25.4
Orientierungshilfe zu Rechtsfragen bei der Einführung häuslicher Telearbeitsplätze

Stand: 17. Oktober 2002

Diese Orientierungshilfe spricht nicht nur datenschutzrechtliche Fragestellungen an, sondern enthält auch Hinweise auf andere rechtliche Aspekte, die vor der Einführung von Telearbeit zu klären sind. Soweit einzelne Themenkreise doppelt angesprochen werden, ist dies darin begründet, dass manche Themenkomplexe mehrfach relevant sind.

1. Schwachstellen von Telearbeitsplätzen

Bei der Telearbeit gibt es im Vergleich zum Büroarbeitsplatz zusätzliche potentielle Schwachstellen:

a) Die Organisation der Telearbeit ist komplizierter, da die räumliche Entfernung größer ist und der Arbeitgeber nur indirekte Möglichkeiten der Einflussnahme hat.

b) Der Arbeitsplatzrechner ist unberechtigten Zugriffen eher ausgesetzt.

c) Der Arbeitsplatzrechner kann zu nicht vorgesehenen Zwecken verwandt werden.

d) Die Kommunikationsverbindung zwischen Arbeitsplatzrechner und Institution geht in der Regel über öffentliche Leitungen.

e) Es gibt einen zusätzlichen Zugang zum Netz der Verwaltung.

f) Die Möglichkeiten des Zugriffs und der Kontrolle durch den behördlichen Datenschutzbeauftragten und den Administrator sind eingeschränkt.

2. Regelungsbereiche

Für die Telearbeit sind zu verschiedenen Bereichen dienstliche Anordnungen, allgemeine Weisungen und technische Vorgaben nötig:

Die Anordnungen und Vorgaben zur Nutzung der dienstlichen Einrichtungen sind für folgende Bereiche erforderlich:

a) zur Nutzung der dienstlichen Einrichtungen am Telearbeitsplatz und

b) zu den Befugnissen des zu Hause arbeitenden Bediensteten im Netz des Dienstherrn

c) zur häuslichen Umgebung des Arbeitsplatzes

d) zur Ausstattung des Arbeitsplatzes

e) zur Absicherung der Kommunikation mit der Dienststelle

f) zum Zugang in das Verwaltungsnetz und dessen Absicherung

g) zu den Protokolldaten und deren Auswertung

h) zu notwendigen Änderungen und deren Vorabanzeige.

Die mit den Bediensteten zu schließenden Einzelvereinbarungen sind in Form von Musterverträgen vorzubereiten.

3. Verantwortlichkeit

a) Die datenverarbeitende Stelle bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

b) Die datenverarbeitende Stelle hat die technischen und organisatorischen Maßnahmen nach § 10 HDSG vorzugeben. Sie muss die vom Mitarbeiter zugesicherten Maßnahmen ausdrücklich bestätigen.

c) Sie muss die Einhaltung aller Maßnahmen kontrollieren.

4. Grundpflichten und -rechte der Bediensteten

Die Bediensteten dürfen die personenbezogenen Daten nur im Rahmen der Weisungen des Dienstherren verarbeiten. Weisungen muss es insbesondere geben

a) zum Verbot der Bearbeitung mit und der Übertragung auf eigene DV-Anlagen

b) zur Nutzung des dienstlichen PC und der über ihn erreichbaren Speicher

c) zur Verwahrung und zur Herausgabe von Arbeitsunterlagen und entsprechenden Dateien

d) zu den Löschungspflichten und deren Befristung

e) zur Internetnutzung und E-Mail über dienstliche PC

f) zur Sicherung des PC gegen unbefugte Nutzung

g) zur Handhabung der vorgegebenen Verschlüsselungstechnik (ggf. durch technische unausweichliche Vorgaben)

h) zum Administratoreneinsatz einschließlich der Kontrollrechte am Telearbeitsplatz

i) zur Verwendung von Programmen nach Auswahl der Dienststelle (Ausschluss der Nutzung eigener Software)

j) zur Verfügbarkeit der Daten und deren Aktualisierung
Es muss organisatorisch und technisch sichergestellt werden, dass am Telearbeitsplatz verarbeitete Daten der Dienststelle ausreichend aktuell zur Verfügung stehen. (Speicherung der Daten auf einem Server der Dienststelle, tägliche Übertragung der Daten zur Dienststelle, evtl. Abrufrecht der Dienststelle ...)

5. Einzelvertraglich zu regelnde Sachverhalte

Folgende Punkte müssen zusätzlich zu in 4. genannten Grundpflichten in den Einzelvereinbarungen mit den Bediensteten geklärt werden:

a) Art der zu verarbeitenden Daten. Hier sind Einschränkungen zu beachten, die sich aus Amts- oder besonderen Berufsgeheimnissen ergeben (Personaldaten, Patientendaten, Sozialdaten).

b) Zutrittsrechte des behördlichen Datenschutzbeauftragten vor Arbeitsaufnahme und während der Telearbeit. Insbesondere sind die vom Bediensteten vorgesehenen Datensicherheitsmaßnahmen zu überprüfen).

c) Zutrittsrechte der behördlichen Administratoren zur Wartung, Behebung von Störungen und bei Veränderungen der Hard- oder Software.

d) Kontrollrechte der Dienststelle, insbesondere das Zutrittsrecht zur Wohnung.
Geregelt werden muss, was geschieht, wenn der Zutritt verweigert wird. Es ist sinnvoll, die Möglichkeit vorzusehen, dass das Telearbeitsverhältnis außerordentlich beendet wird.

e) Rückholrechte des dienstlichen Geräts, auch zu Prüfzwecken.

f) Kontrollrechte des Hessischen Datenschutzbeauftragten. Insbesondere müssen die Zutrittsrechte durch Unterwerfungserklärung der Mitarbeiter entsprechend § 4 Abs. 3 Satz 1 HDSG vereinbart werden. Wenn die Einwilligung verweigert wird, darf ein Telearbeitsplatz nicht eingerichtet werden. Für den Fall, dass der Zutritt durch den Bediensteten im Einzelfall verweigert wird, sollte die Möglichkeit der Beendigung des Telearbeitsplatzes vorgesehen werden.

g) Datensicherung. Festzulegen ist insbesondere die Verantwortung für die Datensicherung (Backup). (Etwa zentraler Datenbeistand bei der Dienststelle, lokaler Datenbestand beim Bediensteten.)

h) Pflicht zur Anzeige von Änderungen im häuslichen Bereich. Grundsatz der Vorabgenehmigung durch die Dienststelle.

i) Hinweis auf die einzuhaltenden Sicherheitsvorkehrungen, die die Dienststelle vorgegeben hat

- technische und organisatorische Maßnahmen
- Passwortschutz
- arbeitsplatzspezifische Sicherheitsvorkehrungen
- Aufbewahrungs- und Verwahrungspflichten
- Sicherheit beim Transport von Datenträgern
- Verschlüsselungsmethoden
- Löschung von Datenträgern nach Weisung der Dienststelle
- Verbot, private Rechner mit dienstlichen Anschlüssen zu verbinden
- Verbot, Dritten Zugriffe auf das Arbeitsgerät zu gestatten.

Diese Hinweise sind in einem Merkblatt zusammenzufassen.

a) Vertraglich festzulegen sind überdies

- - Arbeitsort
- - Arbeitszeit
- - Arbeitsauftrag
- - Arbeitsbemessung bei Stücklohnvereinbarung

b) Kostenerstattung durch die Dienststelle (Umfang, Nachweispflichten und Verfahren im Streitfall)

6. Abstimmung mit dem Personalrat

Grundsätzlich ist der Personalrat bei der Einführung von Telearbeitsmodellen zu beteiligen. Das gilt insbesondere für beabsichtigte Maßnahmen, die zur Überwachung des Bediensteten geeignet sind. Sollen Protokollierungen vorgenommen werden, die über die Aufzeichnungen, die am Arbeitsplatz vorgenommen werden, hinausgehen, so müssen diese mit dem Personalrat angestimmt werden.

7. Technische Sicherungsmaßnahmen

7.1 Standardsicherungen

a) Soweit möglich muss durch technische und organisatorische Maßnahmen die Vertraulichkeit von dienstlichen Unterlagen am Telearbeitsplatz erreicht werden.

b) Das Verwaltungsnetz muss gegen unbefugte Zugriffe geschützt werden. Soweit möglich muss der Dienstherr gewährleisten, dass nur berechtigte Personen vom Telearbeitsplatz aus auf dienstliche Daten zugreifen können.

c) Durch technische Sicherungsmaßnahmen müssen die Vertraulichkeit und die Integrität der zwischen dem Telearbeitsplatz und der Dienststelle übertragenen Daten gewahrt sein.

d) Die Zugriffsrechte müssen auf das erforderliche Maß reduziert sein.

e) Das gesamte Verfahren muss revisionssicher sein.

7.2 Sicherheitsbedingte Einzelmaßnahmen

7.2.1 Sicherungen am Telearbeitsplatz

a) Die Dienststelle stellt die gesamte IT-Ausstattung zur Verfügung. Der Telearbeiter darf keine Änderungen bei Soft- und Hardwarekomponenten vornehmen (können). Software darf nur mit Genehmigung der Dienststelle eingespielt werden.

b) Die Möglichkeit zur verschlüsselten Speicherung von Dateien oder die Verschlüsselung der gesamten Festplatte ist bei sensiblen Daten vorzusehen. Dabei ist ein anerkanntes kryptografisches Verfahren zu nutzen.

c) Durch das Betriebssystem oder zusätzliche Sicherheits-Hard- und Software müssen die Benutzer (Telearbeiter, Administrator) unterschieden werden. Sie dürfen nur im erforderlichen

Umfang Zugriffsrechte besitzen. Zur Authentisierung müssen zumindest Passwörter verlangt werden.

d) Generell ist zu empfehlen, zusätzliche technische Einrichtungen wie chipkartenbasierter Logon oder biometrische Verfahren zu nutzen.

e) Wie bei einem Arbeitsplatz im Büro muss der Bildschirmschoner aktiviert und ein Virenscanner installiert sein.

f) Der Dienstherr muss Behältnisse zur sicheren Lagerung der Datenträger zur Verfügung stellen.

g) Datenträger müssen an die Dienststelle zurückgegeben werden. Es darf kein Zurückbehaltungsrecht im Streitfall geben. Die Dienststelle muss die datenschutzgerechte Vernichtung vornehmen.

7.2.2 Sicherung der Kommunikation und des Dienstellennetzes

a) In einem Sicherheitskonzept sind die Maßnahmen zum Schutz des Dienststellennetzes festzulegen (ggf. auf Basis des Grundschutzhandbuchs). Insbesondere muss die Sicherheit des Kommunikationsrechners gewährleistet werden.

b) Für die Telearbeit sollten spezielle Benutzerkennungen eingerichtet werden, um für die Telearbeit gezielt Berechtigungsprofile einrichten zu können. Die Zugriffsrechte müssen restriktiv vergeben werden. Wurde eine Kennung längere Zeit nicht genutzt, sollte sie gesperrt werden.

c) Die Anbindung des Telearbeitsplatzes muss durch Einrichtung einer geschlossenen Benutzergruppe auf Telekommunikationsebene, virtual private network (VPN) oder andere Sicherheitsfunktionen (Rufnummernprüfung, Call-Back) gesichert werden.

d) Die Datenübertragung muss verschlüsselt erfolgen (anerkanntes kryptografisches Verfahren). Dies gilt für Kommunikationsleitungen, aber auch für Disketten und vergleichbare Datenträger (Akten: in verschlossenen Behältern).

e) Ein direkter Zugang zum Internet oder anderen Online-Diensten vom Telearbeitsplatz aus muss unterbunden werden. Wenn dienstlich ein Zugang erforderlich ist, muss er über einen zentralen, durch eine Firewall gesicherten Punkt, der von der Dienststelle festgelegt ist, erfolgen.

f) Es muss protokolliert werden, wer wann auf welche Datenbestände mit Hilfe des Telearbeitsplatzes zugegriffen hat und welche Daten zwischen Dienststelle und Telearbeitsplatz übertragen wurden (Empfehlung: Dauer der Speicherung von Protokolldaten sechs Monate).

zurück, weiter, Inhalt 31.TB, Sachwortverzeichnis zum 31.TB