Inhaltsübersicht

Information

1. Allgemeines*Hinweis:*

Die Verwendung und Definition der Begriffe **Telearbeit**, **mobile Arbeit** und **Homeoffice** ist in der wissenschaftlichen Literatur und betrieblichen Praxis uneinheitlich.

Auch werden in arbeitsrechtlichen Vorschriften unterschiedliche Begriffe verwendet und definiert; sie umfassen zudem unterschiedliche Anwendungsbereiche und sind untereinander nicht kongruent.

Im Wesentlichen anerkannt ist die Definition der **Telearbeit** als einer Tätigkeit, die regelmäßig (aber nicht notwendig ausschließlich) außerhalb der zentralen Betriebsstätte des Auftraggebers oder des Arbeitgebers erbracht wird, wobei bei der Ausführung dieser Tätigkeit Informations- und Kommunikationstechniken verwandt werden, die die Verbindung mit dem Betrieb des Arbeitgebers oder des Auftraggebers herstellen.

Deshalb wird hier der herkömmliche und ältere Begriff der **Telearbeit** als **Oberbegriff** verwendet.

Vgl. zu den unterschiedlichen Begriffen von Telearbeit, mobile Arbeit und Homeoffice und deren Definition und Formen Telearbeit – Allgemeines und Telearbeit – Definition und Formen .

Es gibt für den Bereich der **Telearbeit** bzw. für die mobile Arbeit oder die Arbeit im **Homeoffice** keine speziellen datenschutzrechtlichen Vorschriften.

Seit dem 25. Mai 2018 gilt die **Datenschutz-Grundverordnung** der EU (DSGVO) in allen EU-Mitgliedsstaaten unmittelbar.

Mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30.06.2017 wurde unter anderem das Bundesdatenschutzgesetz (BDSG) neu gefasst und gilt wie die DSGVO seit dem 25. Mai 2018.

Das Bundesdatenschutzgesetz (BDSG) gilt gem. § 1 Abs. 1 S. 1 BDSG für die Verarbeitung personenbezogener Daten durch **öffentliche** Stellen des Bundes, öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe

der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

Für **nichtöffentliche** Stellen gilt das Bundesdatenschutzgesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (§ 1 Abs. 1 S. 2 BDSG).

Daneben gelten noch **Landesdatenschutzgesetze** der einzelnen Bundesländer, die im Einzelfall beachtet werden müssen.

2. Das neue Bundesdatenschutzgesetz (BDSG - neu 2018)

Das *neu gefasste* Bundesdatenschutzgesetz (BDSG - neu 2018) ergänzt ab dem 25. Mai 2018 die unmittelbar geltende Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) um die Bereiche, in denen die EU-Verordnung den Mitgliedstaaten *Gestaltungsspielräume* belässt. Daneben werden mit dem neuen BDSG wesentliche Teile der Richtlinie (EU) 2016/680 (Datenschutz-Richtlinie Polizei und Justiz) umgesetzt.

Teil 4 des neugefassten BDSG und andere Artikel des Gesetzes enthalten besondere Bestimmungen für Datenverarbeitungen, die nicht unter die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und die Richtlinie (EU) 2016/680 fallen.

3. Datenschutz-Grundverordnung (DSGVO) der EU

Gem. Art. 6 DSGVO ist die Verarbeitung personenbezogener Daten nur aufgrund eines **Erlaubnistatbestands** zulässig ist. Das bedeutet im Einzelnen:

- Die betroffene Person hat ihre Einwilligung gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich;die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich.

Gem. Art. 5 DSGVO sind die folgenden sechs **Grundsätze für die Verarbeitung personenbezogener Daten** einzuhalten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
- Zweckbindung (d.h. Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke);
- Datenminimierung (d.h. dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt);
- Richtigkeit (d.h. alle angemessenen Maßnahmen sind zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden);
- Speicherbegrenzung (d.h. dass Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es erforderlich ist);
- Integrität und Vertraulichkeit (d.h. Sicherstellung einer angemessenen Sicherheit der personenbezogenen Daten, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Gem. Art. 9 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, **untersagt**. Es sei denn es liegen die in Art. 9 Abs. 2 , 3 und 4 DSGVO genannten **Ausnahmen** vor.

4. Datenschutz-Folgenabschätzung

Mit der neuen Datenschutz-Grundverordnung der EU ist eine Datenschutz-Folgenabschätzung vorgeschrieben, wenn ein Form der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge hat (Art. 35 Abs. 1 DSGVO). Das kann bei der **Verwendung neuer Technologien** - wie für das Arbeiten im Home-Office bzw. in Telearbeit - aufgrund der Art, des Umfangs, der Umstände und/oder der Zwecke der Verarbeitung der Fall sein. Besonders kann ein solches Risiko wegen der **besonderen Umstände der Arbeit von zu Hause** im persönlichen Bereich erforderlich sein.

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann gem. Art. 35 Abs. 1 S. 2 DSGVO eine einzige Abschätzung vorgenommen werden.

Der betrieblich Verantwortliche hat bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des **Datenschutzbeauftragten**, sofern ein solcher benannt wurde, einzuholen (Art. 35 Abs. 2 DSGVO).

Eine Datenschutz-Folgenabschätzung ist in den in Art. 35 DSGVO genannten Fällen **erforderlich.**

5. Arbeitgeberpflichten

Der Arbeitgeber trägt die datenschutzrechtliche **Gesamtverantwortung** und muss seine Mitarbeiter zur Einhaltung der bestehenden Gesetze sowie der betrieblichen Regelungen anhalten.

Der Arbeitgeber sollte daher insbesondere auf Folgendes achten:

- Der Arbeitgeber unterweist den Telearbeiter in datenschutzrechtlichen Bestimmungen und sorgt somit für eine ausreichende Qualifikation des Telearbeiters.
- Der Arbeitgeber sorgt für eine entsprechende Qualifikation des Mitarbeiters im Umgang mit der Soft- und Hardware.
- Der Arbeitgeber sorgt dafür, dass sowohl durch die Einrichtung am Telearbeitsplatz (z.B. abschließbare Aktenschränke) als auch durch die zur Verfügung gestellte Soft- und Hardware die Einhaltung der Datenschutzbestimmungen gewährleistet ist (z.B. durch Vorschaltung eines Passwortes oder einer Verschlüsselung).
- Ein betrieblicher Datenschutzbeauftragter darf nach Absprache mit dem Telearbeiter den Telearbeitsplatz besichtigen und ihn auf datenschutzrechtliche Vorschriften hin begutachten.

6. Regelungen für die Praxis

Folgende Aspekte sollten z.B. in den Regelungen für Telearbeit beachtet bzw. geregelt werden:

- **Arbeitszeitregelung:** Die Verteilung der Arbeitszeiten auf Tätigkeiten in der Institution und am häuslichen Arbeitsplatz muss geregelt sein. Auch müssen feste Zeiten der Erreichbarkeit am häuslichen Arbeitsplatz festgelegt werden.
- **Reaktionszeiten:** Es sollte geregelt werden, in welchen Abständen die Telearbeiter aktuelle Informationen abrufen (z.B. wie häufig E-Mails gelesen werden) und in welchem Zeitraum sie darauf zu reagieren haben.
- **Umgang mit vertraulichen Informationen:** Bei der Telearbeit werden Informationen sowohl analog, also z.B. auf Papier, als auch digital bearbeitet. Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden. Daher ist der komplette Lebensweg geschäftskritischer Informationen angemessen abzusichern.
- **Arbeitsmittel:** Es sollte festgeschrieben werden, welche Arbeitsmittel die Telearbeiter einsetzen können und welche nicht genutzt werden dürfen (z.B. nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten wird untersagt. Weiterhin könnte die Nutzung von Datenträgern, wie beispielsweise CDs, DVDs oder USB-Sticks untersagt werden, wenn der Telearbeitsplatz dies nicht erfordert.
- **Datensicherung:** Die Telearbeiter sind zu verpflichten, regelmäßig Datensicherungen der lokal gespeicherten Daten durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherungen in der Institution zur Unterstützung der Verfügbarkeit hinterlegt

wird.

- **Synchronisation von Datenbeständen:** Datenbestände, die sowohl in der Institution als auch an Telearbeitsplätzen bearbeitet werden sollen, müssen geeignet synchronisiert werden. Das Vorgehen bei der Synchronisation muss genau geplant werden, damit es nicht zu Konflikten und damit zu einem Datenverlust kommt, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbeständen geändert bzw. gelöscht haben. Es empfiehlt sich, hierfür geeignete Software einzusetzen.
- **Datenschutz:** Die Telearbeiter sind auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.
- **Datenkommunikation:** Es muss festgelegt werden, welche Daten auf welchem Weg übertragen bzw. welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen. Ebenso ist festzulegen, welche Dokumente zwischen Institution und häuslichem Arbeitsplatz transportiert werden dürfen und wie diese dabei geschützt werden.
- **Transport von Dokumenten und Datenträgern:** Die Art und Absicherung des Transportes von Dokumenten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution ist zu regeln. Vertrauliche Daten auf digitalen Datenträgern sollten nur verschlüsselt transportiert werden.
- **Meldeweg:** Die Telearbeiter sind zu verpflichten, sicherheitsrelevante Vorkommnisse unverzüglich an eine im Vorfeld zu bestimmende Stelle in der Institution zu melden.
- **Zutrittsrecht zum häuslichen Arbeitsplatz:** Für die Durchführung von Kontrollen und für die Verfügbarkeit von Akten und Daten im Vertretungsfall kann ein Zutrittsrecht zum häuslichen Arbeitsplatz (gegebenenfalls mit vorheriger Anmeldung) vereinbart werden.
- **Vertretungsregelung**: Für jeden Telearbeiter sollte ein Vertreter bestimmt werden, der über die laufenden Aktivitäten informiert sein muss, damit er auch kurzfristig die Vertretung übernehmen kann. Dazu müssen die Arbeitsergebnisse durch die Telearbeiter immer sorgfältig dokumentiert werden. Gegebenenfalls sind sporadische oder regelmäßige Treffen zwischen dem Telearbeiter und seinem Vertreter sinnvoll. Ergänzend muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall Zugriff auf die Daten auf den Telearbeitsrechner oder am Telearbeitsplatz vorhandene Unterlagen nehmen kann. Dieser Vertretungsfall sollte probeweise durchgespielt und vom Telearbeiter und seiner Vertretung ausgewertet werden.

Die Regelungen sind jedem Telearbeiter auszuhändigen. Entsprechende **Merkblätter** sind regelmäßig zu aktualisieren.

Die für die Telearbeit im Umgang mit Informationen und der Informations- und Kommunikationstechnik notwendigerweise umzusetzenden Sicherheitsmaßnahmen sind zusätzlich in einer **Sicherheitsrichtlinie** zur Telearbeit zu dokumentieren.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

7. Einrichtung und Organisation des Homeoffice-Arbeitsplatzes

Insbesondere folgende Datensicherheitsheitsaspekte sollten geregelt werden und der Arbeitnehmer sollte auf solche Regelungen in einer schriftlichen Arbeitsanweisung verpflichtet werden:

- klare und zuverlässige Zugangskontrolle, d.h. mindestens abschließbare Schränke oder abschließbares Arbeitszimmer, aber auch Sicherungen gegen unbefugten Zugang zur privaten Wohnung;
- wenn kein eigenes Arbeitszimmer vorhanden, Gestaltung eines eigenen Arbeitsbereiches und/oder eines Arbeitsplatzes, der nicht von Unbefugten einsehbar ist;

- Einsatz betriebseigener Hardware mit sicherer Remote-Anbindung an das Unternehmensnetzwerk, z.B. durch verschlüsselte Virtual Private Networks (VPN);
- Einrichtung von Verschlüsselungssystemen und Vergabe von Passwörtern, Deaktivierung von Ports und Druckerfreigaben und von unautorisierten (WLAN oder LAN)-Zugängen;
- Vergabe von Berechtigungen für Zugriffe auf das System, Regelungen für die Einhaltung von Passwortvergaben, Protokollierung von allen Zugriffen auf dienstliche IT-Anwendungen;
- Anwendung von zuverlässiger, stetig aktualisierter Sicherheitssoftware und Firewall, sowohl für den Homeoffice-Arbeitsplatz, dessen Verbindung zum Betrieb als auch für die private Wohnung und die

dort verwendeten privaten Endgeräte;
- Regelungen für ein Verbot des Zugriffs Dritter oder von Familienangehörigen auf dienstliche Geräte;
- strikte Trennung einer Nutzung von dienstlichen und privaten Endgeräten;
- Verbot dienstliche Telefonate in Anwesenheit anderer Personen oder über Lautsprecher zu führen;
- Verbot einer privaten Speicherung dienstlichen Daten, sofern nicht ausdrücklich gestattet;
- Sperren des Computers bei Verlassen des Arbeitsplatzes durch einen Bildschirmschoner und/oder mit Kennwortschutz;
- Ausdrucke unverzüglich aus dem Drucker entnehmen;
- Papierunterlagen stets sicher in abschließbaren Räumen oder Behältnissen verwahren;
- nicht mehr benötigte Dokumente sofort im Anschluss nach einem Arbeitstag datenschutzkonform oder nach unternehmensinternen Richtlinien entsorgen;
- Regelungen für den Transport von Datenträgern und anderen, insbesondere schriftlichen Unterlagen zwischen Homeoffice und Betrieb;
- Aufräumen und sichere Verwahrung sämtlicher Unterlagen nach dem Ende der Arbeit.

8. Nutzung privater Endgeräte

Private Endgeräte des Arbeitnehmers sollten aus Gründen des Datenschutzes grundsätzlich nicht für betriebliche Zecke genutzt werden.

Wenn es aus betrieblichen, unabweisbaren Gründen notwendig sein sollte, private Endgeräte zu nutzen, sollten zumindest folgende Bedingungen konkret und bezogen auf die betrieblichen Verhältnisse vorgeschrieben werden:

- Einsatz sicherer Remote-Anbindung an das Unternehmensnetzwerk, z.B. durch verschlüsselte Virtual Private Networks (VPN);
- Benutzung eines sichereren Passwortschutzes, aktueller Updates für Betriebssysteme, von Antivirensoftware und weiteren betrieblichen Sicherheitsanwendungen;
- vollständige technische Trennung von betrieblichen und privaten Daten in abgeschotteten Bereichen (z.B. Container-Lösungen) implementieren;
- zentrale Verwaltung der gesamten privaten Endgeräte (Mobile Device Management, MDM) oder einzelner Anwendungen (Mobile Application Management, MAM) für die Erstellung von betrieblichen Sicherungskopien und für die Löschung betrieblicher Daten.

9. Besonders schützenswerte, personenbezogene Daten

Zu den besonders schützenswerten, personenbezogenen Daten gehören vor allem die in Art. 9 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) genannten Angaben zur rassischen und ethnischen Herkunft, Gewerkschaftszugehörigkeit, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Arbeitgeber/Dienstherren sammeln im Laufe eines Berufslebens eine Fülle von persönlichen Daten über ihre Beschäftigten, die ein umfassendes Bild über die Betroffenen geben. Diese Daten bedürfen deshalb nach § 26 Bundesdatenschutzgesetz (BDSG) – für Beamte sowie Beamtinnen und Tarifbeschäftigte in Verbindung mit §§ 106 ff. Bundesbeamtengesetz (BBG) – eines besonderen Schutzes und unterliegen oftmals dem Personalaktengeheimnis.

Als besonders schützenswert sind auch personenbezogene Daten anzusehen, welche die gesetzlichen Sozialversicherungsträger über ihre Mitglieder bzw. Versicherten speichern.

Bei der Entscheidung, ob und ggf. unter welchen Vorkehrungen sich bestimmte Aufgaben für Telearbeit und Mobiles Arbeiten eignen, ist nach Auffassung des Bundesbeauftragten für Informationssicherheit und Datenschutz (Telearbeit und Mobiles Arbeiten, Ein Datenschutz-Wegweiser, Stand Juli 2020) **hinsichtlich des Umgangs mit besonders schützenswerten Daten zu differenzieren.**

Danach ist im Einzelfall zu entscheiden, ob das Risiko für einen Datenmissbrauch angemessen reduziert werden kann oder ob das unvermeidbare Restrisiko eine Datenverarbeitung im Rahmen von Telearbeit oder

Mobilem Arbeiten ausschließt.

Es gilt der **Grundsatz**: **Je sensibler und damit schützenswerter personenbezogene Daten sind, desto stärker sind sie zu schützen**.

Bei der Bewertung, ob und ggf. unter welchen Umständen für eine bestimmte Tätigkeit Telearbeit oder Mobiles Arbeiten in Betracht kommen, muss danach berücksichtigt werden, wie hoch das Risiko eines Missbrauchs oder unbefugten Zugriffs beim Umgang mit personenbezogenen Daten angesichts der gegebenen konkreten Arbeitsabläufe einzustufen ist.

Telearbeit und Mobiles Arbeiten sollten nach Auffassung des Bundesbeauftragten für Informationssicherheit und Datenschutz grundsätzlich als eine **voll elektronische Datenverarbeitung ohne Medienbruch, also ohne Wechsel der Medien**, ausgestaltet werden. Das heißt, die schriftliche Kommunikation mit dem Arbeitgeber/Dienstherrn, die Entgegennahme von Aufgaben, der Umgang mit personenbezogenen Daten und die Übermittlung der Arbeitsergebnisse sollten **automatisiert mit Hilfe von IT-Einrichtungen und über verschlüsselte elektronische Kommunikationswege** stattfinden.

Dadurch entfällt die Notwendigkeit Unterlagen zu transportieren, was ein hohes Risiko des Verlusts, der Beschädigung sowie der unbefugten Kenntnisnahme mit sich bringt. Bei medienbruchfreier Gestaltung birgt Telearbeit ein geringeres Missbrauchsrisiko als das Mobile Arbeiten. Im Gegensatz zu Mobilem Arbeiten können der Arbeitsplatz bei der Telearbeit vom Arbeitgeber/von der Dienststelle kontrolliert und Risiken minimiert werden.

Mobiles Arbeiten birgt hingegen immer das Risiko des Verlustes des mobilen Gerätes. Das hierdurch gegebene Risiko eines unbefugten Zugriffs auf personenbezogene Daten durch unbefugte Dritte kann allerdings reduziert werden, wenn die Daten auf dem mobilen Gerät **verschlüsselt** werden und der Transport des mobilen Gerätes nur **im gesperrten Zustand** erfolgt. Zur Authentifizierung eingesetzte, hardwarebasierte Vertrauensanker wie Sicherheitskarten sollten getrennt vom mobilen Gerät aufbewahrt werden.

(*Quelle: Der Bundesbeauftragte für Informationssicherheit und Datenschutz, in: Telearbeit und Mobiles Arbeiten, Ein Datenschutz-Wegweiser, Stand Juli 2020*)

10. Wahrung von Geschäftsgeheimnissen

Eine besondere Lage ergibt sich daraus, dass der Arbeitnehmer im Homeoffice, also in seinem privaten Bereich, mit Geschäftsgheimnissen in Form von Dateien oder schriftlichen Unterlagen arbeitet, die üblicherweise nicht aus dem betrieblichen Bereich hinausgelangen.

Zur Sicherung von Geschäftsgeheimnissen bei der Arbeit im Homeoffice reicht die übliche Formulierung in Arbeitsverträgen nicht aus, dass der Arbeitnehmer verpflichtet ist, Geschäftsgeheimnisse vertraulich zu behandeln.

Zur Sicherung von Geschäftsgeheimnissen, die im Homeoffice bearbeitet werden, kommen folgende **Maßnahmen** in Betracht:

- Schriftlich fixierte **Definition** dessen, was im Betrieb als Geschäftsgeheimnis anzusehen ist;
- **Kennzeichnung** vertraulicher Dokumente in denen Geschäftsgeheimnisse enthalten sind;
- **Übergabe** von Dokumenten mit Geschäftsgeheimnissen **nur an solche Beschäftigte** im Homeoffice, die diese unbedingt für ihre Arbeit brauchen ("need to know"-Prinzip);
- klare **Hinweise** und **Handlungsanweisungen** für die Beschäftigten in denen u.a. anhand von Risikokonstellationen und anschaulichen Beispielen dargestellt wird,

    - was im Betrieb als Geschäftgeheimnis anzusehen ist,
    - wie vertrauliche Dokumente gekennzeichnet sind,
    - dass vertrauliche Dateien mit Geschäftsgeheimnissen nicht privat gespeichert, auf einen USB-Stick geladen werden oder in anderer oder ähnlicher Weise in den Privatberich gelangen dürfen,

- dass Dokumente mit Geschäftsgeheimnissen nicht oder nur eingeschränkt ausgedruckt werden dürfen,
- das ausgedruckte Dokumente sicher, d.h. abschließbar, verwahrt werden und - soweit angezeigt - sofort nach Gebrauch geschreddert werden müssen,
- dass auf die Einhaltung der üblichen Sicherheitsmaßnahmen besonders geachtet wird, d.h. Nutzung verchlüsselter Kommunikation (VPN-Verbindung), Verwendung von Passwörtern und Einhaltung von Zugangsbeschränkungen und deren sichere Verwahrung sowie korrektes Ausloggen bei Verlassen des Arbeitsplatzes und bei Beendigung der Arbeit am PC bzw. Laptop oder anderen Endgeräten,
- die Einhaltung der speziellen Regelungen für den Transport von Datenträgern und anderen, insbesondere schriftlichen Unterlagen mit Geschäftsgheimnissen zwischen Homeoffice und Betrieb,
- die Verpflichtung zur Einhaltung der dazu im Betrieb einschlägigen - konkret benannten - organisatorischen und informationstechnischen Maßnahmen.

11. Kontrolle der Telearbeit im Homeoffice

Kontrollmaßnahmen des Arbeitgebers bzgl. der Telearbeit, insbesondere der im Homeoffice beschäftigten Arbeitnehmern, bedeuten datenschutzrechtlich gem. Art. 4 Nr. 2 DSGVO eine Verarbeitung personenbezogener Daten; dies unabhängig davon, ob sie verdeckt oder offen vorgenommen werden. Ob sie rechtlich **zulässig** sind ergibt sich aus § 26 BDSG i.V.m. Art. 88 DSGVO .

Sie sind gem. Art. 6 Abs. 1 S.1 a) DSGVO zulässig, wenn der Beschäftigte zu den Kontrollmaßnahmen seine **Einwilligung** erteilt und diese **freiwillig** (Art. 4 Nr. 11 DSGVO) erfolgt. Dabei ist gem. § 26 Abs. 2 S. 1 BDSG bei der Beurteilung der Freiwilligkeit die im Beschäftigungsverhältnis bestehende Abhängigkeit zu berücksichtigen.

Personenbezogene Daten von Beschäftigten dürfen - ohne eine vorherige Einwilligung - gem. § 26 Abs. 1 S. 1 BDSG für Zwecke des Beschäftigungsverhältnisses nur dann verarbeitet werden, wenn dies u.a. für die Entscheidung über die **Begründung** eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen **Durchführung** oder **Beendigung erforderlich** ist.

Zur **Aufdeckung von Straftaten** dürfen personenbezogene Daten von Beschäftigten gem. § 26 Abs. 1 S. 2 BDSG nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Als **präventive digitale Kontollmaßnahmen** des Arbeitgebers gegenüber den im Homeoffice beschäftigten Arbeitnehmern kommen dabei insbesondere in Betracht der Einsatz von

- Keylogger Anwendungen,
- Time Tracking Anwendungen oder
- Screenshot Monitoring.

11.1 Keylogger Anwendungen

Keylogger zeichnen alle Tastatureingaben an einem Computer auf, so dass der Arbeitgeber die gesamten durch die Tastatur gesteuerten Aktivitäten des Arbeitnehmers verfolgen, aufzeichnen und speichern kann und dies dem Arbeitgeber ein lückenloses Nutzungsprofil über dessen Aktivitäten verschafft.

Da ein heimlicher Keylogger-Einsatz in seiner Intensität einer verdeckten Videoüberwachung des Arbeitnehmers gleicht (vgl. hierzu BAG v. 27.7.2017 - 2 AZR 681/16), ist nach herrschender Meinung in der juristischen Literatur ein solcher Einsatz **nicht** als **präventive** digitale Kontollmaßnahme, sondern nur bei einem Anfangsverdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung aus dem Arbeitsverhältnis zulässig (vgl. nur Fuhlrott, NZA 2017, 1309; Däubler, NZA 2017, 1486; Frank/Heine, BB 2021, 250)

11.2 Time Tracking Anwendungen

Mit Time Tracking Anwendungen kann der Arbeitgeber produktive und unproduktive Zeiten des Arbeitnehmers am Computer erfassen und dadurch ein Nutzungsprofil erstellen und z.B. feststellen, zu welchen Zeiten der Arbeitnehmer sich an- oder abmeldet oder wie viel Arbeitszeit er für die Erledigung bestimmter Arbeiten konkret benötigt.

Wenn sich Time Tracking nur auf die digitale **Erfassung von An- und Abmeldezeiten** beschränkt, ist dies wie bei der analogen Erfassung der Arbeitzeit bei Stempeluhren rechtlich **zulässig**.

Wenn Time Tracking darüber hinaus auch festhält wie lange der Arbeitnehmer für die Bearbeitung bestimmter Aufgaben benötigt, wird in der juristischen Literatur nur eine **stichprobenartige Protokollierung** für **zulässig** gehalten.

Dagegen wird eine **dauerhafte lückenlose Erfassung** einzelner Arbeitschritte als Form der Leistungs- und Verhaltenskontrolle angesehen und außer bei einem hinreichenden Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung aus dem Arbeitsverhältnis als **unzulässig** angesehen (Frank/Heine, BB 2021, 250 mit weiteren Hinweisen auf die Literatur).

11.3 Screenshot Monitoring

Bei einem Screenshot Monitoring können stichprobenartig oder in kleineren oder größeren regelmäßigen Abständen Abbildungen bzw. Standbilder einer bestimmten Bildschirmeinstellung angezeigt und gespeichert werden.

Zur **Kontrolle von Verstößen gegen das Verbot einer Privatnutzung** des betrieblichen Computers im Homeoffice wird in der juristischen Literatur eine Anfertigung von drei Screenshots pro Arbeitstag als **hinnehmbar** angesehen; außerdem grundsätzlich als zulässig bei einem hinreichenden Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung aus dem Arbeitsverhältnis (Frank/Heine, BB 2021, 249 mit weiteren Hinweisen auf die Literatur).