



# Überschaubare Hindernisse

Ist die Auftragsdatenverarbeitung am Telearbeitsplatz mit dem Datenschutzrecht vereinbar? Der folgende Beitrag klärt auf über das Spannungsfeld Datenschutz bei der Telearbeit und zeigt per Checkliste, worauf Unternehmer achten müssen, die Telearbeitsplätze umsetzen wollen.

**Verrichten Arbeitnehmer die ihnen übertragenen Aufgaben zumindest teilweise nicht an einem für sie bereitgestellten Arbeitsplatz im Betrieb des Arbeitgebers, sondern über elektronische Kommunikationswege an einem anderen Ort**, insbesondere am eigenen Wohnort, spricht man von einem Telearbeitsplatz. Sofern im Rahmen dieser Tätigkeit personenbezogene Daten verarbeitet oder genutzt werden, sind die Vorschriften des Bundesdatenschutzgesetzes (BDSG) zu erfüllen.

Insofern gibt es im Falle von Telearbeit zunächst keine datenschutzrechtlichen Besonderheiten.

Besonderheiten entstehen erst dadurch, dass dem Arbeitgeber eine direkte Kontrolle der Datenverarbeitung nicht möglich ist. Der gesetzlich vorgesehenen Überwachung der Datenverarbeitung durch den Arbeitgeber, den Datenschutzbeauftragten, die Aufsichtsbehörde, den Betriebsrat usw. werden durch die räumliche Distanz und gesetzliche Regelungen Schranken gesetzt. Nachfolgend

nun ein paar praktische Hinweise, um potentiellen Datenschutzverstößen, wie sie in der Vergangenheit vorgekommen sind, präventiv zu begegnen.

## Pflichten des Arbeitgebers

Grundsätzlich ist die Verlagerung von Tätigkeiten in den häuslichen Bereich bei personenbezogenen Daten mit einem höheren Risiko der Persönlichkeitsverletzungen der Betroffenen verbunden, da ein Missbrauch

einfacher scheint. Die Unternehmen müssen besonders in diesem Fall die technischen und organisatorischen Maßnahmen gem. § 9 BDSG treffen, um die gesetzlichen Anforderungen zum Schutz der Daten zu erfüllen. Schutzmaßnahmen wie die Zutritts-, Zugangs- und Zugriffskontrolle auf die Daten sowie die Kontrolle der gesetzeskonformen Eingabe, Weitergabe und Speicherung müssen weiterhin gewährleistet sein.

Da der Telearbeiter seine Arbeit zuhause und nicht im Gebäude seines Arbeitgebers verrichtet, muss der Arbeitgeber, um seinen gesetzlichen Kontrollpflichten nachzukommen, die Möglichkeit zum Zugang zur Wohnung des Telearbeiters haben. Insofern besteht ein Spannungsverhältnis zwischen der Unverletzlichkeit der Wohnung (Art. 13 GG) und den bestehenden datenschutzrechtlichen Kontrollpflichten.

Da der Arbeitgeber kein grundsätzliches Zutrittsrecht hat, muss es arbeitsvertraglich vereinbart werden. Dabei sind auch Zutrittsrechte für den Datenschutzbeauftragten, den

Betriebsrat, die Gewerbeaufsicht etc. zu berücksichtigen.

### Weitere Anforderungen an den Arbeitgeber:

- Sorgfältige Personalauswahl der Telearbeiter inkl. Prüfung weiterer Arbeitsverhältnisse oder Nebenbeschäftigungen zur Vermeidung von Interessenskonflikten
- Klärung der infrastrukturellen Rahmenbedingungen des Telearbeitsplatzes (Größe der Wohnung, Anzahl der Zimmer, Zahl der dauerhaft anwesenden Personen, Hauptnutzung des Raumes, in dem der Telearbeitsplatz steht, etc.)
- Besondere auf die Telearbeit zugeschnittene und regelmäßig durchgeführte Datenschutzbildungen
- Vereinbarung einer aufhebenden Wirkung des Telearbeitsverhältnisses bei Wegfall der infrastrukturellen oder persönlichen Voraussetzungen des Arbeitnehmers

### Umzusetzende Sicherheitsmaßnahmen

Der Telearbeiter muss selbst Vorkehrungen zum Datenschutz und zur Informationssicherheit treffen. Dazu gehören beispielsweise Maßnahmen wie ein sicherer Umgang mit Passwörtern, ein Arbeitsplatz in einem für die Arbeitszeit verschließbaren Raum und nicht zuletzt ein verlässlicher Umgang mit Unternehmensdaten auch nach dem Ausscheiden des Arbeitnehmers. Entsprechende Regelungen zu den Anforderungen an den Arbeitsplatz und Weisungsbefugnisse sind ebenfalls im Arbeitsvertrag oder einer entsprechenden Anlage festzuhalten.

Darüber hinaus kann der Arbeitgeber den Datenschutz durch prozessuale und technische Maßnahmen sicherstellen. In der Praxis lassen sich ein Großteil der Kontrollpflichten in der Regel durch technische Vorkehrungen erfüllen. Dazu gehört die konsequent aktuelle Festlegung von Personen mit Zugangsberechtigung und deren regelmäßige Authentifizierung z.B. über

Anzeige

biometrische Daten, die Anbindung an Kundensysteme über geeignete technische Anbindungen wie z.B. VPN, die Verhinderung der Funktionen Kopieren, Verändern, Löschen oder das Auslesen von Daten, der Einsatz von One-Time-Passwörtern um unbefugten Zugang zu den Daten zu unterbinden sowie die Dokumentation, wer wann auf welche Daten zugreift oder Daten löscht, einfügt und ändert. Zudem wird die Umsetzung eines papierlosen Arbeitsplatzes empfohlen.

### Kontrollrechte des Auftraggebers im Falle einer Beauftragung von Dritten

Das BDSG sieht für Dienstleistungen im Rahmen einer Auftragsdatenverarbeitung gemäß § 11 BDSG noch einige darüber hinausgehende Pflichten für den Auftraggeber vor. Bei Bearbeitung von personenbezogenen Daten im Auftrag muss gewährleistet sein, dass die Daten auch am Telearbeitsplatz nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber als verantwortliche Stelle wird vom Gesetzgeber verpflichtet, eine datenschutzkonforme Datenverarbeitung durch den Auftragnehmer zu gewährleisten. Daraus ergibt sich zum einen die Verpflichtung einer datenschutzkonformen Vertragsgestaltung zwischen den Vertragsparteien (Geschäftsbesorgungsvertrag, Vereinbarung über die Auftragsdatenverarbeitung), aber zum anderen auch die Kontrollverpflichtung des Auftraggebers vor und während der Datenverarbeitung beim Auftragnehmer und damit letzten Endes auch beim Telearbeiter (Anwendung des Konzepts über die technischen und organisatorischen Maßnahmen). Dabei zeigt sich in der Praxis immer wieder, dass die bestehenden Vereinbarungen über die Auftragsdatenverarbeitung um die besonderen Anforderungen der Telearbeit ergänzt werden müssen. Hierfür sollte man sich ausreichend Zeit nehmen, um die sich daraus ergebenden Konsequenzen zu verstehen und um keine unerfüllbaren Zusätze zu vereinbaren.

### Fazit

Trotz oder gerade wegen der aktuellen Diskussion über die Sicherheit der Datenübertragungswege, in deren Rahmen ganz neue

## CHECKLISTE ZUR EINHALTUNG DER ANFORDERUNGEN DES § 9 BDSG:

<p><b>ORGANISATORISCHES</b></p> <p><b>Datenbestimmung</b> Auswahl der Daten, die am Telearbeitsplatz bearbeitet werden dürfen</p> <p><b>ITK</b> Anforderungen an die Hardware</p> <p><b>Verträge / Richtlinien</b> Arbeitsvertrag, Dienstvertrag, Datenschutzerklärung, Datensicherheitsrichtlinien, Nutzungsumfang der Hardware, Anforderungen an die Datenanbindung</p> <p><b>Schulungen</b> Datenschutzschulungen Schulungen zum Umgang mit Hard- und Software</p>	<p><b>WEITERGABEKONTROLLE</b></p> <p><b>Übertragungswege</b> VPN, Internetanbindung, Transport gedruckter Daten (nur, wenn kein papierloser Arbeitsplatz umsetzbar ist) und Transport von Datenträgern</p>
<p><b>ZUTRITTSKONTROLLE</b></p> <p><b>Arbeitszimmer</b> Lage im Haus, Sicherungsvorkehrungen Zutrittsberechtigungen</p>	<p><b>EINGABEKONTROLLE</b></p> <p><b>Protokollierung</b> Speicherung von Eingaben und Änderungen in Systemen</p> <p><b>Secure-Desktop</b> Kopieren und unkontrolliertes Ändern von Daten verhindern</p>
<p><b>ZUGANGSKONTROLLE</b></p> <p><b>Authentifizierung</b> Abgleich biometrischer Daten</p> <p><b>Verschlüsselung</b> Einsatz geeigneter Software</p> <p><b>Dokumentenmanagement</b> Papierloses Büro, Umgang mit Datenträgern</p> <p><b>Monitor</b> Standort, Passwortschutz, automatische Sperrung ⚡15 min (Bildschirmschoner)</p>	<p><b>AUFTRAGSKONTROLLE</b></p> <p><b>Auftragsdatenverarbeitung</b> Vereinbarung mit freien Mitarbeitern</p>
<p><b>ZUGRIFFSKONTROLLE</b></p> <p><b>Dokumentation</b> Datenzugriffe speichern</p> <p><b>Rechte-Verwaltung</b> Regelung und Kontrolle der Zugriffe</p>	<p><b>VERFÜGBARKEITSKONTROLLE</b></p> <p><b>Updates</b> Abgestimmte Automatisierung der Programmaktualisierungen</p> <p><b>Virenschutz</b> Aktueller und automatisierter Schutz</p> <p><b>Firewall</b> Dem Stand der Technik entsprechender Schutz gegen Angreifer</p> <p><b>Datensicherung</b> Kontrollierte und regelmäßige Backups</p>
	<p><b>TRENNUNGSGEBOT</b></p> <p><b>Separierung</b> Getrennte Verarbeitung und Speicherung von privaten und dienstlichen Daten</p> <p style="text-align: right;">(Checkliste ohne Anspruch auf Vollständigkeit)</p>

Sicherheitslösungen bis zur Marktreife entwickelt und alle Beteiligten nochmal für das Thema sensibilisiert wurden, erscheint das Spannungsfeld zwischen Telearbeit und Datenschutz mit moderaten Mitteln auflösbar. Mit einem ganzheitlichen Konzept für Datenschutz und Datensicherheit,

ist die Auftragsdatenverarbeitung an Telearbeitsplätzen auch ohne datenschutzrechtliche Bedenken umsetzbar.



Felix Prömel (links), LL.M. ist gelernter Jurist und Berater bei der Junokai GmbH, Jens Mühlberg ist bei virtcom ebenfalls Berater tätig und hat sich auf die Virtualisierung von Organisationen und Prozessen spezialisiert.