Neue Technologien und Datenschutz – Konferenz für Mitarbeitervertretungen

Vortrag:

„Mobiles Arbeiten, BetrVG & Datenschutz“

Referent:

Dr. Robert Selk, LL.M.EUR

Rechtsanwalt

Fachanwalt für IT-Recht

Externer Datenschutzbeauftragter

S S H DATENSCHUTZ · IT · IP

Agenda

1. **Überblick**
2. Rechtliche Eckpunkte
3. Sonderthema: BYOD
4. Wie die Mitarbeiter schützen?
   a. Mitwirkung (1. Stufe)
   b. Mitbestimmung (2. Stufe)
5. Tipps für BV

Überblick

- Thema „Mobiles Arbeiten, BetrVG und Datenschutz“ ist komplex
  - Mobiles Arbeiten
    - berührt viele Themen, Querschnittsmaterie, Definition BMAS:
      - *„Mobile Arbeit zeichnet sich dadurch aus, dass Arbeitnehmer ihre Arbeit von einem Ort außerhalb der eigentlichen Betriebsstätte erbringen. Mobile Arbeit kann entweder an einem Ort, der vom Arbeitnehmer selbst gewählt wird oder an einem fest mit dem Arbeitgeber vereinbarten Ort (z.B. Homeoffice) erbracht werden.“*
  - Datenschutz
    - Durch DSGVO seit 2018 neu, übergeordnetes (reines) EU-Recht
      - Nationales Recht hat kaum noch Bedeutung, kann nur noch spezifizieren
      - Deutschland: Nur 1 Paragraph-zu Beschäftigtendaten, ohnehin nachrangig zur DSGVO
        - UND: Fraglich, ob überhaupt DSGVO-konform, liegt derzeit beim EuGH zur Klärung
  - BetrVG
    - Unterscheidet zwischen „Mitwirkung“ und „Mitbestimmung“ des BR
      - Differenzierung oft nicht einfach, hier ist beides relevant!
- Vorgehen
  - Alle drei Bereiche betrachten und Schnittstellen ermitteln
  - Fokus auf Regelungen zur Technik, BV und Datenschutz

Überblick

- Technische Sicht – um welche Hard- und Software geht es?
  - Beim Mitarbeiter
    - Hardware
      - Notebook, Tablet, Handy, etc. (dienstliches Gerät oder privates Gerät („Bring your own device“ – BYOD“))
    - Software
      - Sog. Container, aber auch: Software zur beruflichen Nutzung
        - Lizenzen? Private? Dienstliche?
      - Schutzsoftware, Filtersoftware, ggf. „Endpoint Protection Software“ (sehr umfängliche Funktionen)
  - Verbindung: Zum Internet und zum Arbeitgeber
    - VPN-Tunnel Software zum Verbindungsaufbau
    - WLAN, LAN, GSM/ LTE-Modul
      - Router oder Handy-Modul (auch hier: Dienstliches oder privates Gerät?)
  - Beim Arbeitgeber: Server und dortige Infrastruktur
    - Gegenstück zur Verbindungssoftware/ VPN-Tunnel
    - Verwaltungs-Software „Mobile Device Management“
    - Sonstige AG-Software-Systeme, zur Datenbereitstellung, den Datenbanken, Servern, etc.
- Also: Überall „technische Einrichtungen“ iSv § 87 Abs. 1 Nr. 6 BetrVG
  - Was heißt dies rechtlich?

Agenda

1. Überblick
2. **Rechtliche Eckpunkte**
3. Sonderthema: BYOD
4. Wie die Mitarbeiter schützen?
   a. Mitwirkung (1. Stufe)
   b. Mitbestimmung (2. Stufe)
5. Tipps für BV

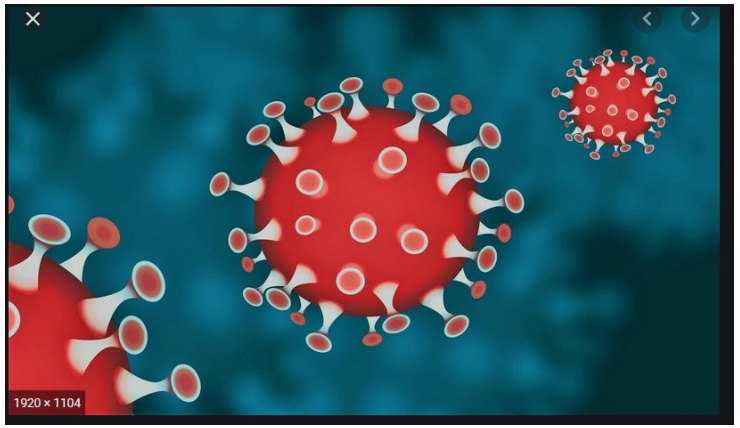
Rechtliche Eckpunkte

- Achtung: DSGVO kennt als EU-Recht „Betriebsrat“ oder „BetrVG“ nicht
  - „Natürlich“ nicht, ist nur in 1 aus 27 Ländern ein dortiges, nationales Spezialgebiet
- Wichtig: Datenschutz und BetrVG verfolgen sehr unterschiedliche Ziele
  - Datenschutz
    - Schutz der Menschen vor einer Verdatung → „Verdatungsschutz“
      - Nicht „Schutz der Daten“ (dies wäre die „Datensicherheit“) !!
    - Ziel/ Inhalt: Verarbeitung personenbezogener Daten muss rechtskonform sein
      - Was erlaubt ist, regelt der (EU-)Gesetzgeber in den (EU-)Datenschutzgesetzen
      - Und zwar aufgrund der DSGVO: EU-weit, reines Europarecht
  - BetrVG
    - Regelt die Mitbestimmung des BR an Vorhaben des AG → sehr deutsches Recht, rein national
    - Setzt Datenschutz-Rechtmäßigkeit zwingend voraus!
      - Diese ist also nicht Gegenstand des BetrVG, ist vielmehr Selbstverständlichkeit (ansonsten ja verboten)
    - Hat Blick gerade nicht auf den einzelnen Mitarbeiter, sondern das „Kollektiv“ → Alle
      - „Kollektives“ Arbeitsrecht
    - Es geht also nicht – wie beim Datenschutz – um die einzelnen Betroffenen, sondern um eine technische Einrichtung insgesamt, um diese „als solche“

Rechtliche Eckpunkte

- Merksatz zum

Datenschutz



Rostschutz = schützt auch nicht den Rost, sondern VOR dem Rost

Agenda

1. Überblick
2. Rechtliche Eckpunkte
3. **Sonderthema: BYOD**
4. Wie die Mitarbeiter schützen?
   a. Mitwirkung (1. Stufe)
   b. Mitbestimmung (2. Stufe)
5. Tipps für BV

Sonderthema: BYOD

- Was gilt bei BYOD? Wie sind Mitarbeiter geschützt?
  - „BYOD“ – „bring your own device“ → Nutzung von Privatgeräten für Dienstzwecke
- Diverse rechtliche Probleme, u.a.
  - Problem 1: Daten auf privaten Geräten sind der Herrschaft und IT-Security des Unternehmens entzogen
    - Kann DSGVO-Verstoß darstellen, auch Verstoß gegen Datensicherheit, Verstoß gegen Steuerrecht
    - U.U. Verstoß gegen Kundenverträge o.Ä., wonach Privatgeräte verboten sein können? → Vertragsstrafen
  - Problem 2: Unternehmen darf nicht einfach auf Privatgerät zugreifen, Einwilligung nötig! U.a. wegen:
    - Strafrecht („fremde Sache“)
    - Datenschutz (wegen dortiger privater Daten)
    - ePrivacy (wegen Eingriff in Privatsphäre – ähnlich wie Schutz der Privatwohnung)
  - Problem 3: Wer ist Eigentümer? Was, wenn nicht Mitarbeiter, sondern z.B. Ehegatte?
  - Problem 4: Lizenzrecht
    - Viele Software-Lizenzen sind für Privatnutzung kostenlos, nicht aber für kommerzielle Nutzung!
    - Lizenzverstoß durch den Arbeitnehmer!
  - Problem 5: Steuerrecht bzw. Vergütungspflicht? Versicherung?
  - Problem 6: Arbeitszeit
  - Etc.

Sonderthema: BYOD

- Diverse Lösungen, z.T. kombiniert
  - Am besten: Technischer Ansatz
    - „Große Lösung“:
      - Schaffen einer isolierten Insel innerhalb des Privatgeräts, die dem Dienstgerät rechtlich gleichgestellt wird („Container“) → Darauf darf AG „ganz normal“ zugreifen, da rein dienstlich → fern-löschen, etc.
    - „Kleinere Lösungen“
      - Zumindest eigene dienstliche Apps (wie M365), die dortige Daten in sich oder gleich nur in der Cloud des AG speichern
        - → Privatgerät bleibt frei davon
      - Oder: zumindest lokaler (rein dienstlicher, abgetrennter) Netzwerk-Speicherort auf AG-Server/ Cloud
  - Zur Not: Organisatorische und /oder nur rechtliche Lösungen
    - Dienstanweisung, dienstliche Daten etwa verschlüsseln zu müssen, Gerät nicht aus der Hand zu geben, auch nicht an Familienangehörige, abzusperren, etc.
    - Problem: Schwierig, oft nicht umsetzbar, wenig sicher
  - Praxis:
    - Meist Kombinationen, je nach Betroffenengruppe
- Praxis für BRs
  - Mitbestimmt nach § 87 Abs. 1 Nr. 6 BetrVG?
    - Ja, soweit technische Einrichtung (ja) und Leistungs-/ Verhaltensdaten (ja), ggf. auch § 87 Abs. 1 Nr. 1 (betriebliche Ordnung)
  - Also: BYOD – wenn relevant - muss in Gesamtkonzept des mobilen Arbeitens mitberücksichtigt werden!

Agenda

1. Überblick
2. Rechtliche Eckpunkte
3. Sonderthema: BYOD
4. Wie die Mitarbeiter schützen?
   a. **Mitwirkung (1. Stufe)**
   b. Mitbestimmung (2. Stufe)
5. Tipps für BV

Stufenbild

- 2 Treppenstufen-Modell

Step 2: Mitbestimmungsrechte BR **(→ § 87 ff BetrVG, hier auch: Art. 88 DSGVO)**

- Hier: technische Einrichtungen: § 87 Abs. 1 Nr. 6 BetrVG
- Auch
  - Allg. Beurteilungsgrundsätze: § 94 BetrVG
  - Bildungsmaßnahmen: § 98 BetrVG
  - Lohngestaltung: § 87 Abs. 1 Nr. 10 BetrVG
  - Etc.

Mitbestimmung

Step 1: Einhaltung der Gesetze **(→ § 80 I 1 BetrVG)**

- ~~Arbeitsrecht~~
- **Datenschutz**
- ~~Ggfls. auch andere~~ Gesetze
  - Steuerrecht
  - Kartellrecht
  - Spezialgesetze, sofern zum Schutz
    - SGB, BundesurlaubsG, etc.

Datenschutz, DSGVO, ergänzend BDSG, u.a.

- Verarbeitungsverzeichnis
  + Rechtsprüfung zur Zulässigkeit
- Datenschutz-Hinweise
- Rollenkonzept und Löschkonzept
- Datenschutz-Folgenabschätzung
- Auftragsverarbeiter (AV)
- Etc.

Mitwirkung

1. Stufe

- § 80 Abs. 1 Nr. BetrVG
  - *„Der Betriebsrat hat folgende allgemeinen Aufgaben (…)*
    - *1. darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden;“*
  - U.a. auch: Die Datenschutzgesetze
    - Primär: DSGVO (ggf. ergänzend sekundär nationale Normen, wie BDSG)
- Wie kann der BR dies umsetzen?
  - Vom AG die datenschutzrechtlich nötigen Datenschutz-Dokumentationen zeigen lassen und prüfen
    - Selbst und/ oder durch Sachverständigen
    - Nämlich: Siehe Treppenstufen-Bild
  - Ziel: Eigenes rechtliches Bild und Einschätzung des BR von
    - Art und Weise, Umfang und Details der Verarbeitung von Mitarbeiterdaten
    - Datenschutzrechtlicher Zulässigkeit
    - Einhaltung aller Datenschutz-Begleitpflichten
      - Datenschutz-Hinweise, Löschen, interne Dokumentation
  - Anmerkung: BR wird in Literatur zum Teil als eine Art „zweiter Datenschutzbeauftragter“ bezeichnet
    - Wenngleich natürlich mit klar parteiischem Blick, DSB dagegen ist neutral

1. Stufe

- Wie erreichen?
  - BR steht aus § 80 BetrVG umfangreicher Auskunftsanspruch gegenüber Arbeitgeber zu
    - Nicht unbedingt zwingend auf die genannten Dokumente als solches, aber den Sachverhalt und Bewertung
  - Was, wenn AG Herausgabe verweigert?
    - Dann muss BR selbst alles (nochmals) prüfen
    - Dafür fast immer Sachverständiger nötig, da komplexe Rechtslage → hohe Kosten
    - Führt dann oft doch zur Herausgabe bzw. (erst) der Erledigung der Themen durch den AG
- Vorgehen
  - Oft gemeinsam in einer gemeinsamen „AG-BR-Arbeitsgruppe“ zur Produktvorstellung, Vorstellung der Datenschutz-Konzepte, Besprechung, Diskussion, gemeinsamer Input, etc.
  - Viele Themen im Datenschutz sind gemeinsame Themen, weniger Verhandlungsthemen
  - In Stufe 1 ohnehin reine Mitwirkung, noch keine Mitbestimmung

Agenda

1. Überblick
2. Rechtliche Eckpunkte
3. Sonderthema: BYOD
4. Wie die Mitarbeiter schützen?
   a. Mitwirkung (1. Stufe)
   b. Mitbestimmung (2. Stufe)
5. Tipps für BV

Stufenbild

- 2 Treppenstufen-Modell

Step 2: Mitbestimmungsrechte BR **(→ § 87 ff BetrVG, hier auch: Art. 88 DSGVO)**

- Hier: technische Einrichtungen: § 87 Abs. 1 Nr. 6 BetrVG
- Auch
  - Allg. Beurteilungsgrundsätze: § 94 BetrVG
  - Bildungsmaßnahmen: § 98 BetrVG
  - Lohngestaltung: § 87 Abs. 1 Nr. 10 BetrVG
  - Etc.

Mitbestimmung

Step 1: Einhaltung der Gesetze **(→ § 80 I 1 BetrVG)**

- Arbeitsrecht
- **Datenschutz**
- Ggf. auch andere Gesetze
  - Steuerrecht
  - Kartellrecht
  - Spezialgesetze, sofern zum Schutz
    - SGB, BundesurlaubsG, etc.

Datenschutz, DSGVO, ergänzend BDSG, u.a.

- Verarbeitungsverzeichnis
  + Rechtsprüfung zur Zulässigkeit
- Datenschutz-Hinweise
- Rollenkonzept und Löschkonzept
- Datenschutz-Folgenabschätzung
- Auftragsverarbeiter (AV)
- Etc.

Mitwirkung

2. Stufe

- Frage: Besteht bei mobilem Arbeiten ein Mitbestimmungsrecht des BR?
  - § 87 Abs. 1 Nr. 6 BetrVG
    - *„Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen:*
      - *6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;“*
    - Identisch übrigens: § 80 Abs. 1 Nr. 21 BPersVG (ähnlich in den Ländern-Personalvertretungsgesetzen)
  - Also – folgende Voraussetzungen müssen erfüllt sein:
    1. Technische Einrichtung? Hier: Ja, siehe oben, Hard- und Software
       - Jede? Nein, nur soweit „Bestimmung/ objektive Eignung zur Leistung- oder Verhaltensüberwachung“
    2. Leistungs- und/ oder verhaltensrelevante Daten? → Abhängig von eingesetzter Hard- und Software
       a. Verhaltensrelevante Daten:
          - Wohl fast immer, da Verhaltensdaten zwangsläufig anfallen (Login, Zeitpunkt, Datenmenge, Rollen und Berechtigungen, Protokolle, Logfiles, etc.)
       b. Leistungsdaten:
          - Beim mobilen Arbeiten dagegen meist nur in Ausnahmefällen

2. Stufe

- Siehe obige Folie
  - Beim Mitarbeiter
    - Hardware
      - Notebook, Tablet, Handy, etc. (dienstliches Gerät oder privates Gerät („Bring your own device“ – BYOD“))
    - Software
      - Sog. Container, aber auch: Software zur beruflichen Nutzung
        - Lizenzen? Private? Dienstliche?
      - Schutzsoftware, Filtersoftware, ggfls. „Endpoint Protection Software“ (sehr umfängliche Funktionen)
  - Verbindung zum Internet und zum Arbeitgeber
    - VPN-Tunnel Software zum Verbindungsaufbau
    - WLAN, LAN, GSM/ LTE-Modul
      - Router oder Handy-Modul (auch hier: Dienstliches oder privates Gerät?)
  - Beim Arbeitgeber: Server und dortige Infrastruktur
    - Gegenstück zur Verbindungssoftware/ VPN-Tunnel
    - Verwaltungs-Software „Mobile Device Management“
    - Sonstige AG-Software-Systeme, zur Datenbereitstellung, den Datenbanken, Servern, etc.

2. Stufe

- Wie ist die Mitbestimmung durch BR auszuüben?
  - § 87 BetrVG: Durch eine „Betriebsvereinbarung“
    - Regelungsabrede?
      - Nein, kennt das BetrVG nicht, die DSGVO und das BDSG auch nicht, beschränken sich auf „Kollektivvereinbarungen“
      - Regelungsabrede hätte auch keine Wirkung für und gegen Mitarbeiter!
        - Bindet nur AG und BR, meist für organisatorische Themen zwischen AG und BR
  - Inhalt der BV
    - Regelung zur Einführung und Anwendung der (aller) vorgenannten „technischen Einrichtungen“
- Achtung – Art. 88 Abs. 2 DSGVO beinhaltet formale Vorgaben an BVs
  - Zitat
    - *„Diese Vorschriften* [SELK: in der BV zur Verarbeitung personenbezogener Beschäftigtendaten] *umfassen geeignete 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.“*
  - BV muss also zwingend „geeignete und besondere Maßnahmen“ enthalten
  - Praxistipp: Diese müssen ohnehin in der 1. Stufe herausgearbeitet worden sein, sich derer bedienen

Zwischenergebnis

- 2 Ebenen für BR wichtig
  - Individual-Ebene (→ Stufe 1)
    - BR achtet darauf, dass AG die (Datenschutz-)Gesetze einhält und die bei mobilem Arbeiten eingesetzte Hard- und Software datenschutz-konform eingekauft und implementiert ist sowie betrieben wird (§ 80 Abs. 1 Nr. 1 BetrVG)
  - Kollektivebene (→ Stufe 2)
    - BV, die Verarbeitung der (leistungs- und verhaltensrelevanten) Beschäftigtendaten genau regelt und Beschäftigte vor - übermäßiger - „Verdatung“ durch AG schützt, bestimmte Prozesse definiert, Transparenz schafft durch Rollen- und Berechtigungskonzepte, Zugriffskonzepte, Löschkonzept, Änderungskonzept, etc.
- Welche Dokumente sollte es am Ende geben?
  1. DS-Hinweise: Gut verständliche und präzise „Mitarbeiter-Datenschutzhinweise Mobiles Arbeiten
  2. In der Regel: Zusatzvereinbarung zum Arbeitsvertrag zum mobilen Arbeiten
     - Wenn BYOD: Dito – auch hier (weitere) Zusatzvereinbarung wichtig bzw. zumeist sogar der Themen wegen zwingend nötig
  3. Betriebsvereinbarung

Agenda

1. Überblick
2. Rechtliche Eckpunkte
3. Sonderthema: BYOD
4. Wie die Mitarbeiter schützen?
   a. Mitwirkung (1. Stufe)
   b. Mitbestimmung (2. Stufe)
5. **Checkliste/ Tipps für BV**

Checkliste/ Tipps für BVs

- ✓ Regelungsgegenstand: Was genau? Hardware? Software? Welche genau?
  - Client-Gerät + dortige Software, ggf. auch Verbindungs-Software
  - Server-Software, ggf. Cloud-Komponenten
- ✓ Daten: Welche Daten sind leistungs- oder verhaltensrelevant?
  - Am besten in Anlage zur BV aufnehmen + definieren
  - Vorsicht bei: Geodaten/ GPS-Funktion
- ✓ Kontrollen: Regelungen zur Leistungs- und Verhaltenskontrolle
  - Leistungskontrolle: Wohl in Praxis nie nötig → zu 100 % verbieten
  - Verhaltenskontrolle: Durchaus wichtig, etwa Login-Zeiten (Sicherheit), aufgerufene Seiten (Blocken, Schutz vor Viren, Mal- oder Spyware, etc.)
  - Regelungen zu Reports und Auswertungen
- ✓ Technische Regelung
  - Zugriffsprozess auf (LV-)Daten: Zwecke, Ablauf, ggf. 4-Augenprinzip, Formularwesen
  - Rollen- und Berechtigungskonzept + Löschkonzept
  - Schnittstellen, Beteiligte Dritte – AV-Dienstleister

Checkliste/ Tipps für BVs

- ✓ Vorgaben zur Gerätenutzung?
  - „Do‘s and Don‘t‘s“
  - Hier ggf. auch Arbeitszeitthemen
- ✓ Regelungen zu Systemänderungen
  - Mechanismus v.a. zu kurzfristigen herstellerseitigen Änderungen
    - Idee: Duldung durch BR, bis Regelung; AG darf solange Daten nicht zur LV-Kontrolle verwenden
- ✓ Wenn Privatgeräte / BYOD
  - Sonderthemen berücksichtigen, siehe oben
- ✓ Kontrollrechte und Sanktionen
  - Kontrollrechte des BR + wo verhandelbar: Beweisverwertungsverbot
    - Achtung: Wird von den Gerichten aber oft NICHT anerkannt!
- ✓ Art. 88 DSGVO
  - Maßnahmen u.a. zur Transparenz sind zwingend!

- Fazit

Fazit – Worauf sollte BR achten?

- Wichtig: Gute Dokumente und Dokumentation – zur rechtlichen Absicherung
  - Gegenüber Mitarbeitern
    - Mitarbeiter-Datenschutz-Hinweise zum mobilen Arbeiten
    - Zusatzvereinbarung mobiles Arbeiten, ggf. mit Beachtung BYOD/ eigene BYOD-Zusatzvereinbarung
    - Betriebsvereinbarung (Dienstvereinbarung) als übergeordneter Rahmen
      - Dort die verschiedenen Aspekte beachten, v.a. auch Art. 88 DSGVO „Schutzmaßnahmen“
  - Im Hintergrund - Vollständige Datenschutz-Dokumentation, v.a.:
    - Verarbeitungsverzeichnis, Art. 30 DSGVO
    - Prüfung + Dokumentation der datenschutzrechtlichen Zulässigkeit, Art. 5 Abs. 2 DSGVO
    - diverse Konzepte (Rollen-/ Berechtigungen, Löschen, Zugriffe, etc.), Art. 25, 32 DSGVO
    - Datenschutz-Folgenabschätzung: Prüfung Erforderlichkeit, ggf. Durchführung, Art. 35 DSGVO
- Nicht vergessen: Gelegentliche Kontrollen durch BR
  - § 80 Abs. 1 Nr. 1 BetrVG: Einhaltung der Datenschutzgesetze, aber auch von BVs!
- Insgesamt
  - Kein einfaches Thema, vielschichtig, Zeit für Verhandlungen wichtig, nicht „schnell-schnell“ agieren
  - Siehe auch zu Beginn: Arbeitszeit-Themen, steuerliche Themen, Lizenzen, etc.

Vielen Dank!

Fragen?

Dr. Robert Selk, LL.M. EUR

selk@ssh-law.de

S S H DATENSCHUTZ · IT · IP