Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern

Datenschutz bei Telearbeit

Orientierungshilfe

Stand: 2002

Postanschrift
Schloss Schwerin
19053 Schwerin

Hausanschrift
Johannes-Stelling-Str. 21
19053 Schwerin

Kommunikation
Telefon (03 85) 5 94 94-0
Telefax (03 85) 5 94 94-58
E-Mail datenschutz@mvnet.de
Internet http://www.lfd.m-v.de

PGP-Fingerprint
ADB5 030A C111
388C A8FD
92B7 EF40 56E6
71DA 3ABA

Inhalt

1 Einleitung

Durch die vielfältig eingesetzte Informations- und Kommunikationstechnik ändern sich die Lebens- und Arbeitsbedingungen in zunehmendem Maße. Telearbeit ist eine neue Arbeitsform, die diesen Veränderungen Rechnung tragen soll. Dabei spielen sowohl die Wünsche des Arbeitgebers nach Kostenreduzierungen und mehr Flexibilität der Arbeitsorganisation als auch das Interesse von Beschäftigten an wohnortnahen Arbeitsplätzen, flexiblerer Arbeitszeit und der besseren Vereinbarkeit von Beruf und Familie eine Rolle. Nicht zuletzt beleben allgemeine Erwägungen wie geringere Verkehrs- und Umweltbelastung sowie regionale Arbeitsmarktförderung die Diskussion um Telearbeit.

In Mecklenburg-Vorpommern hat die Landesregierung auf diese Entwicklung reagiert und in der Verordnung über die Arbeitszeit von Beamten in Mecklenburg-Vorpommern (Arbeitszeitverordnung – AZVO) die Möglichkeit der Telearbeit eingeräumt. Mit § 10a AZVO wurde eine so genannte Experimentierklausel eingeführt, die der Erprobung neuer Arbeitszeitmodelle, insbesondere der Telearbeit, dienen soll.

Der Landesbeauftragte für den Datenschutz ist für den öffentlichen Bereich zuständig. Deshalb richtet sich diese Orientierungshilfe in erster Linie an öffentliche Verwaltungen. Die Aussagen lassen sich aber im Allgemeinen auch auf andere Bereiche übertragen. Im Folgenden werden deshalb die Begriffe **Bedienstete** als Synonym für Arbeitnehmer und Beamte sowie **Dienststelle** für die zentrale Betriebsstätte (Behörde oder Firma) verwendet.

Aus datenschutzrechtlicher Sicht sind bei der Telearbeit vor allem drei Aspekte von Bedeutung:

1. Je nach **Art der zu verarbeitenden Daten** sind Einschränkungen zu beachten. Wegen der nachfolgend beschriebenen Besonderheiten eines Telearbeitsplatzes dürfen sensible personenbezogene Daten nur unter bestimmten Voraussetzungen außerhalb der Dienststelle verarbeitet werden. Das betrifft insbesondere die Daten, die einem Amts- oder besonderen Berufsgeheimnis unterliegen (siehe Punkt 4).

2. Telearbeit kann die **Privatsphäre der Bediensteten** nachhaltig beeinflussen. So könnten Telearbeitsplätze beispielsweise als umfassende Informationsquellen über die Arbeitsweise von Bediensteten „missbraucht“ werden, da ein außerordentliches Potential für die Sammlung, Messung und Auswertung von Daten sowohl über die Leistungsfähigkeit als auch über andere persönliche Eigenschaften bereitsteht (siehe Punkt 5).

3. Telearbeitsplätze werden **außerhalb üblicher Büroumgebungen** eingerichtet. Der Datenaustausch mit der Dienststelle erfolgt in der Regel über öffentliche Leitungen. Es sind deshalb angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit und der Integrität sowohl der zu übertragenden als auch der am Telearbeitsplatz und der in der Zentrale zu speichernden personenbezogenen Daten zu treffen (siehe Punkte 6 und 7).

Diese Orientierungshilfe gibt rechtliche und technische Hinweise zum Thema Telearbeit und erläutert, unter welchen Voraussetzungen Telearbeitsplätze datenschutzgerecht eingerichtet und betrieben werden können und welche rechtlichen und technischen Anforderungen dabei zu beachten sind.

2 Begriff und Formen der Telearbeit

2.1 Definition

Im Zusammenhang mit dem Thema Telearbeit sind in der Literatur unterschiedliche Begriffe zu finden. Übereinstimmend versteht man jedoch unter Telearbeit die Tätigkeiten zur Erledigung eines Arbeitsauftrages, die mit einer gewissen Regelmäßigkeit und unter Nutzung von elektronischen Kommunikationsmitteln (u. a. Computer, Datennetze) an einem Arbeitsplatz verrichtet werden, der außerhalb der Dienststelle liegt. Eine permanente oder zeitweilige Online-Verbindung zum Zentralcomputer muss hierfür nicht zwangsläufig bestehen.

Nicht erfasst werden Tätigkeiten, bei denen Bedienstete ungeplant oder nur gelegentlich außerhalb der Dienststelle tätig sind und dabei eher zufällig einen Computer oder ein Datennetz benutzen.

2.2 Formen der Telearbeit

In der Praxis findet man zurzeit im Wesentlichen drei Varianten von Telearbeitsplätzen, die unterschiedlich datenschutzrechtlich bewertet und datenschutztechnisch ausgestaltet werden.

2.2.1 Häusliche Telearbeit

Bei dieser Form der Telearbeit (auch als Teleheimarbeit, ausschließliche Telearbeit, Home-Based-Telework oder ähnlich bezeichnet) ist der Bedienstete ausschließlich zu Hause tätig und hat keinen Arbeitsplatz mehr in der Dienststelle.

2.2.2 Telearbeitszentrum

Wenn eine Gruppe von Bediensteten von einem gemeinsamen Arbeitsraum aus tätig wird, der in der Nähe ihrer Wohnungen oder auch in einer Wohnung angesiedelt ist, spricht man von einem Telearbeitszentrum (auch als Center-Based-Telework bezeichnet). Handelt es sich dabei um dienststelleneigene Arbeitsstätten, nennt man diese auch Satellitenbüros. Nutzen mehrere Dienststellen ein gemeinsames Büro, wird dies auch als Nachbarschaftsbüro bezeichnet.

2.2.3 Alternierende Telearbeit

Alternierende Telearbeit ist die am meisten verbreitete Form der Telearbeit. Hierbei ist der Bedienstete abwechselnd sowohl in der Dienststelle als auch zu Hause oder an anderen Orten tätig. Neben dem Telearbeitsplatz besteht auch weiterhin der Arbeitsplatz in der Dienststelle fort. Eine besondere Form der alternierenden Telearbeit ist die „mobile Telearbeit“ (auch als On-Site-Telework bezeichnet). Der Bedienstete nutzt dabei einen mobilen Arbeitsplatz (z. B. Notebook, Laptop, Palmtop) an wechselnden Einsatzorten. Besonders verbreitet ist diese Form beispielsweise im Außendienst.

3 Datenschutzrechtliche Grundsatzfragen

Der Umgang mit personenbezogenen Daten ist nur zulässig, soweit eine Rechtsvorschrift (eine spezialgesetzliche Regelung oder das Landesdatenschutzgesetz – DSG M-V) ihn erlaubt beziehungsweise zwingend voraussetzt oder wenn der Betroffene eingewilligt hat (§ 7 DSG M-V – Grundsatz).

Nach den §§ 21 und 22 DSG M-V sind dann die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zu treffen, um die entsprechenden Datenschutzvorschriften einzuhalten. An den Umgang mit personenbezogenen Daten im Rahmen der Telearbeit werden aus datenschutzrechtlicher Sicht hohe Anforderungen gestellt, weil ein größeres Gefährdungspotential als bei der Datenverarbeitung in der Dienststelle vorhanden ist. Insbesondere müssen die Rechtmäßigkeit, Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung nicht nur ständig gewährleistet, sondern auch regelmäßig überwacht werden können (Revisionsfähigkeit – § 21 Abs. 2 Nr. 5 DSG M-V). Die Daten verarbeitende Stelle stößt bei der Durchsetzung dieser Pflichten auf grundsätzliche Schwierigkeiten, da sie bei einem Telearbeitsplatz nicht mehr die uneingeschränkte Organisationsgewalt über Hard- und Software, Datenbestände und handelnde Personen hat.

Für Telearbeitsplätze ist kennzeichnend, dass personenbezogene Daten die Daten verarbeitende Stelle verlassen und die Verarbeitung faktisch nur noch eingeschränkt beaufsichtigt werden kann. Von besonderer Bedeutung ist dabei, dass bei Telearbeitsplätzen in der Regel die infrastrukturellen Sicherungsmaßnahmen fehlen, die bei dienststelleninternen Arbeitsplätzen Standard sind. Am Heimarbeitsplatz sind darüber hinaus weder Datenschutz- noch IT-Fachleute präsent, so dass die regelmäßige Überprüfung der richtigen Funktionsweise der Telearbeitsplätze nur schwer realisierbar ist. Hinzu kommt, dass Kontrollen des Dienstherrn oder der zuständigen Datenschutzkontrollinstanzen (Landesdatenschutzbeauftragter oder behördlicher Datenschutzbeauftragter) im häuslichen Umfeld ohne Einwilligung des Telearbeiters nicht möglich sind und somit die Organisationsgewalt der Daten verarbeitenden Stelle weiter eingeschränkt wird (mehr dazu unter Punkt 5).

All das führt bei Telearbeit zu einem ungleich größeren Risiko der möglichen Beeinträchtigung des Rechtes auf informationelle Selbstbestimmung der von einer derartigen Datenverarbeitung Betroffenen. Datenschutzrechtliche Überlegungen zum Thema Telearbeit müssen deshalb die Minimierung dieses zusätzlichen Risikos zum Ziel haben. Fragen der Mitbestimmung, des Arbeitsrechts, der Haftung oder der Sozialverträglichkeit haben dabei einen hohen Stellenwert, sind jedoch datenschutzrechtlichen Fragen nicht über-, sondern gleichgeordnet. Können die gesetzlichen Vorgaben des Datenschutzes mit wirtschaftlich vertretbaren Maßnahmen nicht umgesetzt werden, muss unter Umständen die Verarbeitung personenbezogener Daten auf Telearbeitsplätzen unterbleiben (siehe dazu Punkt 4).

Die verschiedenen Formen der Telearbeit haben aus datenschutzrechtlicher Sicht unterschiedliche Einschränkungen zur Folge. Telearbeitszentren sind datenschutzrechtlich weniger problematisch. Es besteht kaum ein Unterschied zu der konventionellen Außenstelle einer Dienststelle. Kontrollrechte lassen sich ebenso verankern wie in der Zentrale, und datenschutztechnische Standards sind ohne größere Probleme realisierbar.

Der typische Heimarbeitsplatz für ständige oder alternierende Telearbeit hingegen enthält die oben genannten Risiken in vollem Umfang. Deshalb sind an die erforderlichen technischen und organisatorischen Maßnahmen (siehe Punkte 6 und 7) höhere Anforderungen zu stellen,

und für einige Arten personenbezogener Daten gelten besondere Einschränkungen (siehe Punkt 4).

Mobile Telearbeitsplätze, die vorwiegend an wechselnden Einsatzorten außerhalb der Wohnung des Bediensteten eingesetzt werden, führen zu ähnlichen Bedrohungen wie stationäre Telearbeitsplätze. Einige Risiken, die der Telearbeitsplatz im häuslichen Umfeld mit sich bringt (z. B. mögliche Kenntnisnahme vertraulicher Daten durch Familienangehörige), spielen sicher eine untergeordnete Rolle. Dafür sind jedoch andere Gefahren zu berücksichtigen, die sich gerade aus der Mobilität solcher Geräte ergeben (z. B. Diebstahl). Daten auf mobilen Telearbeitsplätzen sind deshalb unabhängig von ihrer Sensibilität gemäß § 22 Abs. 3 DSG M-V zu verschlüsseln. Die Einschränkungen hinsichtlich der Revisionsmöglichkeiten durch den Dienstherren sind in vergleichbarer Weise zu bedenken wie bei Heimarbeitsplätzen.

4 Amts- und besondere Berufsgeheimnisse

In bestimmten Bereichen ist Telearbeit aus rechtlichen Gründen mit erheblichem technischen Aufwand abzusichern oder von der Einwilligung derjenigen abhängig, deren Daten auf Telearbeitsplätzen verarbeitet werden. Darüber hinaus ist zu berücksichtigen, dass Daten aus diesem Bereich in der Regel den besonderen Verarbeitungsregeln nach § 7 Abs. 2 DSG M-V unterliegen. Insbesondere muss in diesen Fällen eine Vorabkontrolle nach § 19 Abs. 2 DSG M-V erfolgen. Die folgenden Beispiele zeigen, mit welchen Einschränkungen unter Umständen bei der Einrichtung von Telearbeitsplätzen gerechnet werden muss.

4.1 Patientendaten

Mit Patientendaten wird bei ärztlichen oder medizinischen Behandlungen sowie bei der Abrechnung und Kontrolle dieser Leistungen umgegangen. Diese Daten unterliegen neben den datenschutzrechtlichen Bestimmungen der besonderen Geheimhaltungspflicht des § 203 Strafgesetzbuch (StGB). Sie dürfen auch nach Art. 8 Abs. 3 der EG-Richtlinie 95/46 (EG-Datenschutzrichtlinie) nur von ärztlichem Personal verarbeitet werden, das dem Berufsgeheimnis unterliegt. Vor Beschlagnahme gemäß § 97 Abs. 2 Strafprozessordnung (StPO) sind Patientendaten nur geschützt, sofern sie sich im Gewahrsam dieses ärztlichen Personals befinden.

Werden Patientendaten im Rahmen der Telearbeit verarbeitet, muss deshalb gewährleistet sein, dass auf die Mitarbeiter die Bestimmungen zur ärztlichen Schweigepflicht anwendbar sind. Nur so kann beispielsweise der Beschlagnahmeschutz aus § 97 Abs. 2 StPO aufrechterhalten werden.

Der Dienstherr oder Arbeitgeber muss dem Mitarbeiter datenschutzrechtliche Vorgaben machen und kontrollieren, ob sie erfüllt sind (siehe dazu Punkt 5). Er sollte unter Fürsorgegesichtspunkten aber auch prüfen, ob der Mitarbeiter unter den Bedingungen der Telearbeit seine persönliche Pflicht zur Geheimhaltung der Daten erfüllen kann. Das setzt voraus, dass insbesondere technische Maßnahmen umgesetzt werden müssen, die ein Sicherheitsniveau am Telearbeitsplatz gewährleisten, das den Schutz von Patientendaten in vergleichbarer Weise wie etwa im Krankenhaus sicherstellt (siehe Punkt 7).

4.2 Sozialdaten

Ähnliche Schranken sind der Verarbeitung von Sozialdaten auf Telearbeitsplätzen gesetzt. Das im § 35 Abs. 1 Sozialgesetzbuch Erstes Buch (SGB I) normierte Sozialgeheimnis umfasst die Verpflichtung sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind und auch nur an diese weitergegeben werden dürfen. Der besonders hohe Schutzbedarf ist mit vertretbarem Aufwand an Telearbeitsplätzen nur schwer zu realisieren. Die unter den Punkten 6 und 7 beschriebenen technischen und organisatorischen Rahmenbedingungen können das Missbrauchsrisiko im häuslichen Umfeld zwar reduzieren, genügen dem besonderen Schutzbedarf von Sozialdaten möglicherweise jedoch nicht. Nicht zuletzt deshalb muss eine Vorabkontrolle nach § 19 Abs. 2 DSG M-V durchgeführt werden.

4.3 Personaldaten

Der Umgang mit Personaldaten ist geprägt vom so genannten Personalaktengeheimnis, das sich beispielsweise aus den Zweckbindungsbestimmungen und den Zugangsregelungen des Landesbeamtengesetzes (LBG M-V) herleiten lässt. So ist in § 100 Abs. 3 LBG M-V festgelegt, dass zu Personalakten nur Bedienstete Zugang haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Im häuslichen Umfeld ist die erforderliche Vertraulichkeit in ausreichendem Maße nur schwer zu gewährleisten und darüber hinaus kaum zu kontrollieren.

5 Kontrollmöglichkeiten und -grenzen

5.1 Kontrollen durch die Dienststelle

Die Einrichtung von Telearbeitsplätzen entbindet den Dienststellenleiter nicht von Aufsichts-, Fürsorge- und Kontrollpflichten. Mit Blick auf die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz – GG) ist eine Kontrolle des häuslichen Telearbeitsplatzes durch Dienststellenangehörige (Behördenleiter, behördlicher Datenschutzbeauftragter) zunächst jedoch ausgeschlossen. Nur wenn in einer entsprechenden Vereinbarung (siehe Punkt 6.3) jeweils im Einzelfall ausdrücklich ein Zutrittsrecht zur privaten Wohnung eingeräumt wird und sich der Bedienstete somit bestimmten Kontrollen bei der Telearbeit in seiner Wohnung unterwirft, können Dienststellenleiter und Datenschutzbeauftragter ihre Pflichten wahrnehmen. Derartige Vereinbarungen können nur auf freiwilliger Basis geschlossen werden, so dass die Einrichtung eines Telearbeitsplatzes immer von der Einwilligung des Bediensteten und der Haushaltsangehörigen abhängig ist. Wird die Einwilligung jedoch widerrufen, hat dies die sofortige Beendigung des Telearbeitsverhältnisses zur Folge.

5.2 Kontrollen durch den Landesbeauftragten für den Datenschutz

Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung datenschutzrechtlicher Vorschriften bei öffentlichen Stellen. Dazu ist ihm Einsicht in alle Unterlagen und insbesondere Zugang zu Datenverarbeitungssystemen zu gewähren (§§ 30, 31 DSG M-V). Werden personenbezogene Daten im Rahmen der Telearbeit verarbeitet, erstreckt sich das Kontrollrecht prinzipiell auch auf Telearbeitsplätze (siehe dazu auch § 70 Abs. 4 Schulgesetz Mecklenburg-Vorpommern). Auch in diesem Fall setzt das jedoch die Einwilligung des Telearbeiters voraus (Art. 13 GG). Lehnt ein Bediensteter es ab, dass der Landesdatenschutzbeauftragte seine Privaträume betritt, darf kein Telearbeitsplatz für die oben genannten Zwecke eingerichtet werden. Beschränkt sich eine Kontrolle (auch nach 5.1) auf technische Aspekte der Daten-

verarbeitungsanlage des Telearbeitsplatzes (z. B. ordnungsgemäß installierte Software), kann erwogen werden, die Anlage zur Kontrolle in die Dienststelle zu bringen.

5.3 Protokollierung

Die Kontrollmöglichkeiten des Dienstherrn bei Telearbeitsplätzen sind wie oben beschrieben eingeschränkt. Die Protokollierung bei der Verarbeitung personenbezogener Daten hat deshalb besondere Bedeutung. Beispielsweise ist zum Nachweis der Authentizität (§ 21 Abs. 2 Nr. 4 DSG M-V) und zur Gewährleistung der Revisionssicherheit (§ 21 Abs. 2 Nr. 5 DSG M-V) zu protokollieren, wer wann welche Daten eingegeben hat. Durch entsprechende Protokolle muss nachvollziehbar sein, wann ein Telearbeiter Daten übermittelt und auf den zentralen Datenbestand mittels Datenfernübertragungseinrichtungen zugegriffen hat.

Der Verwendung dieser Daten sind enge Grenzen gesetzt, da diese Protokolle personenbezogene Daten des Telearbeiters enthalten, die sehr detailliert Aufschluss über die erbrachte Leistung, über das Arbeitsverhalten und über weitere persönliche Eigenschaften geben können. § 35 Abs. 7 DSG M-V legt ausdrücklich fest, dass derartige Daten nicht für Zwecke der Verhaltens- und Leistungskontrolle genutzt werden dürfen.

In diesem Zusammenhang sind auch die Mitbestimmungsrechte der Personalvertretungen zu berücksichtigen. Die Einführung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, unterliegt gemäß § 70 Abs. 1 Ziff. 2 Personalvertretungsgesetz (PersVG) der Mitbestimmung der Personalvertretung. Telearbeitsplätze, die zwangsläufig personenbezogene Zugriffsberechtigungen und die oben genannten Protokollierungen erfordern, sind zweifelsohne diesen Einrichtungen zuzuordnen. Deshalb sollten Dienststellenleitung und Personalrat im Rahmen von Dienstvereinbarungen Regelungen treffen, die eine Leistungs- und Verhaltenskontrolle auf das zulässige und erforderliche Maß beschränken (siehe dazu Punkte 6.2 und 6.3). Derartige Regelungen sollten sehr detailliert die getroffenen technischen und organisatorischen Maßnahmen erläutern. Dann sind sie auch dazu geeignet, die vom Datenschutzrecht geforderte Transparenz (§ 21 Abs. 2 Nr. 6 DSG M-V) zu gewährleisten.

6 Organisatorische Rahmenbedingungen

6.1 Verhältnis zur Datenverarbeitung im Auftrag

Sowohl bei der Telearbeit als auch bei der Datenverarbeitung im Auftrag verlassen Daten den räumlich eingegrenzten Bereich der Daten verarbeitenden Stelle. Deshalb liegt es nahe, diese beiden Formen miteinander zu vergleichen, um die gegebenenfalls bei der Auftragsdatenverarbeitung geltenden Anforderungen sinngemäß auch bei der Telearbeit anzuwenden.

Die Anforderungen an den Umgang mit personenbezogenen Daten im Auftrag sind in § 4 DSG M-V festgelegt. Damit der Auftragnehmer ordnungsgemäß mit diesen Daten umgeht, muss unter anderem gewährleistet sein, dass

- die Daten verarbeitende Stelle für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich bleibt,
- die nach §§ 21 und 22 DSG M-V erforderlichen technischen und organisatorischen Maßnahmen umgesetzt werden und

– der Auftragnehmer mit personenbezogenen Daten nur im Rahmen der Weisungen des Auftraggebers umgeht.

Bei der Telearbeit handelt es sich nur dann um Datenverarbeitung im Auftrag, wenn der Telearbeiter nicht Beschäftigter der speichernden Stelle ist und wenn er auf der Basis eines Dienst- oder Werkvertrages beispielsweise in der Privatwohnung tätig wird. Die Vorschriften des DSG M-V zur Auftragsdatenverarbeitung (§ 4) sind dann anwendbar. Dieser Fall wird jedoch die Ausnahme sein und soll deshalb hier nicht weiter betrachtet werden.

Telearbeiter sind überwiegend keine Personen externer Stellen. Es sind in der Regel Bedienstete der jeweiligen Dienststelle. Sie können deshalb keine Auftragnehmer sein, so dass die Regelungen zur Datenverarbeitung im Auftrag nicht anwendbar sind. Die zur Organisation der Telearbeit nötigen vertraglichen Regelungen zwischen Dienststellenleitung und Personalvertretung (Dienstvereinbarung) bzw. Telearbeiter (Einzelvertrag) können jedoch in Anlehnung an schriftliche Aufträge zur Auftragsdatenverarbeitung formuliert werden.

6.2 Dienstvereinbarung

Die Dienstvereinbarung zur Einrichtung und zum Betrieb von Telearbeitsplätzen sollte zwischen Dienststellenleitung und Personalvertretung gemäß § 66 PersVG abgeschlossen werden und folgende Details regeln:

Grundsatzfragen:
- Ziele des gesamten Telearbeitsprojektes
- Form der Telearbeit
- Laufzeit des konkreten Projektes
- Beibehaltung des Beschäftigungsverhältnisses
- Beibehaltung des betrieblichen Arbeitsplatzes
- Mitbestimmungsrechte des Personalrates
- Freiwilligkeit der Teilnahme
- Einräumen des Kontrollrechtes für Dienstherren und Datenschutzkontrollinstanzen in der Wohnung des Telearbeiters

Arbeitszeit:
- Aufteilung betriebliche/Telearbeitszeit
- Arbeitszeitfestlegungen bei Betriebsstörungen des Telearbeitsplatzes
- Zuschläge, zum Beispiel für Feiertags- und Sonntagsarbeit
- Verfahren der Arbeitszeiterfassung

Arbeitsmittel:
- Dienststelle stellt die technische Ausstattung kostenlos zur Verfügung
- ausschließliche Verwendung von Hard- und Software, die der Dienstherr für den Telearbeitsplatz getestet und freigegeben hat
- gegebenenfalls Nutzung privater Büromöbel
- Vergütung für die (teilweise) Bereitstellung eines Arbeitsraumes
- Regelung für anfallende Telefon- und Datenübertragungskosten
- Festlegung ergonomischer Standards des Arbeitsplatzes (Arbeitsschutz)
- Verbot der privaten Nutzung dienstlicher Arbeitsmittel

Haftung:
- Regelung des Schadensersatzes bei Beschädigung der technischen Einrichtung durch Bedienstete, Familienangehörige oder sonstige Dritte

Einzelvertrag:
- Einrichtung eines Telearbeitsplatzes nur nach Abschluss einer schriftlichen Vereinbarung zwischen Dienststelle und Bedienstetem

Datenschutz:
- Verpflichtung des Telearbeiters auf das Datengeheimnis (§ 6 DSG M-V)
- Regelungen zum Schutz der Daten und Informationen gegenüber Dritten (insbesondere Familienangehörigen) in der häuslichen Arbeitsstätte
- umfassende Information über Sicherheitsanforderungen und Schutzvorkehrungen, die die Besonderheiten des Telearbeitsplatzes betreffen
- Vorgaben zur sicheren Aufbewahrung von Datenträgern

Protokollierung:
- Umfang der Protokollierungen sowie Verfahren zur Kontrolle und Auswertung der Protokolle

Verstöße:
- Verfahren bei gravierenden Verstößen gegen organisatorische und datenschutzrechtliche Vorgaben

6.3 Einzelvertrag

Auf der Basis der Dienstvereinbarung sollte mit jedem Telearbeitnehmer zusätzlich ein Einzelvertrag geschlossen werden, der die spezifischen Rahmenbedingungen des jeweiligen Einzelfalls berücksichtigt. Unter Berücksichtigung der familiären Verhältnisse und des häuslichen Umfelds könnten dies beispielsweise spezielle organisatorische Fragen oder durch die Arbeitsaufgabe bedingte Aspekte sein. Insbesondere sollten folgende Details zwischen Telearbeitnehmer und Dienststellenleitung geregelt werden:

Arbeitsort:
- genauer Ort des Telearbeitsplatzes (Anschrift, Raum usw.)
- Ausstattung (z. B. Rechnertyp, Softwareausstattung, Peripherie, Kommunikationseinrichtungen, Mobiliar)

Nutzer:
- Festlegung des/der ausschließlichen Nutzer(s) des Telearbeitsplatzes

Arbeitszeit:
- konkrete Aufteilung der wöchentlichen Arbeitszeit zwischen behördlichem und häuslichem Arbeitsplatz
- Zeiten der (telefonischen) Erreichbarkeit des Telearbeiters
- Form der Arbeitszeitabrechnung

Arbeitsauftrag:
- Arten der Übergabe des Arbeitsauftrages (z. B. während der Arbeitszeit in der Dienststelle, postalisch, per DFÜ, per Fax)

Kosten:
- Nutzungsentgelte für den Arbeitsraum (anteilige Miete)
- Übernahme der Telekommunikationskosten durch den Dienstherrn
- Begleichung weiterer Kosten, wie für Heizung oder Reinigung

Datenschutz:
- Einweisung in die für Telearbeit getroffenen arbeitsplatzspezifischen technischen und organisatorischen Maßnahmen
- konkrete arbeitsplatzspezifische Sicherheitsvorkehrungen
- sichere Aufbewahrung vertraulicher dienstlicher Unterlagen
- Verbot der Privatnutzung des Telearbeitsplatzes
- Regelung für den sicheren Transport von Daten (wie Akten, Disketten)
- Details zur Vernichtung von Akten und zur Löschung von Datenträgern

Kontrolle:
- schriftliche Einverständniserklärung des Telearbeiters und der Haushaltsangehörigen für die Kontrollen des Dienstherrn und der Datenschutzkontrollinstanzen in der Wohnung

- Information über alle Protokolle sowie deren Nutzung und Auswertung

Wartung: - Verfahren der Wartung des Arbeitsplatzes (Fernwartung oder vor Ort)

7 Technische Maßnahmen

Neben den unter Punkt 6 genannten organisatorischen Rahmenbedingungen sind technische Maßnahmen erforderlich, die sicherstellen, dass

- bei der Kommunikation zwischen Telearbeitsplatz und Dienststelle die Vertraulichkeit und die Integrität der übertragenen Daten gewährleistet sind (§ 21 Abs. 2 Nr. 1 und 2 DSG M-V),
- nur Berechtigte von zu Hause aus auf dienstliche Daten zugreifen können (§ 22 Abs. 1 DSG M-V),
- dienstliche Unterlagen am Telearbeitsplatz vertraulich behandelt werden (§ 21 Abs. 2 Nr. 1 DSG M-V) und
- das gesamte Verfahren der Telearbeit revisionssicher ist (§ 21 Abs. 2 Nr. 5 DSG M-V).

Dazu sind folgende Einzelmaßnahmen umzusetzen:

- Die Benutzung des Telearbeitsplatzes darf nur hierfür berechtigten Personen möglich sein (§ 22 Abs. 1 DSG M-V). Es sind entsprechende Identifikations- und Authentifikationsmechanismen vorzusehen. Hierzu sollte der Telearbeitsplatz mit einer Sicherheitshard- oder -software ausgestattet sein, die mindestens die Eingabe eindeutiger Kennungen und Passwörter ermöglicht und auch verlangt. Passwörter müssen den anerkannten Regeln zur Länge, Struktur und Gültigkeitsdauer unterliegen. Sie dürfen nur verschlüsselt im System abgelegt und auf Datenleitungen nur verschlüsselt übertragen werden.

- Das Risiko, bei der Passworteingabe beobachtet zu werden, ist im häuslichen Bereich groß. Um sicherzustellen, dass nur der berechtigte Telearbeiter auf die Daten zugreifen kann (§ 22 Abs. 1 DSG M-V), sollten zusätzliche technische Einrichtungen, wie chipkartenbasierte Zugangskontrollsysteme oder Fingerabdrucklesegeräte eingesetzt werden, die neben der Kenntnis des Passwortes zusätzlich den Besitz eines personenbezogenen Merkmals oder einer personenbezogenen Eigenschaft erfordern und einen unbefugten Zugriff erschweren.

- Werden personenbezogene Daten auf den Speichermedien des Telearbeitsplatzes vorgehalten, sind sie mit einem anerkannten kryptographischen Verfahren zu verschlüsseln (§ 22 Abs. 3 DSG M-V). Dadurch wird die Vertraulichkeit der verarbeiteten Daten sowohl gegenüber den im Haushalt lebenden weiteren Personen als auch im Falle des Diebstahls des Telearbeitsplatzes sichergestellt.

- Datenübermittlungen zwischen Telearbeitsplatz und Zentrale sollen grundsätzlich nur in verschlüsselter Form erfolgen. Das betrifft sowohl den leitungsgebundenen Datenaustausch als auch den Datenträgeraustausch per Diskette, Streamer, Magnetband oder vergleichbaren Speichermedien (§ 22 Abs. 3 DSG M-V).

- Die gesamte IT-Ausstattung stellt die Dienststelle zur Verfügung. Alle Hard- und Softwarekomponenten müssen getestet und zur Nutzung freigegeben sein (§ 19 Abs. 1 DSG M-V). Veränderungen durch den Telearbeiter dürfen nicht möglich sein. Die Administration von Telearbeitsplätzen darf ausschließlich durch entsprechend autorisiertes Personal der Zentrale (vor Ort oder per Fernwartung) erfolgen (§ 22 Abs. 2 DSG M-V). Bei allen Administrationstätigkeiten am Telearbeitsplatz sind die Hinweise zu berücksichtigen, die der Landesbeauftragte für den Datenschutz in der Orientierungshilfe „Forderungen an Wartung und Fernwartung“ veröffentlicht hat.

- Es sind Maßnahmen zu treffen, die einen unbefugten Zugriff auf die Programme und die Datenbestände des IT-Systems der Dienststelle verhindern. In einem Sicherheitskonzept nach § 22 Abs. 5 DSG M-V, das auf der Basis einer Risikoanalyse erstellt wird, sind die erforderlichen Einzelmaßnahmen festzulegen (siehe hierzu „Grundschutzhandbuch“ des Bundesamtes für Sicherheit in der Informationstechnik – BSI). Folgende kommen in Frage:

  - kein Zugang zum Internet oder zu anderen Online-Diensten vom Telearbeitsplatz aus
  - falls jedoch die dienstliche Notwendigkeit für einen derartigen Zugang besteht oder falls der Telearbeitsplatz über das Internet mit der Dienststelle verbunden werden soll, darf dieser Zugang nur über den zentralen und durch Firewall abgesicherten Übergabepunkt der Dienststelle erfolgen (die Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ der Datenschutzbeauftragten von Bund und Ländern gibt hierzu detaillierte Hinweise)
  - Einrichtung geschlossener Nutzergruppen beziehungsweise virtueller privater Netze (VPN) zur Anbindung des Telearbeitsplatzes
  - Nutzung weiterer von Kommunikationsdiensten angebotener Sicherheitsfunktionen (z. B. Rufnummernprüfung, call-back-Verfahren)
  - Einrichtung spezieller Kennungen für Telearbeitsplätze im IT-System der Zentrale, die von den Kennungen des Mitarbeiters als dienststelleninterner Nutzer verschieden sind
  - Reduzierung der Zugriffsrechte bei externem Zugriff auf das erforderliche Minimum
  - automatische Sperrung der Kennungen von Telearbeitsplätzen, die längere Zeit nicht benutzt wurden
  - Aktivierung von Filtermechanismen schon auf den unteren Schichten des OSI-Referenzmodells, die auf der Basis entsprechender Berechtigungsprüfungen so früh wie möglich unberechtigte Anschlussnummern, Adressen und Diensteanforderungen zurückweisen

- Zum Zwecke der Revision (§ 21 Abs. 2 Nr. 5 DSG M-V) muss die Anwendungssoftware oder eine spezielle Sicherheitssoftware protokollieren, wer wann auf welche Datenbestände mit Hilfe des Telearbeitsplatzes zugegriffen hat und wann welche Daten zwischen Zentrale und Telearbeitsplatz übertragen wurden. Die Protokolle sind für einen ausreichend langen Zeitraum (üblicherweise 6 bis 12 Monate) zu Kontrollzwecken aufzubewahren. Die unter Punkt 5.3 genannten Zweckbindungsgrundsätze sind hierbei zu berücksichtigen. Zugriff auf Protokolldaten dürfen deshalb nur speziell dafür autorisierte Personen erhalten, beispielsweise der behördliche Datenschutzbeauftragte oder der Revisionsbevollmächtigte.

– Für die Aufbewahrung von Datenträgern (elektronische und in Papierform) am Telearbeitsplatz hat der Dienstherr verschließbare Behältnisse bereitzustellen. Nach Beendigung der Telearbeit sind sämtliche Arbeitsunterlagen dort einzuschließen.

– Nicht mehr erforderliche Daten sind unverzüglich zu löschen. Alle verwendeten Datenträger (elektronische und papierene) sind grundsätzlich in die Dienststelle zurückzubringen, wenn sie am Telearbeitsplatz nicht mehr benötigt werden. Datenträger dürfen nur in der Dienststelle durch hierfür geeignete Verfahren (z. B. mit Reißwolf oder Schredder) vernichtet werden.

8 Fazit

Datenschutzrechtliche Vorschriften stehen der Einrichtung von Telearbeitsplätzen grundsätzlich nicht entgegen. Es sind aber technische und organisatorische Maßnahmen umzusetzen, die entsprechend der Sensibilität der zu verarbeitenden personenbezogenen Daten erforderlich und angemessen sind. Vor der Einführung von Telearbeit ist deshalb ein Sicherheitskonzept zu erstellen, das die geeigneten Maßnahmen detailliert festlegt.

Bestimmte Daten sollten nicht auf Telearbeitsplätzen verarbeitet werden. Das betrifft insbesondere Patientendaten, die der ärztlichen Schweigepflicht, und andere sensible Daten, die einem Amts- oder besonderen Berufsgeheimnis unterliegen. Werden dennoch Telearbeitsplätze für die Verarbeitung dieser Daten eingerichtet, ist im Rahmen der Vorabkontrolle nach § 19 Abs. 2 DSG M-V die Zulässigkeit der Datenverarbeitung zu prüfen.

Technische Maßnahmen müssen durch organisatorische Regelungen ergänzt werden. Neben der Dienstvereinbarung zwischen Personalrat und Dienststelle ist die Einzelvereinbarung zwischen Bedienstetem und Dienststelle von besonderer Bedeutung, weil nur in diesem Rahmen das für die Kontrolle notwendige Zutrittsrecht zu den Privaträumen des Telearbeiters gewährt werden kann.

Telearbeitsplätze können nur auf Basis der Freiwilligkeit eingerichtet werden. Der Bedienstete kann die Einwilligung jederzeit widerrufen, was zur sofortigen Beendigung des Telearbeitsverhältnisses führt.