. B. auf Baustellen, im Eingangsbereich des Betriebs, in Betriebshallen und -räumen usw.) ohne Zustimmung der betroffenen Personen einen Verstoss im strafrechtlichen Sinne gemäss Art. 179bis bis 179^{quater} Strafgesetzbuch darstellen kann. Überwachte Bereiche (Video, akustisch usw.) sind klar als solche zu kennzeichnen.

3.4 Information und Anhörung der Arbeitnehmenden

Wenn Überwachungs- und Kontrollsysteme erforderlich sind, die neben ihrem eigentlichen Zweck auch noch für die Überwachung der Arbeitnehmenden eingesetzt werden können, haben die Arbeitnehmenden ein Anrecht auf Information und Anhörung durch den Arbeitgeber gemäss den Artikeln 5 und 6 ArGV 3.
Der Arbeitgeber muss Entscheide in Bezug auf Fragen des Gesundheitsschutzes begründen, wenn er den Einwänden der Arbeitnehmenden oder deren Vertretung im Betrieb nicht oder nur teilweise Rechnung trägt (vgl. Wegleitung zum Art. 48 ArG).

3.5 Einsicht in betriebliche Unterlagen und Daten

Den Vollzugsbehörden des Arbeitsgesetzes muss auf deren Verlangen hin Einsicht in sämtliche Unterlagen und Daten der betriebenen Kontroll- und Überwachungssysteme gewährt werden.
Im Einvernehmen mit dem Inhaber der Datensammlung oder auf dessen Vorschlag hin kann eine von der Datenerfassung betroffene Person ihre Daten an Ort und Stelle einsehen. Die Auskunft kann auch mündlich erteilt werden, wenn die betroffene Person eingewilligt hat und vom Inhaber oder der Inhaberin identifiziert worden ist.

Weiterführende Informationen

Aktuelle Rechtsprechung zum Artikel 26 ArGV 3:

- BGE 130 II 425
  Das Bundesgericht hält fest, «dass ein Überwachungssystem gemäss Artikel 26 ArGV 3 verboten ist, wenn es ausschliesslich oder hauptsächlich darauf abzielt, das Verhalten der Arbeitnehmerinnen und Arbeitnehmer als solches zu überwachen. Andererseits ist seine Verwendung nicht verboten, wenn es zwar objektiv eine solche Überwachungswirkung hat, aber aus legitimen Gründen gerechtfertigt ist, wie etwa aus Sicherheitsgründen oder aus Gründen, die mit der Organisation oder Planung der Arbeit oder mit der Natur des Arbeitsverhältnisses selbst zusammenhängen. Allerdings muss das gewählte Überwachungssystem in Anbetracht der Gesamtheit der Umstände als verhältnismässiges Mittel zum verfolgten Ziel erscheinen und die betroffenen Arbeitnehmer müssen vorab über seine Verwendung informiert worden sein».
- BGE 145 IV 42
  Eine Überwachung, die von der Polizei mit Zustimmung des Arbeitgebers installiert wurde, stellt eine Zwangsmassnahme dar, deren Ergebnis mangels Genehmigung durch das Zwangsmassnahmengericht mit Unverwertbarkeit zu belegen ist.

- BGE 143 II 443
  Kontrolle der Internetnutzung am Arbeitsplatz oder des dienstlichen Mobiltelefons. Die personenbezogene Auswertung namentlich aufgezeichneter Daten hat in unzulässiger Weise stattgefunden. Weil ein unzulässiges Beweismittel vorliegt, ist eine Interessenabwägung vorzunehmen. In diesem Fall durfte der Arbeitgeber das Resultat unrechtmässig erlangter Informationen verwerten. Die fristlose Auflösung des Arbeitsverhältnisses erfolgt aus schwerwiegenden Gründen, nachdem der Angestellte nicht erlaubte Internetseiten übermässig häufig besucht hat. Sie stellt keine Verletzung des Verhältnismässigkeitsgrundsatzes dar.
- BGE 139 II 7
  Einsatz von Spyware (Installation von Spyware zur Überwachung der Computeroperationen eines Beamten; heimlicher Einsatz von Spyware zur Überprüfung des Verdachts, dass ein Beamter die ihm zur Verfügung gestellten Computerressourcen für Zwecke missbraucht, die nichts mit seinen Amtspflichten zu tun haben). Mit der Verneinung der Verwertbarkeit eines auf diese Weise widerrechtlich erlangten Beweismittels fällt die Grundlage für eine Entlassung dahin.
- 4A_518/2020 vom 25.08.2021
  Art. 328 Abs. 1 OR sieht vor, dass der Arbeitgeber im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers schützt und achtet. Gemäss Art. 328b OR darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie die Eignung des Arbeitnehmers für das Arbeitsverhältnis betreffen oder für die Durchführung des Arbeitsvertrages erforderlich sind. Eine Arbeitgeberin, die auf die privaten Nachrichten eines Arbeitnehmers zugreift, verletzt die Persönlichkeit des Arbeitnehmers.

Publikationen

Weitere Erläuterungen zu Themen im Zusammenhang mit der technischen Überwachung von Arbeitnehmenden (Überwachung am Arbeitsplatz aus der Sicht des Datenschutzes; Überwachung der Internet- und E-Mail-Nutzung; Telefon- und Videoüberwachung; Sicherheitsmassnahmen bei Audio- und Videokonferenzen) sowie diversen Publikationen befinden sich in der Website des Eidg. Datenschutzbeauftragten EDÖB zu finden: www.edoeb.admin.ch