Telearbeit...
aber datenschutzgerecht

Orientierungshilfe und Checkliste

Landesbeauftragter für den Datenschutz Niedersachsen

Vorbemerkung

Telearbeit wird in Wirtschaft und Verwaltung zunehmend als Mittel zur Kostenreduzierung und zur Flexibilisierung der Arbeitszeit eingesetzt. Unter Telearbeit versteht man im allgemeinen eine berufliche Tätigkeit, die außerhalb konventioneller Betriebsstätten unter Nutzung von Telekommunikation durchgeführt wird. Als Organisationsformen sind heute erkennbar:

- Teleheimarbeit, bei der die Beschäftigten zu Hause arbeiten.
- Alternierende Telearbeit als Kombination aus Büroarbeit und Arbeit zu Hause.
- Telearbeit in Satellitenbüros, die Unternehmen bzw. Behörden für mehrere Mitarbeiter in Wohnortnähe einrichten.
- Virtuelle Büros, die von rechtlich unabhängigen und räumlich getrennten Selbständigen auf Dauer oder für die Abwicklung von Projekten eingerichtet werden.
- Telecenter, die mit multifunktionaler Informations- und Kommunikationstechnologie ausgestattet sind.
- Mobile Telearbeit, bei der, unterstützt durch entsprechende Informations- und Kommunikationstechnik (z.B. Notebooks mit Mobilanschluß), unabhängig von einer festen Arbeitsstätte gearbeitet werden kann.

Die Telearbeiter stehen in unterschiedlichen Arbeitsverhältnissen zu ihren Auftraggebern, z. B. auf der Basis eines konventionellen Arbeitnehmerverhältnisses, Tätigkeit nach dem Heimarbeitsgesetz, Mitarbeit nach mitarbeiter-ähnlichem Status und als selbständige Handelsvertretung.

Für die technische Realisierung des Datenaustausches zwischen Telearbeitsplatz und Arbeitsstätte stehen diverse Möglichkeiten zur Verfügung, so z.B.:

- Konferenzsystem
  Hierbei werden Daten von zu Hause oder von unterwegs an den Kommunikationsrechner der Firma über Modem/ISDN übertragen. Dazu ruft der Telearbeiter in der Firma an, damit ein Firmenmitarbeiter die Verbindung zum Telearbeitsplatz aufbauen kann. Nach der Übertragung wird am Kommunikationsrechner ein Virencheck durchgeführt, und die Daten werden zur Weiterverarbeitung (ggf. über Diskette) freigegeben (Schleusenmechanismus). Die Administration erfolgt durch den Telearbeiter.
- Remote-Access zu einer Workstation
  Der Telearbeiter wählt sich über eine Modemverbindung über den Firmen-PC in ein Netzwerk. Dadurch hat er von zu Hause aus dieselben Zugriffsrechte (z.B. auch E-Mail), als wenn er selbst in der Firma an seinem Arbeitsplatz wäre. Die Administration erfolgt durch den Telearbeiter.
- Remote-Access zu einem Server
  Der Telearbeiter meldet sich zum Datenaustausch oder Nutzung des E-Mail-Verfahrens an einen Server über das Modem/ISDN an. Die Identifikation und Authentifikation des Telearbeiters wird überprüft und nach dem „Call-Back"-Verfahren zurückgerufen (erneuter Verbindungsaufbau). Die Administration erfolgt zentral.
- E-Mail als öffentliche Lösung über das Internet
  Der Telearbeiter greift beim Datenaustausch über das öffentliche Telefonnetz auf das Internet zu. Von hier aus geht die Verbindung zu einem Server, der mit einer Firewall abgesichert ist. Bei diesem Verfahren können Daten über das Internet auch an Externe gelangen oder im öffentlichen Internet mitgehört werden.
- E-Mail als öffentliche Lösung über Mailbox
  Für den Telearbeiter wird eine Mailbox eingerichtet, in die E-Mails und Dokumente hinterlegt werden können. Es besteht keine direkte Verbindung zur Firma.

Datenschutz

Für die Telearbeit im Rahmen eines Arbeits- oder Dienstverhältnisses trägt grundsätzlich der Arbeitgeber die datenschutzrechtliche Verantwortung. Dabei ist für Stellen der Wirtschaft (nicht-öffentliche Stellen) das Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen in Niedersachsen das Niedersächsische Datenschutzgesetz (NDSG) anzuwenden.

Nach § 9 BDSG bzw. § 7 NDSG haben datenverarbeitende Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen. Der Aufwand für die Maßnahmen muß unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen. Die Datensicherung kann dann als wirksam angesehen werden, wenn die getroffenen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch leisten. Sicherungsziele sind:

- Gewährleistung der Vertraulichkeit der Daten,
- Sicherstellung der Integrität der Daten,
- Gewährleistung der Authentizität der Daten,
- Gewährleistung der Authentifikation von Benutzern,
- Gewährleistung der sicheren Zustellung,
- Sicherstellung der Verfügbarkeit,
- Sicherstellung der Revisionsfähigkeit.

Erfolgt eine Verarbeitung personenbezogener Daten durch Telearbeiter auf der Basis von Werkverträgen in der Privatwohnung oder in Nachbarschafts- oder Satellitenbüros, unterliegt die Telearbeit in der Regel den Vorschriften der Datenverarbeitung im Auftrag (§ 11 BDSG bzw. § 6 NDSG). Ein solcher Telearbeiter darf die Daten nur nach den Weisungen des Auftraggebers verarbeiten und nutzen. Auch hier bleibt der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Dies gilt nicht, sobald dem Telearbeiter eine rechtliche Zuständigkeit für die Aufgabe zugewiesen worden ist (sog. Funktionsübertragung).

Für die Telearbeit sind Kontrollmöglichkeiten nicht nur durch den Arbeitgeber, sondern auch durch den internen Datenschutzbeauftragten (§§ 36, 37 BDSG bzw. § 8 NDSG), den Landesbeauftragten für den Datenschutz (§ 22 NDSG) bzw. die Aufsichtsbehörde für die Datenverabeitung im nicht-öffentlichen Bereich (§ 38 BDSG) zu gewährleisten. Hierfür muß ein Zugang zum häuslichen Arbeitsplatz gesichert sein. Dazu bedarf es wegen der Unverletzlichkeit der Wohnung jedoch der ausdrücklichen Einwilligung der betroffenen Beschäftigten. Dies muß zur Voraussetzung für die Ausübung der Telearbeit erklärt werden. Erfolgt der Widerruf einer solchen Einwilligung, ist die Telearbeitsmöglichkeit sofort aufzuheben.

Gefahren- und Risikoanalyse

Telearbeit in Wirtschaft und Verwaltung schafft neben vielen Vorteilen auch Gefahren und Risiken für die erklärten Sicherungsziele. Konkrete Gefahren sind z.B. der unkontrollierte Einsatz von Betriebsmitteln, die fehlerhafte Administration von Zugangs- und Zugriffsberechtigungen, Computerviren, der Mißbrauch von Fernwartungszugängen, die Nutzung der luk-Technik durch unbefugte Personen und das Eindringen in Kommunikationsnetze. Die Auftraggeber sind verpflichtet, vor der Entscheidung über den Aufbau und die technische Ausgestaltung von Telearbeitsplätzen zu prüfen, ob und in welchem Umfang mit der Telearbeit wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien Gefahren für die Rechte der Betroffenen verbunden sind (Art. 20 EU-Datenschutzrichtlinie bzw. § 7 Abs. 3 NDSG). Telear-

beitsplätze dürfen danach nur eingerichtet werden, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können.[1]

Technische und organisatorische Maßnahmen

Eine ausreichend sichere Form der Telearbeit wird erreicht, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen ausreichenden Schutz bieten. Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich nach der Sensibilität der verarbeiteten Daten und nach der jeweiligen technischen Anbindung des Telearbeitsplatzes. Wird eine dieser Maßnahmen vernachlässigt, ist eine sichere Telearbeit nicht möglich.
Neben meiner Checkliste können Sie zur datenschutzgerechten Ausgestaltung eines Telearbeitsplatzes weitere datenschutzrelevante Rechtsvorschriften, Empfehlungen, Orientierungshilfen, Checklisten sowie sonstige Materialien unter der Internetadresse www.lfd.niedersachsen.de finden bzw. herunterladen. Darüber hinaus bietet auch das IT-Grundschutzhandbuch[2] wertvolle Hilfen zur Grundsicherung eines Telearbeitsplatzes.

Wenn ein Telearbeitsplatz nicht ausreichend durch technische und organisatorische Maßnahmen gesichert werden kann, muß auf die Telearbeit mit personenbezogenen Daten verzichtet werden.

Handlungsempfehlungen

Die Orientierungshilfe weist auf Gefahren und Risiken bei Aufbau und Einsatz von Telearbeitsplätzen hin und gibt konkrete Empfehlungen für technische und organisatorische Sicherungsmaßnahmen. Dabei wird unterstellt, daß zwischen dem Arbeitsplatz zu Hause und der Arbeitsstätte eine Telekommunikationsverbindung besteht.

Die Orientierungshilfe will
- Geschäfts- und Behördenleitung,
- Personalleitung und Personalvertretung sowie
- Organisations- und DV-Leitung

in die Lage versetzen, die erforderliche Technikfolgenabschätzung vorzunehmen und ein Konzept für einen datenschutzgerechten Telearbeitsplatz zu finden.

Die LfD-Orientierungshilfe erhebt keinen Anspruch auf Vollständigkeit. Änderungs- und Erweiterungsvorschläge werden gern entgegengenommen.

[1] Orientierungshilfe für Technikfolgenabschätzungen
[2] Bundesamt für Sicherheit in der Informationstechni (BSI), IT-Grunschutzhandbuch, 1998

Checkliste

Die folgende Checkliste soll eine Hilfestellung für die Erarbeitung datenschutzgerechter Lösungen bei der Einrichtung von Telearbeitsplätzen leisten. Sie konzentriert sich auf die Gesichtspunkte des technisch-organisatorischen Datenschutzes bei der Telearbeit. Die Checkliste unterteilt folgende Bereiche:

- Infrastrukturelle Sicherheit des Telearbeitsplatzes
  Der Telearbeitsplatz muß so gestaltet sein, daß im unsicheren Einsatzfeld eine sichere Nutzung möglich ist. Es müssen vergleichbare Sicherheitsstandards wie bei einem Büroraum/Gebäude in einem Unternehmen/Behörde gelten.
- Organisation der Telearbeit
  Die datenverarbeitende Stelle muß ihre Organisation so gestalten, daß die Kontrollmaßnahmen wirksam werden können. Dabei müssen die getroffenen Regelungen über die Telearbeit den besonderen Anforderungen des Datenschutzes entsprechen.
- Sicherheit des Telearbeitsrechners
  Die Frage nach angemessenen Datensicherungsmaßnahmen stellt sich verstärkt bei Telearbeitsrechnern. Schon bei der Anschaffung der Geräte sollte auf eine Sicherheitsausstattung Wert gelegt werden. Mindestanforderungen an den Telearbeitsrechner sind zu definieren.
- Sichere Kommunikation zwischen Telearbeitsrechner und Arbeitsstelle
  Da die Kommunikation über öffentliche Netze geführt wird, sind besondere Sicherheitsanforderungen für die Kommunikation zwischen Telearbeitsrechner und Arbeitsstelle zu erfüllen.
- Sicherheit des Kommunikationsrechners der Arbeitsstelle
  Der Kommunikationsrechner stellt eine öffentlich zugängliche Schnittstelle dar, über die der Telearbeiter Daten der Arbeitsstelle nutzen kann. Hier ist ein Mißbrauch durch Dritte zu verhindern.

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen

- Erfüllt
- Nicht erfüllt
- Trifft nicht zu.

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkungstext ergänzt werden. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

1.	Infrastrukturelle Sicherheit des Telearbeitsplatzes	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
1.1	Der Zugang zum Telearbeitsplatz ist gesichert durch: • Besondere Schließzylinder, Zusatzschlösser oder Riegel bei Türen • Zusätzliche Sicherungen bei einstiegsgefährdeten Türen oder Fenstern (z.B. Rolladen) • Sicherung von Kellerlichtschächten • Verschluß von nicht benutzten Nebeneingängen • Verschluß von Fenstern und nach außen gehenden Türen in der Zeit, in der der Raum des Telearbeitsplatzes nicht benutzt wird				
1.2	Dienstliche Unterlagen (auch z.B. Datensicherungsbänder) werden in einem verschließbaren Schrank aufbewahrt.				
1.3	Familienangehörige haben keinen Zugriff auf dienstliche Unterlagen.				
1.4	Betriebs- und Sachmittel (Druckerpapier, Disketten etc.) werden datenschutzgerecht entsorgt.				
1.5	Fremde Personen halten sich nicht unbeaufsichtigt in dem Raum des Telearbeitsplatzes auf.				
1.6	Der Aktentransport/Datenträgertransport erfolgt in verschlossenen Behältnissen.				
1.7	Hard- und Software sind Eigentum des Arbeitgebers				
1.8	Ggf. Zusatzfrage:				

2	Organisation der Telearbeit	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
2.1	Die Regelungen über die Telearbeit sind in einer schriftlichen, allen Telearbeitern bekannten Anweisung festgelegt.				
2.2	Der Datenschutzbeauftragte hat die Möglichkeit einer Kontrolle (Einwilligungserklärung).				
2.3	Die Regelungen über die Wartung /Administration der Telearbeitsrechner sind in einer schriftli-				

2	Organisation der Telearbeit	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
	chen Anweisung festgelegt.				
2.4	Der Telearbeiter ist darauf hingewiesen worden, daß ein unkontrollierter Einsatz anderer Betriebsmittel (z.B. andere Hardware-Komponenten) nicht erlaubt ist.				
2.5	Protokollierungen über Inbetriebnahme, Benutzungen und Sicherheitsverstöße werden durchgeführt und regelmäßig kontrolliert.				
2.6	Die Protokollierungen werden nicht zur Verhaltens- und Leistungskontrolle verwendet.				
2.7	Die Telearbeiter sind ausführlich im Umgang mit der Technik und dem Datenschutz geschult worden.				
2.8	Ggf. Zusatzfrage:				

3	Sicherheit des Telearbeitsrechners	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
3.1	Der Zugriff auf Daten oder Programme des Telearbeitsrechners ist gesichert durch: • Paßwortschutz (fürs Booten, Bios, Netzwerk, Applikation), möglichst in Verbindung mit einer Chipkarten-Autorisierung • Pausenfunktion mit Tastatur- und Bildschirmsperre				
3.2	Die benutzten luk-Geräte werden von einer zentralen Stelle konfiguriert.				
3.3	Verändernde Zugriffe auf die Betriebssystemebene und auf Programme sind nur von der zentralen Systemadministration möglich.				
3.4	Lokale Datenbestände werden zwangsweise verschlüsselt. Die Verschlüsselungsmethode und die Schlüssel werden von der Zentrale vorgegeben.				
3.5	Nicht mehr erforderliche Daten werden frühstmöglich gelöscht.				
3.6	Auf dem Rechner werden nur dienstliche Daten verarbeitet und gespeichert.				

3	Sicherheit des Telearbeitsrechners	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
3.7	Der gespeicherte Datenbestand ist auf ein Minimum beschränkt				
3.8	Täglich läuft ein Virenscanner über den gespeicherten Datenbestand.				
3.9	Die Datensicherung erfolgt auf Diskette oder ähnlichen Datenträgern in mehreren Generationen. Die Sicherungsdatenträger sind unter Verschluß.				
3.10	Der Telearbeitsrechner kann Telefaxe senden und empfangen (integrierte Telefaxlösungen).				
3.11	Auf den Einsatz konventioneller Telefaxgeräte ist aus Datensicherungsgründen verzichtet worden.				
3.12	Das Rechnergehäuse ist verplombt, um Hardwaremanipulationen zu verhindern.				
3.13	Eine Dokumentation über die Systemkonfiguration liegt vor.				
3.14	Ggf. Zusatzfrage:				

4	Sichere Kommunikation zwischen Telearbeitsrechner und Arbeitsstelle	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
4.1	Die Router sind in einer gesicherten Umgebung aufgestellt. Unbefugte haben keinen Zugang zum Router.				
4.2	Bei lokaler Wartung und bei Fernwartung/Administration sind die eingeräumten Zutritts-, Zugangs- und Zugriffsrechte auf das notwendige Minimum beschränkt.				
4.3	Mögliche Kommunikationspartner sind eindeutig festgelegt.				
4.4	Bei der Übertragung werden sämtliche Daten verschlüsselt.				
4.5	Dokumente werden bei der Übertragung mit einer digitalen Signatur versehen.				
4.6	Ein Schlüsselmanagement ist eingerichtet worden.				
4.7	Die Konfiguration der ISDN-Karten ist dokumentiert.				

4	Sichere Kommunikation zwischen Telearbeitsrechner und Arbeitsstelle	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
4.8	Bei den ISDN-Netzkoppelelementen gibt es keine Fernwartung.				
4.9	Bei der Kommunikationssoftware sind die Paßwortabsicherung und die Protokollierungsfunktionen aktiviert.				
4.10	Die Protokolldateien werden regelmäßig kontrolliert.				
4.11	Alle nicht benötigten Funktionalitäten auf dem Router und der ISDN-Karte sind deaktiviert.				
4.12	Ggf. Zusatzfrage:				

5	Sicherheit des Kommunikationsrechner der Arbeitsstelle	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
5.1	Das Firmennetz ist durch eine Firewall geschützt.				
5.2	Bei Modem-Einsatz wird ein „Call-Back“-Verfahren genutzt.				
5.3	Ein Virenscanner wird täglich benutzt.				
5.4	Autorisierungen erfolgen über ein Challenge-Response-Verfahren.				
5.5	Für jeden Telearbeiter sind nur die Zugriffsrechte vergeben, die zur Aufgabenerfüllung erforderlich sind.				
5.6	Die Zugriffsrechte eines Telearbeiters sind zeitlich begrenzt, soweit dies organisatorisch möglich ist.				
5.7	Eine Dokumentation über die Systemkonfiguration liegt vor.				
5.8	Es wird eine Protokollierung über • erfolgreiche und nicht erfolgreiche Login-Versuche, • Kennwortänderungen, • Aktionen der Benutzerverwaltung (Löschung und Neueinrichtung von Benutzern) durchgeführt.				
5.9	Ggf. Zusatzfrage:				

5	**Sicherheit des Kommunikationsrechner der Arbeitsstelle**	**Erfüllt**			
			Nicht erfüllt		
				Trifft nicht zu	
					Bemerkung