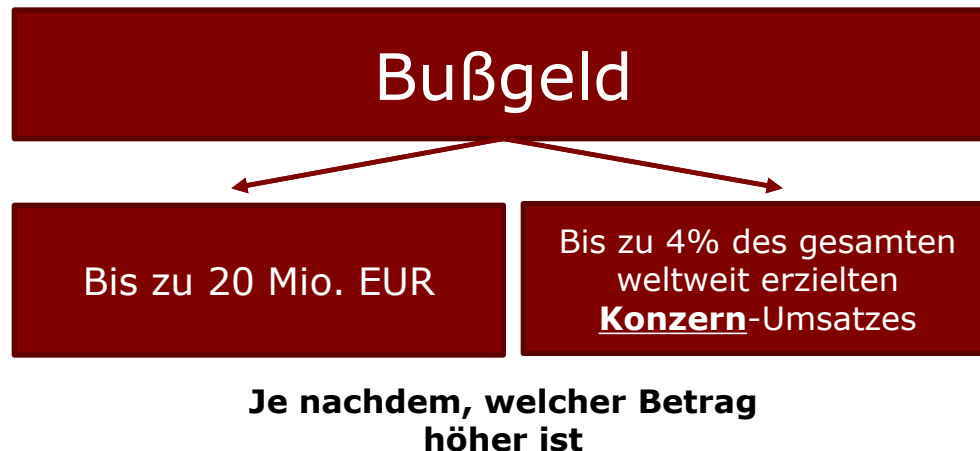


DS-GVO in der Personalpraxis



Haftungsrisiko für das Unternehmen

- Haftungsrisiko steigt enorm an
- Schadensersatz materiell und immateriell (Art. 82 Abs. 1 DSGVO)
- Bußgelder (Art. 83 DSGVO)
 - Fast alle wesentlichen Bestimmungen der DSGVO betroffen.
 - Geldbußen müssen in jedem Einzelfall **wirksam**, **verhältnismäßig** und **abschreckend** sein.



Geltung ab 25. Mai 2018



- Unmittelbar in der gesamten EU
- Geltungsbereich
 - Für **sämtliche Unternehmen** in der EU und für Unternehmen außerhalb der EU („Drittstaaten“), wenn sie Personen in der EU Leistungen anbieten (auch kostenlose Dienste) bzw. das Verhalten von Personen in der EU beobachten (Tracking, Profiling, etc.)
- Folgende Ziele werden verfolgt:
 - Stärkung der Aufsichtsbehörden
 - Stärkung der Verbraucherrechte
 - Umfassende Neuordnung des gesamten Datenschutzes in Europa

Relevante Einzelnormen der DSGVO

- Art. 4 Begriffsbestimmungen – wie z.B. „personenbezogene Daten“, „Verarbeitung“ oder „Verantwortlicher“
- Art. 5 Grundsätze der Datenverarbeitung (Transparenz, Zweckbindung, Datensparsamkeit)
- Art. 6 Rechtmäßigkeit der Datenverarbeitung
- Art. 7 Bedingung für die Einwilligung und den Widerruf
- Art. 13 und 14 Informationspflichten gegenüber Betroffenen
- Art. 15 Auskunftsrecht der Betroffenen
- Art. 17 Recht auf Löschung
- Art. 33, 34 Meldepflichten bei Datenpannen
- Art. 88 Datenverarbeitung im Beschäftigungskontext – Öffnungsklausel

Grundprinzipien der Datenschutz- Grundverordnung



Datenschutzrechtliche Grundsätze, Art. 5 DSGVO

Überarbeitung des Status Quo?!

- Rechtmäßigkeit der Verarbeitung nach Treu, und Glauben, Transparenz, Art. 5 I lit. a) → **allenfalls Transparenz**
 - Zweckbindung, Art. 5 I lit. b) → **präzise genug?**
 - Datenminimierung, Art. 5 I lit. c) → **fehlt oftmals**
 - Datenrichtigkeit, Art. 5 i lit. d) → **oftmals fehlen Korrekturprozesse**
 - Speicherungsbegrenzung, Art. 5 I lit. e) → **fehlt oftmals**
 - Integrität und Vertraulichkeit → Art. 5 I lit. f) → **Einzelfall**
-
- → **Grundsätze stellen gleichzeitig Sicherungsmaßnahmen dar!**

Wann ist Umgang mit personenbezogenen Daten zulässig?

Nichts Neues

- Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)
 - Umgang mit personenbezogenen Daten ist verboten, wenn nicht
 - **Einwilligung** des Betroffenen vorliegt,
 - **Gesetzgeber** die Handlung **explizit erlaubt** (Erlaubnistatbestand).
 - Erfüllung eines Vertrags oder Durchführung einer vorvertraglichen Maßnahme
 - Erfüllung einer rechtlichen Verpflichtung
 - Schutz lebenswichtiger Interessen
 - Erfüllung öffentlicher Aufgaben
 - Wahrung berechtigter Interessen (Erwägungsgrund 48: mögliches berechtigtes Interesse an Übermittlung innerhalb des Konzerns)

Änderungen des BDSG

*Alle reden von
Einwilligung,
wir brauchen sie oft
nicht!*

§ 26 BDSG neu

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(2) „Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer **Einwilligung**, so sind für die Beurteilung der **Freiwilligkeit** der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder der Arbeitgeber oder die beschäftigte Person gleichgelagerte Interessen verfolgen. Die **Einwilligung bedarf der Schriftform, soweit nicht** wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU 2016/679) **in Textform aufzuklären.** (...)

Einwilligung?



- Def. Art. 4 Nr. 11 DSGVO:
- „Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich angegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“

Einwilligung, § 26 II BDSG n.F. (konkretisiert durch den EG 32 DSGVO)

Art. 6 I, 7 DSGVO und § 26 III 3 BDSG n.F.

- keine Schriftform, aber Nachweispflicht
- NEU: Kopplungsverbot
- NEU: Mindestalter
- (16 Jahre als Grenze, Art 8 DSGVO bei Kindern und Jugendlichen)
- Auskunft (Art. 15 DSGVO)

Einwilligung, § 26 II BDSG n.F. (konkretisiert durch den EG 32 DSGVO)

- Art. 6 I, 7 DSGVO und § 26 III 3 BDSG n.F.
- Berechtigung und Löschung (Art. 16, 17 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- erhöhte Transparenzpflichten, „Richtigkeit“, Zweckänderung
- ggf. neue Einwilligung?
- anlassbezogen, ansonsten Rückgriff auf andere Erlaubnistb.
- aus ArbV. herausnehmen

- *Alte Rechtslage:* Umstritten, ob Einwilligung im Beschäftigungsverhältnis möglich ist (Freiwilligkeit?)
- *Neue Rechtslage:* Einwilligung im Beschäftigungsverhältnis ist möglich (EG 155 DSGVO)

Aber: Abhängigkeit und Umstände der Einwilligung berücksichtigen.

- Indiz für Freiwilligkeit, wenn Vorteil für AN oder gleichgelagerte Interessen des AG/AN

Anforderungen aus der DSGVO

**Gilt auch im
Beschäftigten
datenschutz**

- **Informationspflichten** gegenüber dem Betroffenen (Art. 13, 14 DSGVO):
 - Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten
 - Zwecke der Datenverarbeitung
 - Ggf. berechtigte Interessen des Verantwortlichen oder eines Dritten
 - Empfänger/Kategorien von Empfängern personenbezogener Daten
 - Übermittlung von Daten in ein Drittland
 - Dauer der Datenspeicherung/Kriterien für die Dauer der Speicherung
 - Weitergabe von Daten an Auftragsverarbeiter (oder Funktionsübertragung?)
 - Umfang der Betroffenenrechte
- Entsprechendes **Auskunftsrecht** des Betroffenen (Art. 15 DSGVO)
- **Löschungsanspruch** des Betroffenen (Art. 17 DSGVO):
 - „Recht auf Vergessenwerden“

Öffnungsklausel für Beschäftigtendatenschutz



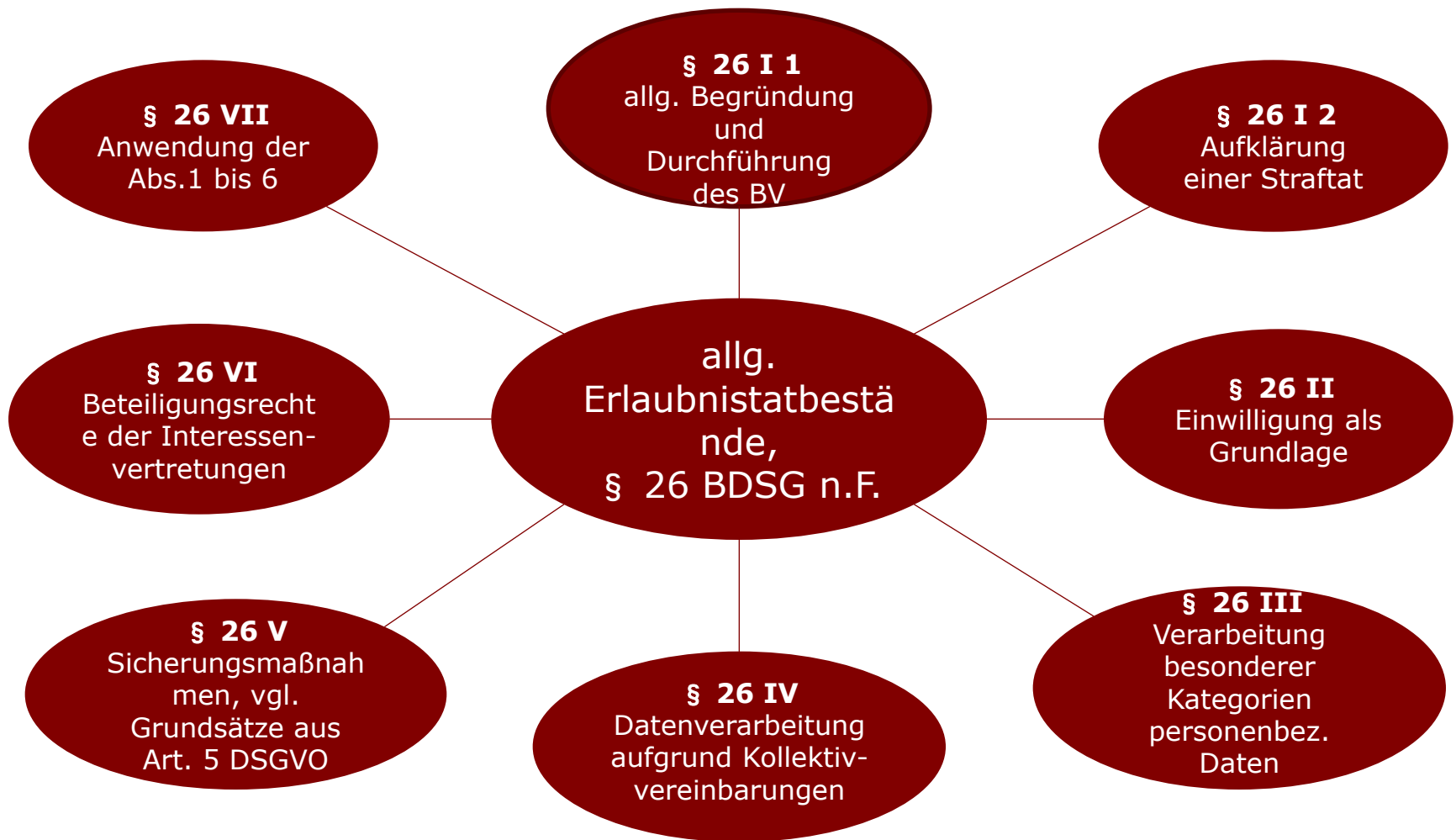
Art. 88 Datenverarbeitung im Beschäftigungskontext

(1) Die Mitgliedstaaten können **durch Rechtsvorschriften oder durch Kollektivvereinbarungen** spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der **Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext**, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeits-platz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses, vorsehen.

(2) Diese Vorschriften **umfassen** angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die **Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe** oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, **und die Überwachungssysteme am Arbeitsplatz.**

§ 26 BDSG neu

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses



Notwendige Vorbereitungsmaßnahmen

Muster-BV für private Nutzung des Internets und des betrieblichen E-Mail-Postfachs:

www.lida.bayern.de



- Erstellung eines **Verarbeitungsverzeichnisses**
 - Was wird wo und wie gespeichert/ausgewertet/genutzt?
- **Überprüfung** der bestehenden arbeitsvertraglichen **Einwilligungen**/Einwilligungen von Kunden bzw. Externen
- Überprüfung der bestehenden **Betriebs/Dienstvereinbarungen/Tarifverträge, Richtlinien, Arbeitsverträge**, etc.

Notwendige Vorbereitungsmaßnahmen

Vgl. hierzu: Kurzpapiere der Bundesbeauftragten für Datenschutz und Informationsfreiheit vom 17.09.2017

www.bfde.bund.de

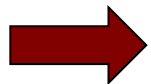


- **Information/Schulung** Mitarbeiter
- Einführung eines **Datenschutzmanagementsystems**
- Datenerhebung, Verarbeitung, Speicherung sauber **dokumentieren**
 - Musterschriftsatz fertigen?

Abschluss einer IT-Rahmenbetrieb/dienstvereinbarung

Mitbestimmungsrecht des BR/PR bei Einführung von IT-Systemen

- 87 Abs. 1 Nr. 6 BetrVG sieht bei Einführung und Anwendung von techn. Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der AN zu überwachen, eine Mitbestimmungspflicht vor („Der BR hat ... mitzubestimmen“).
- BAG, Beschluss vom 21.01.2004, Az.: 1 ABR 7/03: *„Überwachung“ i.S.d. § 87 Abs. 1 Nr. 6 BetrVG ist ein Vorgang, durch den Informationen über das Verhalten oder die Leistung des AN erhoben und – jedenfalls i.d.R. – irgendwie aufgezeichnet werden, um sie auch späterer Wahrnehmung zugänglich zu machen (...). **Zur Überwachung „bestimmt“ sind techn. Einrichtungen dann, wenn sie objektiv geeignet sind, Verhaltens- o. Leistungsinformationen über den AN zu erheben u. aufzuzeichnen; auf die subj. Überwachungsabsicht des AG kommt es nicht an.***
- Betriebssysteme: Dateidownload, Ausführung Programme, öffnen/darstellen Dateien, USB-Nutzung, Account- und Browsernutzung



Mitbestimmung BR

... Die technische Eignung reicht für die Eröffnung des Mitbestimmungsrechts aus ...

- Wächterfunktion des § 68 I, Nr. 2 BPersVG
- § 75 III Nr. 17 BPersVG



Beispiele technischer Überwachungseinrichtungen

- *optische, akustische oder sonstige Kontrollgeräte: Iris- oder Fingerprint-Scanner-System bei biometrischen Zugangskontrollsystemen, Einsatz von Abhörgeräten, Geräten zum Mithören von Verkaufsgesprächen*
- *die Installation von Mikrofonen („Wanzen“)*
- *technische Geräte beim Einsatz von E-Mails und bei der Nutzung des Internets, Fahrtenschreibern*
- *Fernsehmonitore, Fotoapparate, Filmkameras, Multimomentkameras , Mikrofone*
- *Stechuhren, Videoanlagen, Arbeitswirtschaftsinformationssystem ARWIS, die Einführung eines elektronischen Datenverarbeitungssystems*
- *Bürokommunikationssysteme*
- *Standardinternetprogramme*

Einführung neuer IT-Tools

§ 26 IV BDSG: Kollektivvereinbarung

- Datenverarbeitung auf der Grundlage von Kollektivvereinbarungen zulässig
- Art. 88 II DSGVO ist zu beachten: Inhaltliche Anforderungen
- Bes. Maßnahmen zur Wahrung der menschlichen Würde, berechtigter Interessen, Grundrechte

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

- Art 88 II DSGVO umsetzen und beachten
- Datenschutzrechtliche Grundsätze, Art 5 DSGVO*
- Umsetzung der Informationspflicht, Art 12 DSGVO*
- Datenschutzfolgeabschätzung, Art. 35 I 1 DSGVO, sofern einschlägig (Bsp. Abs. 3)
- Weiterer Anpassungsbedarf (= Verhältnismäßigkeit)

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

Hinweis auf Datenschutzgrundsätze (abstrakt):

- Transparenz, Art. 5 Abs. 1 a)
- Umfang der Datenverarbeitung
- Leicht zugängliche, verständliche Information über Datenverarbeitung
- Identität des Verantwortlichen für Datenverarbeitung
- Aufklärung über Risiken, Vorschriften, Garantien, Rechte und deren Geltendmachung, 12-15 DSGVO

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

- Zweckbindung, Art. 5 Abs. 1 b)
- Festgelegte, eindeutige und legitime Zwecke
- Änderungen des Verarbeitungszwecks nur, wenn mit ursprünglichem Erhebungszweck vereinbar
- Datenminimierung und Speicherbegrenzung, Art. 5 Abs. 1 c) und e)
- Beschränkung für die Zwecke der Verarbeitung auf das notwendige Maß
- Identifizierung der betroffenen Personen nur soweit wie für die Zwecke erforderlich

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

- Datenrichtigkeit, Datenaktualität
- Integrität und Vertraulichkeit, Art. 5 Abs. 1 f)
 - Gewährleistung angemessener Sicherheit
 - Geeignete technische und organisatorische Schutzmaßnahmen
 - Kein Zugriff von Unbefugten auf Daten und Geräte

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

Informationspflichten:

- Informationen über Kontakte,
Art. 13 Abs. 1 a), b), e), 14 Abs. 1 a), b), e)
- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Empfänger personenbezogener Daten oder Kategorien von Datenempfängern

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

- Informationen über Einhaltung von Datenschutzgrundsätzen, Art. 13 Abs. 1 c), Abs. 2 a), 14 Abs. 1 c), Abs. 2 a)
 - Zwecke der Datenverarbeitung
 - Datensicherheit
 - Verfahren bei Datenschutzverletzung
 - Dauer der Speicherung, Löschfristen
 - Kriterien für die Festlegung der Dauer, falls Dauer nicht angegeben werden kann
 - Ergebnis der Datenschutz-Folgenabschätzung und der Risikoeinschätzung
 - Hinweis auf Datenverarbeitung in Drittländern
 - Informationen über die Logik einer automatisierten Datenverarbeitung
 - Datenübermittlung innerhalb der Unternehmensgruppe/Konzern
 - Überwachungssysteme am Arbeitsplatz
 - Dokumentations- und Rechenschaftspflichten

Einführung neuer IT-Tools

Also: Anpassung der alten Kollektivvereinbarung ?! → Checkliste:

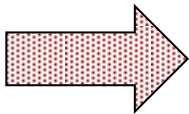
- Informationen über Rechte der Arbeitnehmer, Art. 13 Abs. 2 b), d), 14 Abs. 2 c), e)
 - Auskunft, Art. 15
 - Berichtigung, Art. 16
 - Einschränkung der Datenverarbeitung, Art. 18
 - Löschung, Art. 17, 24
 - Herausgabe von personenbezogenen Daten, Art. 20
 - Widerspruchsrecht bei Profiling-Maßnahmen, Art. 21 Abs. 1, 4 Nr. 4
 - Beschwerderecht bei der Aufsichtsbehörde, Art. 13 Abs. 2 d)

Abschluss einer IT- Rahmenbetriebs/dienstvereinbarung

Was spricht dafür?

Erleichtert Einführung und Einsatz von IT-Systemen

- definiert gemeinsames IT-Grundverständnis
- verhindert ein innovationsfeindliches Klima
- zentrale, wiederkehrende Regelungsbereiche werden „vor die Klammer“ gezogen
- Regelung von Basisstandards
- Absicherung der Mitbestimmungsrechte BR
- gemeinsames Grundverständnis zur Zulässigkeit der privaten Nutzung



Sinnvoll, da viele Vorteile

Abschluss einer IT- Rahmenbetriebs/dienstvereinbarung

Die wichtigsten Regelungsinhalte

- **Präambel und Zielsetzung**
 - Einführung innovativer IT-Systeme wichtig für Wettbewerbsfähigkeit
 - soweit Anforderungen IT-RahmenBV erfüllt, keine weiteren Regelungen
 - moderne IT i.V.m. Schutz Persönlichkeitsrechte MA
 - keine Überwachung von Leistung und Verhalten
- **Systemaufzeichnungen über Benutzerverhalten (Logfiles, Transaktionsprot., etc.)**
 - Zweckbindung
 - Zugriffsberechtigungen
 - Weitergabe von Informationen
 - Speicherfristen
 - Spezifizierung für Anwendersysteme, die Bearbeiterkennzeichen speichern
 - keine Speicherung von Bewegungsdaten

Abschluss einer IT-Rahmenbetriebsvereinbarung

Die wichtigsten Regelungsinhalte

- **Zugriffsberechtigungen**
 - Definition der Speicherbereiche
 - Zugriff auf persönliche Speicherbereiche und E-Mail-Postfach bei längerer Abwesenheit
 - Angelegenheit duldet keinen Aufschub
 - Versuch schriftlicher Einwilligungen MA
 - wenn nicht möglich, BR und HR anwesend, wenn Systemadministrator einsieht
- **Zugriff Systemadministratoren**
 - bei akuter Gefahr für Systemsicherheit
 - keine Weitergabe von Kenntnissen über private Inhalte
 - Einverständnis MA für Zugriff auf private Bereiche

Abschluss einer IT- Rahmenbetriebs/dienstvereinbarung

Die wichtigsten Regelungsinhalte

- **Definition von Systemarten**
 - personaldatenverarbeitende Systeme
 - Grundsätze der Verhältnismäßigkeit, Zweckbindung, Normenklarheit
 - ggf. gesonderte Vereinbarung
 - betriebsdatenverarbeitende Systeme
 - Zweck: Beschreibung und Steuerung von techn. und organ. Abläufen
 - Auswertungen haben Bezug auf Einzelpersonen zu vermeiden
- **Private Nutzung von IT-Arbeitsmitteln**
 - Trennung von Arbeit- und Privatsphäre immer schwieriger
 - betriebliche Nutzung hat absolute Priorität
 - private Nutzung ohne Beeinträchtigung betrieblicher Belange erlaubt; Regelungen in Internet Policy
 - gesonderte BV bei Zugriff über mobile Endgeräte

Abschluss einer IT- Rahmenbetriebs/dienstvereinbarung

Die wichtigsten Regelungsinhalte

- **Qualifizierung und Gesundheitsschutz**
- **Zusammenwirken der Betriebsparteien**
 - Workshop zum Erfahrungsaustausch und zur Projektplanung
 - lokale Workshops möglich
 - neue Systeme werden rechtzeitig vorgestellt; Beratung, ob IT-RahmenBV ausreicht
 - gilt auch für wesentliche Veränderungen aktueller Systeme □ neue Möglichkeiten der Leistungs- und Verhaltenskontrolle, Veränderung Arbeitsorganisation, Ergonomie
 - Ziel: einvernehmliche Regelungen

Überwachungs- und Kontrollmaßnahmen

Empfehlungen der Aufsichtsbehörde

- Schriftliche Vereinbarung bzgl. der betrieblichen und/oder privaten Nutzung

Hierin: eindeutige Festlegung der Fragen bzgl. des Zugriffs, der Protokollierung, Auswertung und Durchführung von Kontrollen und Hinweis auf in Betracht kommende Überwachungsmaßnahmen und Sanktionen

- AG sollte nur die private Nutzung des Internets anbieten, welche auch die Nutzung von Webmail-Diensten umfasst. Private Nachrichten nur von privatem Web-Mail- Account. Betriebliches Postfach ausschließlich betrieblich nutzen.
- Private Nutzung des betrieblichen Accounts gestattet: E-Mails mit erkennbar privatem Inhalt dürfen nur im Umfang der Einwilligung zur Kenntnis genommen werden.
- Hinweis auf Deaktivierung der persönlichen betrieblichen E-Mail-Adresse bei Verlassen des Unternehmens

Überwachungs- und Kontrollmaßnahmen

Beweisverwertungsverbote

- Grundsatz im Zivilrecht: freie richterliche Beweiswürdigung, § 46 II ArbGG, § 286 I 1 ZPO
- □i.E.: Abwägung der widerstreitenden Interessen
- APR des AN und den berechtigten Interessen des AG
- Beweisverwertungsverbot: Kernbereich der Lebensführung
 - (-) bei gezielter Überwachung
 - Abwägung bei Zufallsfunden*
 - Verstoß gegen BV/DV führt nicht automatisch zu Verwertungsverbot
- Grundsatzurteil des BAG (BAG, 20.06.2013, Az. 2 AZR 546/12 BeckRS 2014, 65256): Datenverarbeitung muss erforderlich sein □Interessenabwägung im Einzelfall.
- Sonst gilt: Schwere des Eingriffs berücksichtigen und Verhältnismäßigkeit abwägen, insbesondere, ob der Eingriff in Rechtsordnung durch Eingriff perpetuiert wird.

Das BAG (21.11.2013 – 2 AZR 797/11)

Zur Verwertung der Videoaufzeichnung:

Hinweise für die Praxis:

- Nach § 32 Abs. 1 Satz 2 BDSG (zukünftig: § 26 BDSG) muss der konkrete Verdacht vor der Datenerhebung dokumentiert werden.
- Es muss belegt werden können, dass zur Überprüfung des Verdachts die beabsichtigte Datenerhebung erforderlich und verhältnismäßig ist.
- Weniger einschneidende Mittel zur Aufklärung müssen ausgeschöpft sein. Die verdeckte Überwachung muss praktisch das einzig verbleibende Mittel darstellen und darf nicht unverhältnismäßig sein.
- Bei „Zufallsfunden“ muss das Beweisinteresse des AG höher zu gewichten sein als das Interesse des AN an der Achtung seines allgemeinen Persönlichkeitsrechts.
- Das ist nur anzunehmen, wenn es um eine schwerwiegende Pflichtverletzung geht und die Videoüberwachung selbst dann noch nicht unverhältnismäßig ist.

Noch Fragen?



Dr. Martin Römermann
Rechtsanwalt-Fachanwalt für Arbeitsrecht

SKW Schwarz Rechtsanwälte
Kranzler Eck Kurfürstendamm 21 10719 Berlin

T +49 (0) 30 889 26 50-55
F +49 (0) 30 889 26 50-10

m.roemermann@skwschwarz.de
www.skwschwarz.de