

Beschäftigtendatenschutz: Was ist zu beachten?

RA Dr. Kai Hüther
Fachanwalt für Arbeitsrecht
rapräger Rechtsanwälte

0. Agenda

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Einleitung
2. Die gesetzlichen Grundlagen
 - a. die europarechtlichen Vorgaben und die nationalen Maßgaben
 - b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

II. Wesentliche Anwendungsbereiche

1. Kontrolle von Mitarbeitern

- a. Gefahren bei Kontrollmaßnahmen
- b. Datenverarbeitung zur Aufdeckung von Straftaten
- c. Videoüberwachung
- d. Ortung
- e. Aktivitäten in sozialen Medien
- f. Einsatz von Detektiven
- g. Privatnutzung dienstlicher IT

0. Agenda

2. Datenschutz bei der Anbahnung und Begründung von Arbeitsverhältnissen

- a. Fragerecht des Arbeitgebers bei Bewerbungsgesprächen
- b. Auffinden bzw. Ansprechen von potentiellen Bewerbern über das Internet
- c. Onlinerecherchen in Bewerbungsverfahren
- d. Anfrage beim ehemaligen Arbeitgeber
- e. Die Datenschutzerklärung und Umgang mit den Daten der Bewerber

3. Die Personalakte

III. Die Datenschutzverpflichtung

IV. Der Datenschutzbeauftragte

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Einleitung

2. Die gesetzlichen Grundlagen

a. Die europarechtlichen Vorgaben und die nationale Umsetzung

- EU-Datenschutz-Grundverordnung (DSGVO) ist seit Mai 2018 in allen EU-Ländern verbindlich
- § 88 des DS-GVO als Ermächtigungsgrundlage für den deutschen Gesetzgeber
- § 26 BDSG als nationale Umsetzung Im Lichte der DSGVO zu interpretieren:
 - Nicht benutzerfreundlich für den Rechtsanwender; unbestimmte Rechtsbegriffe
 - Heranziehung der Rechtsprechung des BAG

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Einleitung
2. Die gesetzlichen Grundlagen

Zentrale Norm: § 26 BDSG:

- *„**Personenbezogene Daten** von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses **verarbeitet** werden, wenn dies für die Entscheidung über die Begründung eines **Beschäftigungsverhältnisses** oder nach Begründung des **Beschäftigungsverhältnisses** für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten **erforderlich** ist.“*

I. Grundsätzliches zum Beschäftigtendatenschutz

2. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

- **Adressat: Der „Verantwortliche“**
 - Nicht alleine Arbeitgeber
 - Auch Auftragnehmer oder Dritte
 - Betriebsräte und Interessenvertretungen

I. Grundsätzliches zum Beschäftigtendatenschutz

2. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

- „Beschäftigte“
 - Arbeitnehmerinnen und Arbeitnehmer einschließlich der Leiharbeiterinnen und Leiharbeiter
 - zu ihrer Berufsbildung Beschäftigte
 - Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitanden)
 - in anerkannten Werkstätten für behinderte Menschen Beschäftigte
 - Freiwillige nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz leisten, Zivildienstleistende, Soldaten
 - Beamte
 - Bewerber und ausgeschiedene Arbeitnehmer
 - arbeitnehmerähnliche Personen

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

- Was sind „**personenbezogene Daten**“?
 - Personenbezogene Daten sind alle Informationen über eine natürliche Person, die sich der Person unmittelbar oder mittelbar zuordnen lassen.
 - Bsp.: Unmittelbar: Name, singuläre Position im Unternehmen; Mittelbar: Personalnummer, IP-Adresse
- besondere Kategorie: „**sensible personenbezogene Daten**“
 - besonders zu schützenden Daten, sh. § 88 DSGVO
 - Erfordern besonders vorsichtigen Umgang
- Was bedeutet „**Verarbeiten**“?, Art. 4 Ziff. 2 DSGVO
 - Jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung
 - i.E.: Alles, was mit Daten geschieht

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

- Die Zulässigkeit der Verarbeitung: Was heißt also „**Erforderlichkeit**“?
 - Es sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.
 - Prüfung in Schritten:
 - Geeignetheit
 - Mildestes, gleich effektives Mittel
- Die „**Einwilligung**“ in die Datenverarbeitung
 - Problem: Freiwilligkeit

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

Fall: Einwilligung

AN ist seit 4 Monaten erkrankt. AG fordert im Rahmen eines Krankenrückkehrgespräches Auskünfte über die den AU-Zeiten zugrundeliegenden Leiden und deren Ursachen. Erteile der AN diese Informationen nicht, werde er überlegen, ob er das Arbeitsverhältnis krankheitsbedingt kündigen werde. Der AN erteilt seine Einwilligung und gibt die begehrten Informationen preis. Nach Sichtung der betreffenden Daten kündigt der Arbeitgeber, weil nach den ärztlichen Befunden der AN nicht mehr genesen wird. AN erhebt Kündigungsschutzklage. Hat diese Erfolg?

Lösung:

- **An sich rechtfertigt eine durchgehende AU von 4 Monaten noch keine krankheitsbedingte Kündigung; nach 4 Monaten kann nach der Rspr. Des BAG noch keine negative Gesundheitsprognose gestellt werden. Der Arbeitgeber beruft sich aber auf die ärztliche Einschätzung, die er erlangt hat; der AN werde nicht wieder genesen**
- Die Einwilligung wurde aber nicht freiwillig erteilt, weil negative Auswirkungen für den Fall in Aussicht gestellt wurden, dass die Einwilligung nicht erteilt werde
- Die Erfassung und Nutzung der Gesundheitsdaten ist damit unzulässig
- Die Daten dürfen für die Rechtfertigung der Kündigung nicht verwendet werden
- Der AG wird im Verfahren ohne Beweisaufnahme unterliegen
- Außerdem: Es droht ein Bußgeld durch die Landesbeauftragte für den Datenschutz und sogar ein Schmerzensgeld; es sind nämlich besonders sensible Daten betroffen und das Allg. Persönlichkeitsrecht wurde konkret verletzt.

I. Grundsätzliches zum Beschäftigtendatenschutz

1. Die gesetzlichen Grundlagen

b. Grundlagen zum Verständnis: Wichtige Rechtsbegriffe

- Informationspflichten bei jeder begehrten Einwilligung zu beachten:
 - Zwecke der Einwilligung
 - Gesellschaften
 - Hinweis auf Freiwilligkeit
 - Hinweis auf Recht zum Widerruf: jederzeit und ohne Grund (Problem: Wenigstens plausibler Grund? Was ist bei Trotzreaktion?)
- Textform genügt; keine Aufnahme in den Arbeitsvertrag sondern Erfüllung der Informationspflichten und sodann Einwilligung

II. Wesentliche Anwendungsbereiche

1. Kontrolle der Mitarbeiter

a. Gefahren bei Kontrollmaßnahmen

- Sofortiges Einstellen der Maßnahme
- „Anzeige“ bei Landesbeauftragten für Datenschutz und Informationsfreiheit (Ordnungswidrigkeit!)
- Beweisverwertungsverbot
- Schmerzensgeld bei konkreter Verletzung des Allg. Persönlichkeitsrechts
- Offene oder verdeckte Datenerhebung: idR nur offene Überwachung zulässig (psych. Anpassungsdruck)

b. Datenverarbeitung zur Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG

- *„Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn **zu dokumentierende tatsächliche Anhaltspunkte den Verdacht** begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung **erforderlich ist** und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“*
- Einfacher Verdacht (Anfangsverdacht) genügt
- Passt nicht bei untergesetzlichen Regelverstößen; dann aber Prüfung der Erforderlichkeit (s.o.)

II. Wesentliche Anwendungsbereiche

1. Kontrolle der Mitarbeiter

Fall: „Key Logger“

- AG setzt Key Logger ein, weil er vermutet, dass am Arbeitsplatz mehr privat gesurft wird als gearbeitet. Dabei entdeckt er, dass AN (1 Jahr im Betrieb) sich mehrfach per Email abfällig über den AG geäußert hat; AG sei ein „Ausbeuter und Menschenschinder.“ AG kündigt dem AN.
- Hat die Kündigungsschutzklage des AN Erfolg?

Lösung:

- Üble Nachrede genügt als Kündigungsgrund
- Aber: Beweisverwertungsverbot prüfen
- Zufallsfunde grds. verwertbar
- Aber: Verbot der Totalüberwachung
- Folge: Verwertung unzulässig
- Außerdem: Allg. Persönlichkeitsrecht ist verletzt; daher: Schmerzensgeld (aber nicht hoch)

II. Wesentliche Anwendungsbereiche

1. Kontrolle der Mitarbeiter

c. Videoüberwachung

- Prüfung der Erforderlichkeit: Frage der Intensität des Eingriffs in das All. Persönlichkeitsrecht
- Verdeckte (heimliche) Überwachung wohl nur zur Aufdeckung von Straftaten bei konkreten Verdachtsmomenten, d.h. nicht schon zur Kontrolle der Redlichkeit
- in nicht-öffentlichen Bereichen idR unzulässig
- Überwachung erzeugt Anpassungsdruck
- Möglich zum Schutz von Rechtsgütern:
 - Sicherheit der Mitarbeiter (Gefahrenbereiche)
 - Bei großen materiellen Werten

d. Ortung

- Erfassung von Bewegungsdaten per GPS, RFID, Mobiltelefone
- Im dienstlichen Bereich ggf. zulässig: präventive Abwehr von Straftaten; Sicherheit der Mitarbeiter
- Verdeckt nur zur Aufdeckung von Straftaten

II. Wesentliche Anwendungsbereiche

1. Kontrolle der Mitarbeiter

e. Aktivitäten in sozialen Medien

- Häufig Anlass für verhaltensbedingte Kündigungen
- Außerdienstliches Verhalten kann ausnahmsweise Relevanz für Arbeitsverhältnis haben
- Unzulässig: Verschaffen von Zugangsdaten zu privaten Chatgruppen/Netzwerken

f. Einsatz von Detektiven

Fall: AG will per Detektiveinsatz klären, ob ein krank geschriebener Mitarbeiter tatsächlich krank ist. Er hält den Mitarbeiter für grds. eher arbeitsscheu und hat ein vages „Bauchgefühl“, dass der AN „blau macht“. Der von ihm eingesetzte Detektiv liefert dem AG ein Video. Dieses zeigt den AN bei diversen privaten Aktivitäten, ua beim Spaziergang mit seine Hund und beim Besuch eines Waschsalons. Es liegt eine Arbeitsunfähigkeitsbescheinigung vor. Der AG kündigt, weil der AN angegeben hat, Rückenbeschwerden zu haben, was nach Ansicht des AG nicht mit den gezeigten Privataktivitäten zu vereinbaren sei. Ist die Kündigung wirksam? Muss der An dem AG die Detektivkosten erstatten? AN fühlt sich verfolgt und will Schmerzensgeld- zu Recht?

Lösung:

- Lt. BAG Kontrolle bei Verdacht von „Krankfeiern“ auch im Privatbereich zulässig
- Ohne Verdachtsmomente aber unzulässig
- Folge: Keine Erstattung der Detektivkosten; keine Beweisverwertung; Schmerzensgeld

II. Wesentliche Anwendungsbereiche

1. Kontrolle der Mitarbeiter

g. Privatnutzung dienstlicher IT

- Mitbestimmungsfreie Entscheidung, ob MA IT privat nutzen dürfen
- Exzessive Nutzung als Kündigungsgrund
- Verbot der Privatnutzung ratsam
- **„Gute Praxis“: entscheidend ist, ob angemessene Vorkehrungen zum Schutz des Allg. Persönlichkeitsrechts das MA getroffen wurden**
 - Transparenz über ob, Umfang und Zwecke der Einsichtnahme in den dienstlichen E-Mail Account mit erlaubter Privatnutzung
 - Trennung dienstliche/private Sphäre
 - Vorrangige mildere Mittel
 - Schonendes Vorgehen
 - Jedenfalls klare Regelungen für die erlaubte private Nutzung und das Verbot der Privatnutzung

II. Wesentliche Anwendungsbereiche

2. Datenschutz bei der Anbahnung und Begründung von Arbeitsverhältnissen

a. Fragerecht des Arbeitgebers

- Aufzeichnungen während Bewerbungsgesprächen als Datenverarbeitung
- berechtigtes Interesse des Arbeitgebers nur, wenn für das Bewerbungsverfahren erforderlich (Bezug zur Tätigkeit)
- Keine Anfechtung bei „Recht zur Lüge“; Offenbarungspflicht im Einzelfall zu prüfen
- Anwendungsfelder:
 - Schwerbehinderung
 - Vorstrafen
 - Gesundheitliche Handicaps
 - Religionszugehörigkeit
 - Sexuelle Orientierung
 - Schwangerschaft
 - Geordnete Vermögensverhältnisse

b. Auffinden bzw. Ansprechen von potentiellen Bewerbern über das Internet

c. Onlinerecherchen im laufenden Bewerbungsverfahren

d. Anfrage beim ehemaligen Arbeitgeber

II. Wesentliche Anwendungsbereiche

2. Datenschutz bei der Anbahnung und Begründung von Arbeitsverhältnissen

e. Die Datenschutzerklärung und Umgang mit den Daten der Bewerber

- Information der Bewerber über die Datenverarbeitung im Wege der Datenschutzerklärung wegen Art 13 DSGVO
- Inhalt:
 - Kontaktdaten des potenziellen Arbeitgebers und des Datenschutzbeauftragten (sofern ein solcher bestellt werden muss, oder freiwillig bestellt ist)
 - Rechtsgrundlage und Zweck der Verarbeitung (dies ist in der Regel §26 Abs. 1 S. 1 BDSG)
 - Speicherdauer der Bewerbungsunterlagen bzw. die Kriterien für die Aufbewahrungsdauer
 - Mögliche Empfänger der Bewerbung (zum Beispiel andere Niederlassungen oder Tochterfirmen innerhalb der Unternehmensgruppe)
 - Mögliche Drittstaatentransfers (zum Beispiel in die USA) und die hierfür verwendeten Datenschutz-Garantien (zum Beispiel sog. EU-Standardvertragsklauseln oder die Einwilligung des Bewerbers)
 - Beschwerderecht des Betroffenen bei der zuständigen Aufsichtsbehörde
 - Hinweis auf das Widerrufsrecht bei Einwilligung des Betroffenen
 - Belehrung über die Rechte des Betroffenen (zum Beispiel Auskunftsrecht, Art. 15 DSGVO, Recht auf Datenberichtigung, Art. 16 DSGVO, Recht auf Löschung, Art. 17 DSGVO, Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO, Widerspruchsrecht, Art. 21 DSGVO, Recht auf Datenübertragbarkeit, Art. 20 DSGVO).
- Platzierung wichtig
- Zugriff nur durch möglichst engen Personenkreis
- Löschen nach Abschluss des Verfahrens; Ausnahme: Aufnahme in Bewerberpool

II. Wesentliche Anwendungsbereiche

2. Die Personalakte

- Die klassischen Grundsätze der Personalaktenführung
 - Nicht: „je mehr desto besser“
 - Vertraulichkeit
 - Richtigkeit
 - Zulässigkeit
 - Transparenz
- Der Inhalt der Personalakte
 - Keine besonders sensible Daten; Gesundheitsdaten besonders zu sichern und mit Berechtigungskonzept
 - Keine nicht mehr benötigten Daten
 - Keine Unterlagen, bei denen die Aufbewahrungsfrist abgelaufen ist
- Herausforderung Aufbewahrungsfristen
- Herausforderung Datensicherheit

III. Die Datenschutzverpflichtung

- Warum ist eine Datenschutzverpflichtung erforderlich?
 - Nicht optional, sondern gesetzliche Verpflichtung für alle Arbeitgeber, Art. 29, 32 Abs. 4 DSGVO
 - Nur, wenn alle Mitarbeiter den Datenschutz befolgen, kann ein Arbeitgeber datenschutzkonform arbeiten
- Gestaltung der Verpflichtung
 - Grob: Datenschutzmaßgaben sind zu befolgen
 - Aber: genaue Erläuterung, ggf. mit Beispielen
 - Best Practice: Merkblatt; Erläuterung und Unterschrift
 - Schriftlich zwecks Beweissicherung

IV. Der Datenschutzbeauftragte

- **Bestellungspflicht**, wenn im Unternehmen in der Regel **mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind**; wird er nicht bestellt, sieht die DS-GVO Bußgelder bis zu 10 Millionen EUR oder 2% des weltweiten Jahresumsatzes vor
- Konkret: Ab 10 Computerarbeitsplätzen
- Ist eine Bestellung nicht vorgeschrieben, ist eine **freiwillige Bestellung zu empfehlen**; Grund: Das Unternehmen ist zuständig für die Einhaltung der datenschutzrechtlichen Bestimmungen, d.h. Datenschutz ist Chefsache!
- Zumal interne Datenschutzbeauftragte, also eigene AN als Datenschutzbeauftragte, einem starken Sonderkündigungsschutz unterfallen, ist die **Bestellung eines externen DSB anzuraten**, sprich also Beauftragung eines DSB im Rahmen eines Dienstleistungsvertrages
- Der fachlich entsprechend qualifizierte DSB **berät das Unternehmen umfassend** zu den sich aus dem BDSG und der DS-GVO ergebenden Verpflichtungen.
- Im Einzelnen hat er **insbesondere folgende Aufgaben**:
 - Unterrichtung über die bestehenden datenschutzrechtlichen Pflichten
 - Beratung zur Umsetzung und Einhaltung der datenschutzrechtlichen Maßgaben
 - Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften (insbes. BDSG und DS-GVO)
 - Zusammenarbeit mit der Aufsichtsbehörde
 - Ansprechpartner für betroffene Personen und Mitarbeiter

Vielen Dank und bis zum nächsten Mal!

RA Dr. Kai Hüther

Fachanwalt für Arbeitsrecht

0681-306 41 40

huether@rapraeger.de