SUFFEL & KOLLEGEN
RECHTSANWÄLTE

I. Einführung

II. Weichenstellung: Art der Nutzung

III. Datenschutzrechtliche Grundlagen

IV. Kollektivrechtliche Grundlagen

V. Gestaltungsmöglichkeiten

VI. Reaktionsmöglichkeiten bei Pflichtverstößen von Arbeitnehmern

VII. Risiko I: Haftung gegenüber Dritten

VIII. Risiko II: Strafrechtliche Aspekte

I. Einführung

1. Von der realen zur virtuellen Realität
   a) aus unternehmerischer Sicht (Sicherheit u. Leistungskontrolle)
   b) aus Arbeitnehmersicht (Überwachungsfreiheit)
2. Technische Grundlagen
   -> „Achillesferse" Firewall
3. Rechtliche Rahmenbedingungen
   -> Kein spezielles AN-Datenschutzrecht
   -> EU-Richtlinie in Planung
   -> Interessenausgleich über Datenschutz- und Arbeitsrecht

II. Weichenstellung (1)

1. Privatnutzng

-> jede nicht dienstliche Außenkommunikation ist privat

2. Dienstliche Nutzung

-> dienstliche Nutzung, wenn dienstl. Bezug (+)

II. Weichenstellung (2)

Umfang der Nutzungsbefugnisse ?

Grundsatz: ob und Umfang der privaten E-mail und Internetnutzung = Entscheidungshoheit des AG

Aber: spezielle Diskriminierungsverbote und arbeitsrechtlichen Gleichbehandlungsgrundsatz

Mittel: Einzelweisung, Internetpolicy, Arbeitsvertrag, Benutzungsordnung, Betriebsvereinbarung

Art: ausdrücklich - konkludent

II. Weichenstellung (3)

Problem: Konkludente Regelung zu auch privaten Nutzung von Email und Internet

1. Keine vermutete Einwilligung des AG

2. Betriebliche Übung

AG kennt die private Nutzung oder hätte sie kennen müssen und hat sie geduldet;

Zeitraum 6-12 Monate

II. Weichenstellung (4)

Reichweite der Befugnis zur *auch privaten Nutzung ?*

-> Umfang der erteilten Erlaubnis maßgeblich

-> uneingeschränkte Erlaubnis bedeutet kein Recht zur schrankenlosen Privatnutzung

-> Problem: ohne klare Regelung lässt sich die Abgrenzung“noch erlaubt / bereits verboten“ mangels fehlender rechtlicher Vorgaben kaum ziehen

II. Weichenstellung (5)

Pflicht zur Nutzung von Email und Internet ?

-> Ja, bei entsprechender Einweisung

Konsequenzen für AN beim fehlerhaften Umgang mit der IuK-Technologie ?

-> u.U., bei entsprechender Einweisung und konkreter Regelung seitens des AG

III. Datenschutzrechtliche Grundlagen

1. Ausgangspunkt:

   Das Recht auf informationelle Selbstbestim-Mund

2. Gesetzliche Grundlagen

   a) BDSG

   b) TKG

   c) TMG

3. Tarifverträge oder Betriebsvereinbarungen

4. Einwilligung

III. Datenschutzrechtliche Grundlagen (1)

Das Recht auf informationelle Selbstbestimmung, Art 2 Abs. 1 i.V.m. Art 1 GG

-> „Herrschaft" über die eigenen Daten

-> Abwehrrecht des Bürgers gegen den Staat

-> und Bestandteil der objektiven Wertordnung

=> z.B. Fürsorgepflicht des AG für den AN

III. Datenschutzrechtliche Grundlagen (2)

BDSG (Bundesdatenschutzgesetz)

-> Auffanggesetz; greift nur wenn andere gesetzliche Vorschriften nicht greifen;

-> § 4 Abs.1: Erhebung, Verarbeitung, Nutzung und Übermittlung personenbezogener Daten nur, wenn von BDSG oder anderen RV vorgesehen oder Einwilligung des Betroffenen vorliegt

-> § 32 BDSG: EVNÜ+, Zweckbestimmung des Arbeitsverhältnisses oder berechtigte Interessen des AG überwiegen das schutzwürdige Interesse des AN

-> § 31 BDSG: Datensicherung und Gewähr der EDV

III. Datenschutzrechtliche Grundlagen (3)

gesetzliche Rechtfertigung:

-> § 32 BDSG: EVNÜ+, Zweckbestimmung des Ar beitsverhältnisses oder berechtigte Interessen des AG überwiegen das schutzwürdige Interesse des AN

-> § 31 BDSG: Datensicherung und Gewähr der EDV

-> Tarifverträge (selten)

-> Betriebsvereinbarung -> Mitbestimmungsrecht des Betriebsrates bei Einführung technischer Überwachungsmaßnahmen, § 87 Abs. 1 Nr. 6 Be trVG

-> schriftliche vorherige Einwilligung, §§ 4, 4a BDSG

III. Datenschutzrechtliche Grundlagen (5)

Knackpunkt Telekommunikationsgesetz (TKG)

Zweck: Förderung des Wettbewerbs, flächendeckende Versorgung mit Telekommunikation und ***Wahrung der Nutzerinteressen****, insbesondere*

-> Wahrung des Fernmeldegeheimnisses und

-> Wahrung des Datenschutzes

Dem Fernmeldegeheimnis und datenschutzrechtlichen An forderungen ist nur ein „**Diensteanbieter**", unterworfen, **§ 88 Abs. 2, Satz 1 TKG**

III. Datenschutzrechtliche Grundlagen (6)

Knackpunkt Telekommunikationsgesetz (TKG)

„**Diensteanbieter**", § 3 Nr. 6a, b TKG ist

„jeder, der ganz oder teilweise geschäftsmäßig Telekom munikationsdienste erbringt oder an der Erbringung von Telekommunikationsdiensten mitwirkt".

geschäftsmäßiges Erbringen, **§ 3 Nr. 10 TKG** + wenn

„***Dritten* nachhaltig Telekommunikation mit oder ohne Gewinnerzielungsabsicht angeboten wird"**

Arbeitnehmer ist „Dritter", wenn Email & Internet auch für die private Nutzung zur Verfügung gestellt werden

III. Datenschutzrechtliche Grundlagen (7)

Knackpunkt Telekommunikationsgesetz (TKG)

Konsequenz:

AG unterliegt gegenüber AN dem Fernmeldegeheimnis und den datenschutzrechtlichen Anforderungen des TKG. Damit ist eine **Erhebung, Verarbeitung oder Nutzung** der bei der Nutzung von email und Internet entstehenden Daten nur noch möglich, wenn dies gerechtfertigt ist, also der AN in die EVN seiner Daten **eingewilligt** hat, oder aber ein gesetzlicher **Rechtfertigungs-tatbestand** vorliegt. Dabei differenziert das TKG zwischen **Be-stands- und Verbindungsdaten**

III. Datenschutzrechtliche Grundlagen (8)

Knackpunkt Telekommunikationsgesetz (TKG)

Bestandsdaten:

sind Daten eines ***Teilnehmers***, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, § 3 Nr. 3 TKG

Verkehrsdaten:

sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, § 3 Nr. 30 TKG.

III. Datenschutzrechtliche Grundlagen (8)

§§ 91 ff TKG regeln den Datenschutz für Telekommunikationsdaten der Teilnehmer und Nutzer

-> § 95 Abs. 1 Satz 1 TKG i.V.m. § 3 Nr. 3 TKG:
EVN der Bestandsdaten eines Teilnehmers +, wenn für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erforderlich ist.

-> § 97 Abs. 1 Satz 1 TKG
Verkehrsdaten nach § 96 Abs. 1 Nrn. 1 bis 5 TKG dürfen verwendet werden, soweit diese Daten zur Ermittlung des Entgelts und zur Abrechnung benötigt werden.

III. Datenschutzrechtliche Grundlagen (9)

Erhebung und Nutzung von Bestands- und Verkehrsdaten von Teilnehmern und Nutzern

-> **§ 100 Abs. 1 TKG**:

, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanla gen erforderlich ist,

-> § 100 Abs. 3 TKG:

, soweit dies bei Vorliegen konkreter Verdachtsmomente der Aufdeckung / Unterbindung von Leistungserschleich- ungen oder rechtswidrige Inanspruchnahmen von Tele kommunikationsdiensten erforderlich ist

III. Datenschutzrechtliche Grundlagen (10)

-> Maßnahmen, die nicht von den genannten gesetzlichen Recht fertigungsgründen gedeckt, bedürfen es der ausdrücklichen Einwilligung, die nach § 94 TKG auch elektronisch erfolgen kann;

-> außerdem muss AG geeignete Schutzmaßnahmen ergreifen, um den Zugriff unbefugter Dritter auf die Daten des AN zu verhindern

III. Datenschutzrechtliche Grundlagen (11)

Telemediengesetz (vormals TDG und TDDSG)

Findet keine Anwendung auf Dienst- und Arbeitsverhältnisse

Aber bei auch „privater Nutzung“ wird der AG zum Dienstean-bieter. Damit gelten dann die datenschutzrechtlichen Bestim-mungen des TMG auch im Verhältnis zum AN, d.h. Das Anony-misierungsgebot des TMG gilt auch hier mit der Konsequenz, dass insbesondere die Auswertung von Internet und E-mail logfi-les nur bei entsprechender Rechtfertigung gegeben ist.

IV. Kollektivrechtliche Grundlagen

1. Mitbestimmung in Fragen der Ordnung des Betriebs gemäß § 87 Abs. 1 Nr. 1 BetrVG

   -> Ordnungsverhalten; subsidiär zu Abs.1 Nr.6

2. **Einführung technischer Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG**

3. Personalvertretungsrechtliche Regelungen

   -> entsprechen weitestgehend den Regelungen des BetrVG

IV. Kollektivrechtliche Grundlagen (1)

Einführung technischer Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG - zentrale Norm im IT-Bereich

Zweck:

-> Schutz der Persönlichkeitrechte des AN;

-> Wahrung der Persönlichkeitsrechte im Falle einer Überwachung

Voraussetzung:

-> Technische Einrichtung zur Überwachung, z.B. Fire wall (Geeignetheit genügt)

IV. Kollektivrechtliche Grundlagen (2)

Einführung technischer Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG - zentrale Norm im IT-Bereich

Reichweite: Einführung und Anwendung

-> ab der Entscheidung des AG bzgl. Einführung eines Überwachungssystems; Geeignetheit genügt

-> bei trennfähigen Softwaresystemen besteht das Mitbestimmungrecht nur bzgl. der Überwachungskomponente

-> keine Mitbestimmung, wenn vollständige Anonymisierung der Daten erfolgt (selten)

IV. Kollektivrechtliche Grundlagen (3)

Einführung technischer Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG - zentrale Norm im IT-Bereich

Schranken der Mitbestimmung

-> entgegenstehende gesetzliche oder tarifliche Regelung

-> § 75 Abs. 2 BetrVG: Mitbestimmung als unzulässiger Ein griff in das Persönlichkeitsrecht des AN

IV. Kollektivrechtliche Grundlagen (4)

Sonstige Rechte des Betriebsrates zur Wahrung der Mitbestimmung:

- **->Informationsrechte nach § 80 Abs. BetrVG**
- **-> Mitbestimmungsrecht bei Schulungsmaßnahmen bzw. Maßnahmen der betrieblichen Weiterbildung**

V. Gestaltungsmöglichkeiten (1)

1. Arbeitsvertrag
2. Betriebs- oder Dienstvereinbarung

-> Einräumung der Nutzungsbefugnisse als freiwillige Leistung

->Klare und eindeutige Regelung bzgl. Zulässigkeit der Art der Nutzung

-> In jedem Fall Regelungen

zur Einhaltung technischer Schutzmaßnahmen

Datenschutz und Schutz von Betriebsgeheimnissen

3. Ohne Regelung → betriebliche Übung

V. Gestaltungsmöglichkeiten (2)

Regelungen bei Gestattung der privaten Nutzung

-> Widerrufsvorbehalt, Vorrang der dienstlichen Nutzung
(Betr. Übg. i.d.R. nicht widerruflich; Änderungskdg.)

-> Zeit-/mengen-/ typenmäßige Einschränkung der Privat nutzung

-> Arbeitnehmerdatenschutz und Kontrollbefugnisse des Ar beitgebers

-> Trennung von dienstlicher und privater Nutzung, z.B. un terschiedliche Passwörte, getrennte Email acounts

-> Kostenbeteiligung des Arbeitnehmers

-> **Vertretungsregelungen!**

VI. Handlungsoptionen bei Pflichtverstößen von Arbeitnehmern

1. Arbeitsrechtliche Reaktionsmöglichkeiten

-> Aufklärung / Abmahnung / Kündigung

-> Rechtsprechungsbeispiele

2. Haftung des Arbeitnehmers für Pflichtverstöße

-> Grundsatz: Haftung für jeden schuldhaften Verstoß

-> Einschränkung der Haftung bei betrieblich veranslasster Tätigkeit

3. Aber:

Verwertungsverbot für rechtswidrig, insbesondere da tenschutzwidrig erlangte Informationen

VII. Risiko 1 - Haftung gegenüber Dritten

1. Haftung aus bestehenden Vertragsverhältnissen
   -> Weitergabe sensibler Daten / Verletzung von NDA
   -> Versand von „malware“
2. Haftung aus vom Arbeitnehmer begründeten Ver tragsverhältnissen
3. Deliktische Ansprüche
   -> Haftung des Mitarbeiters +
   -> Haftung des AG nur bei Auswahlverschulden

VIII. Risiko 2 - Strafrechtliche Aspekte

-> Pornographie - § 184 StGB

-> Beleidigungsdelikte nach §§ 185 ff. StGB, Volksverhetzung nach § 130 StGB etc.

-> Sachbeschädigung, Datenveränderung und Computersabotage, § 303 ff. StGB

-> Unerlaubte Verwertung von Urheberrechten, §§ 106ff UrhG

-> Geheimnisverrat nach § 17 UWG

-> Verletzung des persönlichen Lebens- oder Geheimbereichs, § 202 ff. StGB

IX. Muster Betriebsvereinbarung/Arbeitsvertrag/ Richtlinie/Weisung

Vielen Dank für Ihre Aufmerksamkeit !

Jan Schröder
SUFFEL & KOLLEGEN, Rechtsanwälte
Leutragraben 2-4
07743 Jena
Tel: 03641 – 507720
Fax: 03641 – 507777
Jan.Schroeder@jenAnwalt.de
www.jenAnwalt.de