

# Mitarbeiterüberwachung – was ist erlaubt?

- Taschenkontrollen / Torkontrollen
- Telefonüberwachung
- GPS Daten
- Videoüberwachung
- E-Mail Kontrolle





- Um Eigentums- und Vermögensdelikte durch Arbeitnehmer zu vermeiden, hat der Arbeitgeber die Möglichkeit, Taschenkontrollen durchzuführen.

BAG, 09.07.2013 – 1 AZR 275/12 –:

*„Die Taschenkontrollen greifen allerdings in die **Privatsphäre der betroffenen Arbeitnehmer** ein. Diese umfasst Angelegenheiten, die wegen ihres Informationsinhalts typischerweise als „privat“ eingestuft werden, weil ihre öffentliche Erörterung oder Zurschaustellung als unschicklich gilt, das Bekanntwerden als peinlich empfunden wird oder nachteilige Reaktionen der Umwelt auslöst ...*

*Der Inhalt mitgeführter Taschen oder auch von Mantel- und Jackentaschen ist in diesem Sinne privat. Ihr Inhaber möchte die darin mitgeführten Gegenstände typischerweise nicht ohne seine Einwilligung Dritten gegenüber zeigen. Darüber hinaus wird durch Taschenkontrollen auch das Ehrgefühl von Arbeitnehmern beeinträchtigt, denn hiermit bringt der Arbeitgeber zum Ausdruck, dass er ihnen nicht uneingeschränkt vertraut.“*

- BAG, 09.07.2013 – 1 AZR 275/12 –
- „(2) Die Beeinträchtigungen des Persönlichkeitsrechts durch die in der BV-Torkontrolle vorgesehenen Taschenkontrollen genügen jedoch den Anforderungen des **Verhältnismäßigkeitsgrundsatzes**.
- (a) Die in der BV-Torkontrolle vereinbarten Taschenkontrollen sind **geeignet**, das Eigentum der Arbeitgeberinnen zu schützen. Da hierdurch Diebstähle aufgedeckt werden können und durch die Auswahl der zu kontrollierenden Arbeitnehmer über einen **Zufallsgenerator** die Beschäftigten jederzeit damit rechnen müssen, kontrolliert zu werden, entfaltet dieses Überwachungssystem repressive wie präventive Wirkung. Dieser Annahme steht nicht entgegen, dass die Anzahl der bislang aufgedeckten Diebstähle gering ist. Dies kann ohne Weiteres auch auf der abschreckenden Wirkung der Kontrollen beruhen.
- (b) Die Taschenkontrollen sind **erforderlich**. Andere, gleich wirksame und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel stehen den Betriebsparteien zum Schutz des Eigentums der Arbeitgeberinnen vor Diebstählen nicht zur Verfügung.

*Eine Kameraüberwachung bei Verlassen des Betriebsgeländes wäre nicht gleich wirksam, da mitgeführte Gegenstände in Taschen oder Behältnissen nicht erkannt werden könnten. Eine Videoüberwachung in den Arbeitsbereichen würde das allgemeine Persönlichkeitsrecht der Arbeitnehmer stärker beeinträchtigen, da diese einer dauerhaften Beobachtung ausgesetzt wären. Ein Verbot des Mitführens von Taschen auf das Betriebsgelände wäre nicht in gleicher Weise geeignet, Diebstähle zu verhindern, weil hierdurch die Mitnahme der eher kleinräumigen Parfum- und Kosmetikprodukte in Bekleidungstaschen nicht verhindert werden kann.*

*(c) Die in Nr. 4 der BV-Torkontrolle vorgesehenen Kontrollmaßnahmen tragen dem Gebot der **Verhältnismäßigkeit im engeren Sinn** Rechnung. Die Arbeitgeberinnen haben unbestritten vorgetragen, im Rahmen von Inventuren sei festgestellt worden, dass von Oktober 2009 bis September 2010 insgesamt 1890 „Stück Parfüm“ zu einem Wert zwischen 20 Euro und 250 Euro entwendet worden seien. Bei einem gemittelten Wert von 135 Euro ergibt sich hieraus ein Schaden in einer Größenordnung von ca. 250 000 Euro... Die Auswahl der zu kontrollierenden Person erfolgt nach Nr. 4.2 BV-Torkontrolle durch einen **Zufallsgenerator**. Dies vermeidet eine Stigmatisierung, da hierdurch für alle Arbeitnehmer klargestellt ist, dass die Kontrolle nicht durch ein Verhalten der jeweils kontrollierten Person veranlasst ist. Die Durchführung der Kontrollmaßnahmen in dem von außen nicht einsehbaren Pförtneraum gewährleistet, dass **andere Arbeitnehmer die Kontrolle nicht beobachten können**.*

*Des Weiteren ist die Kontrollintensität in Nr. 4.3 BV-Torkontrolle gestaffelt und abhängig von konkreten Verdachts Umständen.*

*Zunächst wird eine Sichtkontrolle der mitgeführten Behältnisse vorgenommen.*

*Nur in begründeten Verdachtsfällen ist die Leerung sämtlicher Kleidertaschen vorgesehen, im Falle der Weigerung, die Durchführung dieser Kontrollmaßnahme durch die Polizei.*

*Der Kontrollzyklus ist angemessen. Pro Jahr werden an 30 Tagen insgesamt 86 Arbeitnehmer kontrolliert.*

*Dass die Kontrolle „durch dazu bestimmte Personen“ – gegebenenfalls also auch externe Sicherheitsmitarbeiter – und ohne Hinzuziehung eines Betriebsratsmitglieds durchgeführt wird, ist nicht zu beanstanden. Es ist nicht ersichtlich, dass eine Kontrolle durch eigene Mitarbeiter und in Anwesenheit eines Betriebsratsmitglieds das Persönlichkeitsrecht der Arbeitnehmer weniger beeinträchtigt.“*



## Taschenkontrollen / Torkontrollen

- Obwohl es einen Eingriff in die Privatsphäre darstellt, sind Taschenkontrollen unter bestimmten Voraussetzungen zulässig:
- Es besteht ein dringender Verdacht, dass Ware entwendet worden ist.
- Es wird nur stichprobenartig kontrolliert. Es dürfen immer nur verschiedene Mitarbeiter nach dem Zufallsprinzip kontrolliert werden. Ein bestimmter Mitarbeiter darf nur dann kontrolliert werden, wenn ein schwerwiegender Verdacht gegen ihn besteht.
- Taschenkontrollen unterliegen der Mitbestimmung des Betriebsrats gemäß § 87 Absatz 1 Nr. 1 BetrVG. Es bedarf mithin einer Betriebsvereinbarung. Bei Verletzung dieses Mitbestimmungsrechts hat der Betriebsrat einen Unterlassungsanspruch.
- Wichtig bei der Taschenkontrolle ist, dass lediglich Bereiche kontrolliert werden dürfen, die sich nicht am Körper befinden. Hosen- und Jackentaschen dürfen also nur im Ausnahmefall kontrolliert werden, wenn ein begründeter Verdacht besteht, dass der Arbeitnehmer Ware entwendet hat.
- Dies kann jedoch nicht vor allen anderen Mitarbeitern erfolgen, sondern muss an einem nicht einsehbaren Ort geschehen.

## Ausflug: Heimliche Schrankkontrolle

- Das BAG hat mit Urteil v. 20.06.2013 – 2 AZR 546/12 –ausgeurteilt:

*„Arbeitnehmer müssen gleichwohl darauf vertrauen können, dass ihnen zugeordnete Schränke nicht ohne ihre Einwilligung geöffnet, dort eingebrachte persönliche Sachen nicht ohne ihr Einverständnis durchsucht werden.*

*Geschieht dies dennoch, liegt regelmäßig ein schwerwiegender Eingriff in ihre Privatsphäre vor. Er kann nur bei Vorliegen zwingender Gründe gerechtfertigt sein. ...Erforderlich iSd § 32 I 2 BDSG bzw. verhältnismäßig im Sinne einer Beschränkung des allgemeinen Persönlichkeitsrechts kann eine Schrankkontrolle aber nur sein, wenn sie **geeignet, erforderlich und angemessen** ist. Dem Arbeitgeber dürfen keine ebenso effektiven, den Arbeitnehmer weniger belastenden Möglichkeiten zur Aufklärung des Sachverhalts zur Verfügung stehen. Außerdem muss die Art und Weise der Kontrolle als solche den Verhältnismäßigkeitsgrundsatz wahren. ... **Eine in Anwesenheit des Arbeitnehmers durchgeführte Schrankkontrolle ist gegenüber einer heimlichen Durchsuchung das mildere Mittel.** Die Kontrolle in seinem Beisein gibt dem Arbeitnehmer nicht nur die Möglichkeit, auf die Art und Weise ihrer Durchführung Einfluss zu nehmen. Er kann sie unter Umständen – etwa durch freiwillige Herausgabe gesuchter Gegenstände – sogar ganz abwenden. Die verdeckte Ermittlung führt ferner dazu, dass dem Betroffenen vorbeugender Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz erschwert wird. Die Heimlichkeit einer in Grundrechte eingreifenden Maßnahme erhöht typischerweise das Gewicht der Freiheitsbeeinträchtigung...“*



## Telefonüberwachung

- Das **heimliche Abhören** von Telefongesprächen ist generell unzulässig.
- Das **Mithören** eines Telefongesprächs z.B. durch Lautsprecher ist zulässig, sofern der Arbeitnehmer zugestimmt hat (BVerfG, NZA 1992, 307).
- Das **heimliche Mithörenlassen** von Telefongesprächen zwischen Arbeitgeber und Arbeitnehmer verletzt das allgemeine Persönlichkeitsrecht und ist unzulässig; auf diese Art erlangte Beweismittel dürfen nicht verwertet werden (Schrader/Mahler, Interne Ermittlungen des Arbeitgebers und Auskunftsgrenzen des Arbeitnehmers, NZA-RR 2016, 57 ff).

Mit Urteil vom 23.04.2009 – 6 AZR 189/08 - hat das BAG zu der Frage der Beweisverwertung eines **zufällig mitgehörten Telefongesprächs**, auf welches sich die Arbeitnehmerin wegen angeblicher Unwirksamkeitsgründe der Kündigung berief, die Beweisverwertung bejaht. Die Entscheidung wurde insbesondere damit begründet, dass aufgrund technischer Neuerungen die Gefahr des zufälligen Mithörens deutlich erhöht sei.





## GPS Daten

- Es ist datenschutzrechtlich unproblematisch, wenn die Ortung zur reinen **Standortbestimmung** erfolgt, um ggfls. weitere Aufträge zu einer standortnahen Zieladresse vergeben zu können. Auch die Erfassung der Arbeitszeit kann mittels eines Ortungssystems erfolgen.
- Bei weitergehenden Anwendungsbereichen wie einer genauen **Streckenverfolgung**, wird es kritisch. Hier muss sichergestellt sein, dass die Daten nicht auch zu einer Verhaltens- und Leistungskontrolle verwandt werden, so die Landesdatenschutzbeauftragte NRWs, Helga Block im Jahresbericht 2019. Zur generellen Vermeidung von Problemen bei der Streckenverfolgung durch GPS-Techniken empfiehlt die Datenschutzbehörde NRW den Arbeitgebern auf alternative Kontrollmethoden zu setzen, wie etwa manuell gepflegte Fahrtenbücher.
- Beim Einsatz von GPS – Ortung muss der Betriebsrat gemäß **§ 87 Abs. 1 Nr. 6 BetrVG** beteiligt werden.



## Videüberwachung

- Eine Videoüberwachung ist nur dann zulässig, wenn sie nicht in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung der Arbeitnehmer eingreift. Zu beachten sind im Arbeitsverhältnis Art. 88 DSGVO in Verbindung mit § 26 Abs. 1 S. 1 BDSG.
- Man unterscheidet die **offene Videoüberwachung** von der **verdeckten (heimlichen) Videoüberwachung**. Die verdeckte Videoüberwachung unterliegt engen Grenzen und ist nur in Ausnahmefällen zulässig.
- Zusätzlich wird differenziert zwischen der Videoüberwachung in **öffentlich zugänglichen** Bereichen und in **nicht – öffentlich zugänglichen** Bereichen.
- Die Einführung und Anwendung von Videoüberwachungsanlagen ist mitbestimmungspflichtig nach § 87 Abs. 1 Nr. 6 BetrVG.

## Offene Videoüberwachung von Mitarbeitern

- ✓ Die Überwachung **öffentlich zugänglicher Räume**, wie etwa von Verkaufsräumen, mit optisch-elektronischen Einrichtungen („Videoüberwachung“) ist in der DSGVO nicht ausdrücklich geregelt.
- ✓ Unverändert zulässig sind Videoaufnahmen jedenfalls dann, soweit sie zur Wahrnehmung des Hausrechts oder anderer, konkret festgelegter und berechtigter Zwecke erforderlich sind und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen (§ 4 I BDSG). Der mit der Kontrolle verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers muss gegen das Überwachungsinteresse des Arbeitgebers abgewogen werden. (**geeignet, erforderlich, verhältnismäßig** / Dauer der Überwachung / Anzahl der beteiligten Personen)
- ✓ Die Beobachtung muss bekanntgegeben werden (§ 4 II BDSG). Durch die DSGVO kam hinzu, dass nicht nur der Umstand der Beobachtung, sondern auch der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen erkennbar zu machen sind. Das hat – nach dem ebenfalls geänderten Wortlaut – „zum frühestmöglichen Zeitpunkt“ zu geschehen.

Eine permanente Videoüberwachung kann aber weder auf das Weisungsrecht noch auf das Hausrecht gestützt werden (Maschmann, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, 115).

## Offene Videoüberwachung von Mitarbeitern

„Die tatsächlichen Anhaltspunkte für den Verdacht sind **zu dokumentieren**, § 26 Abs. 1 S. 2 BDSG.

*Inventurdifferenzen bei Betrieben des Einzelhandels begründen für sich allein noch keinen hinreichenden Anfangsverdacht, solange der Arbeitgeber nicht andere Ursachen für ein bestehendes Manko – z.B. Fehlbuchungen, Entwendung nicht im Verkaufs-, sondern im Lagerbereich – ausgeschlossen hat.*

*Es bedarf konkreter Feststellungen, warum eine Videoüberwachung das praktisch einzig verbliebene Mittel darstellt, Unregelmäßigkeiten aufzuklären oder einen Verdacht in personeller Hinsicht weiter einzugrenzen.*

*Befinden sich die zu überwachenden Arbeitsplätze in nicht öffentlich zugänglichen Räumen (z.B. Büros, Lagerräumen), gilt statt § 4 BDSG der § 26 I BDSG, der aber keine weitergehenden Voraussetzungen enthält. ....*

*Die Videoaufnahmen sind **zu löschen**, wenn sie zur Erreichung des mit der Aufnahme verfolgten Überwachungszwecks nicht mehr erforderlich sind (Art. 5 I Buchst. e DSGVO iVm Art. 17 III Buchst. e DSGVO). Die Speicherung von Bildsequenzen aus einer rechtmäßigen offenen Videoüberwachung, die vorsätzliche Handlungen eines Arbeitnehmers zulasten des Eigentums des Arbeitgebers zeigen, soll nach einer aktuellen Entscheidung des BAG **nicht durch bloßen Zeitablauf unverhältnismäßig werden, jedenfalls solange die Ahndung der Pflichtverletzung durch den Arbeitgeber arbeitsrechtlich möglich ist**. Das Gericht hielt es daher für zulässig, dass ein Ladeninhaber Videoaufzeichnungen gegen einen Mitarbeiter verwendete, die sechs Monate lang unbeachtet blieben und erst danach ausgewertet wurden. Der rechtmäßig gefilmte Vorsatztäter sei nicht schutzwürdig („Datenschutz ist nicht Tatenschutz“).“, so Maschmann a.a.O.*

## Verdeckte Videoüberwachung

Nach der Rechtsprechung des BAG liegen die Anforderungen bei der verdeckten Videoüberwachung noch höher, weil der Arbeitnehmer keine Abwehrstrategie entwickeln kann.

Teilweise (Maschmann; Venetis/Oberwetter, Videoüberwachung von Arbeitnehmern, NJW 2016, 1051) wird in der Literatur sogar vertreten, dass die verdeckte Videoüberwachung im öffentlichen Raum nach der DSGVO gar nicht mehr zulässig sei.

*„§ 6 b BDSG ist demnach nur auf einen Teil der Arbeitsplätze anwendbar, da eine große Anzahl von Beschäftigten in Betrieben oder Betriebsteilen arbeitet, die nicht öffentlich zugänglich sind.“*

*Ein Problem bietet ferner der Fakt, dass bei bestimmten Arbeitsplätzen keine konkrete Zuordnung dahingehend erfolgen kann, ob sie öffentlich zugänglich sind oder nicht. Als Beispiel seien die Kassenbereiche bei Discountern genannt. Es ginge jedoch an der Realität vorbei, solche Bereiche von der „Öffentlichkeit“ auszuklammern.“*

## Verdeckte Videoüberwachung / Zufallsfund

BAG, 22.09.2016 - 2 AZR 848/15 –

In einem Supermarkt waren in der Vergangenheit erhebliche Inventurverluste im Bereich Tabakwaren zu verzeichnen. Sämtliche Ermittlungen blieben ohne Erfolg. Der Verdacht richtete sich gegen zwei Kassiererinnen. Als letztes Mittel griff der Supermarkt zur verdeckten Videoüberwachung für die Dauer von 14 Tagen.

Die Auswertung der Videoaufzeichnungen ergab zufällig, dass die stellvertretende Filialleiterin mehrmals eine „Musterpfandflasche“ einbongte und den so erzeugten Bon über 3,25€ einlöste und das Geld der Kasse entnahm.

Gegen die Kündigung erhob die Mitarbeiterin Klage und berief sich auf ein Beweisverwertungsverbot wegen Verletzung ihres allgemeinen Persönlichkeitsrechts.

Das BAG kam zu dem Schluss, dass dann, wenn die verdeckte Videoüberwachung als solche rechtmäßig ist, auch der Zufallsfund verwertet werden kann. Dem steht auch eine Verletzung des Mitbestimmungsrechts des Betriebsrats nach § 87 Abs. 1 Zi. 6 BetrVG nicht entgegen.



## Praxistipp

**Im Falle des – offenen oder verdeckten – Einsatzes von Videokameras zur Arbeitnehmerüberwachung sind insbesondere folgende Punkte zu berücksichtigen:**

(Moll, Münchner Anwaltshandbuch Arbeitsrecht, 5. Aufl. 2021)

1. Es muss einen konkreten Anlass für den Überwachungseinsatz (Anfangsverdacht einer schwerwiegenden Straftat) geben, dieser ist ausreichend zu dokumentieren;
2. es ist ausreichend, wenn der Arbeitgeber seinem Tatverdacht gegen eine abgrenzbare Arbeitnehmergruppe nachgeht;
3. zudem darf dem Arbeitgeber keine Abhilfe auf andere Art und Weise, also durch weniger einschneidende Mittel, möglich sein;
4. der Einsatz von Videokameras muss räumlich und zeitlich beschränkt sein;
5. in der Gesamtbewertung darf der Einsatz von Videoaufnahmen nicht unangemessen erscheinen;
6. schließlich darf die so erlangte Videoaufnahme nicht zu anderen als zu Beweis Zwecken benutzt werden;



## Stück: Datenschutz = Tatenschutz? Ausgewählte datenschutz- und arbeitsrechtliche Aspekte nach DSGVO sowie BDSG 2018 bei präventiver und repressiver Compliance (CCZ 2020, 77)

Nach der DSGVO bestehen besondere Dokumentationspflichten. Die wesentlichen datenschutzrechtlichen Grundsätze sind dabei:

- **Keine Datenverarbeitung ohne Erlaubnisgrundlage**: (Art. 6; 88 DSGVO; § 26 Abs. 1 BDSG 2018), wobei im Beschäftigungskontext § 26 Abs. 1 BDSG 2018 die Erlaubnisnorm ist.
- Der **Zweck der Datenverarbeitung muss schon vor Datenerhebung feststehen** (Art. 5 Abs. 1 lit. b), Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).
- Das „**need to know Prinzip**“ (Art. 5 Abs. 1 lit. f DSGVO) erfordert, dass nur die diejenigen Mitarbeiter in einen bestehenden Verdacht eingeweiht werden, die diese Informationen zwingend benötigen, und auch – zB mittels besonderer Vertraulichkeitsverpflichtungserklärung (NDA) – „vergattert“ werden.
- Bezüglich jeder Datenverarbeitung muss eine **schriftliche Dokumentation** über die Einhaltung der Vorschriften sowie der dafür eingesetzten technischen und organisatorischen Maßnahmen erfolgen (Art. 5 Abs. 2, 24 Abs. 1 DSGVO).
- Umfassende Informations- und Mitteilungspflichten bei der Datenverarbeitung sind einzuhalten (Art. 13 f. DSGVO). Hiervon kann jedoch nach § 33 Abs. 1 Nr. 2 a BDSG, Art. 14 Abs. 5 lit. c DS-GVO ausnahmsweise abgewichen werden, insbesondere zur Betrugsbekämpfung, so dass auch verdeckte Detektiveinsätze und heimliche Videoüberwachung weiter möglich sind.
- Ebenso muss über das bestehende Auskunfts- und Berichtigungsrecht und das Recht auf Löschung informiert werden (Art. 15 ff. DSGVO). Eine Verpflichtung zur Einbindung des betrieblichen Datenschutzbeauftragten besteht nicht, empfiehlt sich aber.



## Kontrolle von E - Mails / ausschließlich dienstliche Nutzung



- Es ist zu differenzieren, ob es sich ausschließlich um einen dienstlichen Account handelt oder, ob die private Nutzung erlaubt ist.

### Kontrolle bei untersagter Privatnutzung

- Beim rein dienstlich genutzten Account sind Kontrollen grundsätzlich zulässig (BAG, NZA 2017, 1327; GMR, 12.01.2016 - 61496/08 – Barbulescu/ Rumänien), schon um die Einhaltung des Verbots der Privatnutzung zu überprüfen. Von ein- und ausgehenden Mails kann der Arbeitgeber genauso Kenntnis nehmen wie bei Schriftverkehr.

Dies bezieht sich auf info@ Adressen, abteilungsbezogene Adressen wie personalabteilung@ sowie Adressen, die den Namen enthalten wie Dimitri.Hoffmann@. Davon ausgenommen sind Geheimnisträger wie Betriebsrat oder Betriebsarzt.

Wenn der Absender der Mail die Einsichtnahme durch den Arbeitgeber vermeiden möchte, muss er die Mail als persönlich / vertraulich kennzeichnen und verschlüsseln.

- Das Verbot der Privatnutzung ist mitbestimmungsfrei (LAG Hamm, 07.04.2006 - 10 TaBV 1/06 -).

## Kontrolle von E - Mails / erlaubte Privatnutzung



- Hat der Arbeitgeber die private Nutzung ausdrücklich gestattet oder sie zumindest widerspruchlos geduldet, ist die Rechtslage für Arbeitgeber schwierig.

(1) Denn es wird vertreten, dass er als **Anbieter von Telekommunikationsdiensten** i.S.d. § 3 Nr. 6 Telekommunikationsgesetz (TKG) bzw. von Telemedien § 2 Nr. 1, § 11 Telemediengesetz (TMG) gilt, LAG Hessen – 10 Sa 601/18 -. (Von den obersten Gerichten ist die Fragestellung bis heute nicht geklärt.)

Inhalts- und Verbindungsdaten unterfallen damit dem **Fernmeldegeheimnis** nach § 88 Abs. 2 TKG, § 206 StGB. Ein Zugriff ist danach ausgeschlossen.

- (2) Diejenigen, die anderer Auffassung sind (LAG Niedersachsen, - 12 Sa 875/09 -; LAG Berlin – Brandenburg, - 5 Sa 657/15 -) argumentieren wie folgt: „Ein Diensteanbieter i.S.d. § 3 Nr. 6 TKG erbringt Telekommunikationsdienste ganz oder teilweise geschäftsmäßig. ... Das geschäftsmäßige Erbringen von Telekommunikationsdiensten ist in § 3 Nr. 10 TKG legaldefiniert als das „nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. ... Es sprechen im Ergebnis wohl die gewichtigeren Argumente dafür, Arbeitnehmer hier nicht als „Dritte“ i.S.v. § 3 Nr. 10 TKG anzusehen, so dass es auch an der geschäftsmäßigen Erbringung mangeln dürfte.“
- Sie kommen über die DSGVO und § 26 BDSG zu einem gewissen Spielraum für Arbeitgeber.

## Kontrolle von E - Mails / erlaubte Privatnutzung



Bei erlaubter Privatnutzung, muss der Arbeitgeber die Privatsphäre des Arbeitnehmers beachten. Er darf nur dann Einsicht in das E-Mail-Postfach nehmen, wenn hierzu ein **berechtigter Anlass** besteht. Dieser kann zB tatsächlichen Anhaltspunkten für den Verdacht einer Straftat (§ 26 I BDSG) oder bei konkreten Anhaltspunkten für eine Arbeitspflichtverletzung gegeben sein.

Dabei ist der **Grundsatz der Verhältnismäßigkeit** zu beachten. So sollte die Kontrolle offen in Anwesenheit des Beschäftigten und unter Hinzuziehung des Datenschutzbeauftragten und des Betriebsrates erfolgen. Außerdem ist das Lesen offensichtlich privater E-Mails ausgeschlossen, es sei denn, es bestehen konkrete Anhaltspunkte, dass sich die Straftat gerade aus dem Inhalt dieser privaten E-Mails ergibt (zB beim Verrat von Geschäftsgeheimnissen).

**Praxistipp:** Die Arbeitnehmer sollten verpflichtet werden, private E-Mails zB durch gesonderten Betreff zu kennzeichnen und/oder private E-Mails unverzüglich in einem extra Ordner zu verschieben. Damit wird auf einfache Weise eine eindeutige Zuordnung erreicht.

Außerdem sollten die Vorgaben zur E-Mail-Nutzung und zum Einsichtsrecht im Arbeitsvertrag und/oder in einer Betriebsvereinbarung eindeutig geregelt werden. Da es sich bei der Privatnutzung um einen Vorteil handelt, **ist es datenschutzrechtlich möglich, die Erlaubnis an eine Einwilligung des Beschäftigten zu angemessenen Einsichts- und Kontrollrechten des Arbeitgebers zu koppeln (Art. 7 DSGVO, § 26 II BDSG).**

*Quelle: Müller, Beschäftigtendatenschutz im Arbeitsrecht: dienstliche und private E-Mail-Nutzung, öAT 2019, 1.*

- ✓ BAG, 27.07.2017 – 2 AZR 681/16 – (**Keylogger**): Der ständige Einsatz einer Spähsoftware wie eines Keyloggers, der alle Tastatureingaben des Arbeitnehmers aufzeichnet, speichert und noch dazu Screenshots herstellt, ist ohne Anhaltspunkte für eine schwere Pflichtverletzung oder Straftat unverhältnismäßig. Die Ergebnisse können im Prozess nicht verwertet werden.



Arbeitgeberverband  
**Region** Braunschweig e.V.