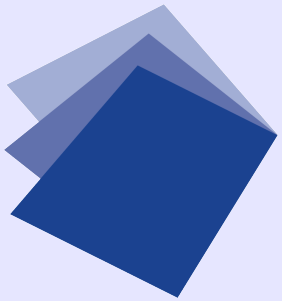
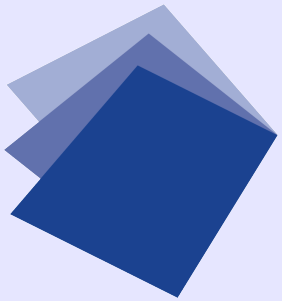
Beschäftigtendaten



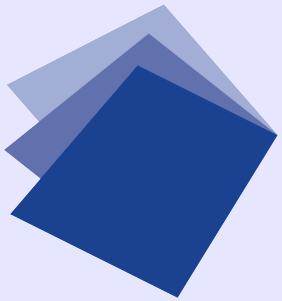
- Beschäftigtendaten, auch besondere Kategorien, dürfen nach Art. 88 DS-GVO i. V. m. § 26 BDSG nur verarbeitet werden:
  - erforderlich für Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses,
  - Einwilligung (gesetzl. Schriftform),
  - kraft Tarifvertrag oder
  - kraft Betriebsvereinbarung.
- Das gilt auch für Daten im Internet und Intranet.

Bewerberdaten - Fragerecht



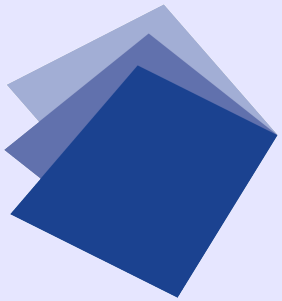
- Fragerecht des Arbeitgebers (§ 26 Abs. 1 BDSG):
  - Schwangerschaft: ✗
  - Sexuelle Orientierung: ✗
  - HIV-Infektion: ✗
  - Religion: ✗
  - Vorstrafen: ✓/✗ (wenn relevant)
  - Schwerbehinderung: ✓/✗ (str.)

Bewerberdaten - Löschung



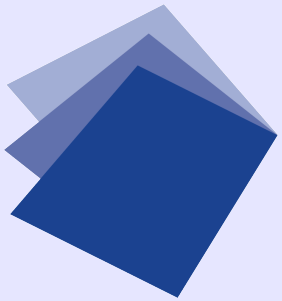
- Bewerberdaten dürfen 4 bis 6 Monate nach Ablehnung gespeichert werden (wegen §§ 15, 22 AGG).
- Speicherung von Bewerberdaten in „Bewerber-Pool“: nur zulässig, wenn im Einzelfall separat eingewilligt wurde.
- Auch bei Einstellung ist die private Telefonnummer grundsätzlich zu löschen (LAG Erfurt 6 Sa 442/17).

Videoüberwachung



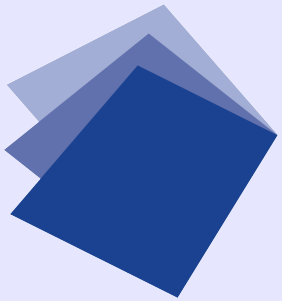
- Videoüberwachung von Mandanten ist nach Art. 6 Abs. 1 Buchst. f nur zulässig, wenn ein überdurchschnittliches Risiko von Straftaten besteht (vgl. BVerwG 6 C 2.18 – Zahnarztpraxis).
- Videoüberwachung von Beschäftigten ist, wenn sie dauerhaft erfolgt, persönlichkeitsrechtswidrig (BAG 1 ABR 16/07).
  - Das BAG lässt dennoch eine Verwertung rechtswidrig erlangter Videoaufnahmen oft zu (etwa BAG 2 AZR 395/15).
- Bei Videoüberwachung: Hinweisschilder mit Info-Pflichten beachten und Daten nach ca. 2 bis 3 Tagen löschen.

Arbeitnehmerüberwachung PC



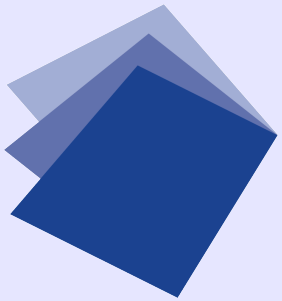
- Der Arbeitgeber darf Internetseiten (ohne Speicherung) sperren (BGH I ZR 3/14).
- Anlasslose Protokollierung von Internetseiten nur, soweit zur technischen Störungsbeseitigung erforderlich (§ 26 BDSG).
- Keine Protokollierung des DSB oder ggf. Betriebsrats, da unabhängig und zur Verschwiegenheit verpflichtet (§§ 79, 99 BetrVG, § 38 BDSG).

Arbeitnehmerüberwachung PC bei Privatnutzung



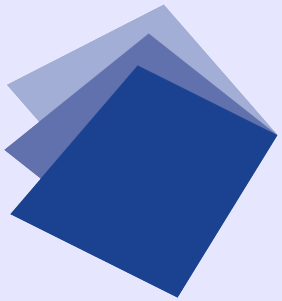
- Bei erlaubter Privatnutzung gilt das Fernmeldegeheimnis (§ 88 TKG).
- Filterung eingehender privater E-Mails ist Nachrichtenunterdrückung nach § 206 StGB (OLG Karlsruhe 1 Ws 152/04).
- Eingehende potenziell private E-Mails darf der Arbeitgeber nicht lesen (§ 206 StGB).
- Für ausgehende potenziell private E-Mails gilt dasselbe, er kann jedoch anweisen, dass der Arbeitnehmer ihn bei dienstlichen Mails manuell auf CC setzt.
- Mögliche Lösung: Privatnutzung untersagen und Funktionsadressen verwenden.

Arbeitnehmerüberwachung PC: Krankheit



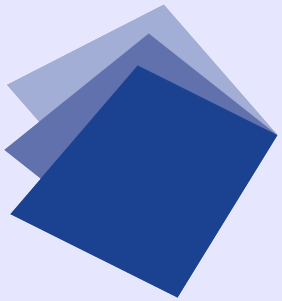
- Bei erlaubter Privatnutzung der E-Mail-Adresse darf der Arbeitgeber auch bei Krankheit des Arbeitnehmers die E-Mails nicht lesen oder automatisch weiterleiten (§ 88 TKG).
- Der Arbeitgeber kann lediglich eine automatische Abwesenheitsnotiz einrichten, wonach eingehende E-Mails nicht gelesen werden, der Absender sich aber an einen Kollegen wenden kann.

Arbeitnehmerüberwachung: Termine und Abwesenheit



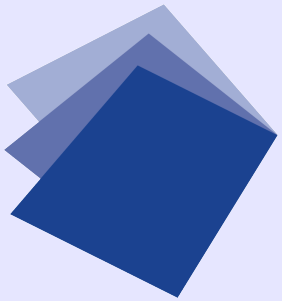
- Termine der Beschäftigten sind im elektronischen Terminkalender grundsätzlich auszublenden.
- Auch Abwesenheitsgründe von Beschäftigten, etwa Krankheit, gehen weder Kollegen noch Mandanten etwas an (§ 26 BDSG), sondern nur die Personalabteilung.

Datenschutz-Compliance



- Mitarbeiter sollten – über § 203 StGB hinaus - auf Datengeheimnis verpfichtet werden (Art. 29 DS-GVO).
- Eine Datenschutz-Richtlinie in der Kanzlei ist dringend zu empfehlen (Art. 29, 5 Abs. 2 DS-GVO, Art. 8 EMRK).
- Bußgeld auch wegen unzureichender Aufsicht möglich (§ 130 OWiG).
- Typische Inhalte einer Datenschutz-Richtlinie:
  - Umgang mit Personal- und Mandantendaten (social media);
  - Privatnutzung dienstlicher Medien;
  - Zugriff auf Beschäftigtendaten bei Abwesenheit;
  - Prüfung neuer Datenverarbeitungs-Vorhaben;
  - Vorgehen bei Folgenabschätzung (Art. 35);
  - Datenschutz-Schulungen;
  - Clean desk policy.

Datenschutz-Compliance IT



- Eine IT-Sicherheits-Richtlinie in der Kanzlei ist wegen Art. 32 DS-GVO ebenfalls zu empfehlen.
- Typische Inhalte einer IT-Sicherheits-Richtlinie:
  - Zulässige IT-Nutzung;
  - App-Installation auf mobilen Geräten;
  - Zugriffsberechtigungen der Mitarbeiter;
  - Passwortqualität und kontrollierte -Rücksetzung;
  - Bildschirmsperre.