„Homeoffice“ & Datenschutz

Arbeiten im „Home-Office“, Nutzung des Heim-Büros und Telearbeit, das sind seit einigen Wochen verstärkte Maßnahmen, die zur Bewältigung der COVID-19 Krise als mögliche Verhaltensweisen von Seiten der Österreichischen Bundesregierung propagiert werden.

Die Notwendigkeit einer Vereinbarung zur Telearbeit mit Mitarbeiter*Innen wurde bereits erörtert, und es wurde auch eine Mustervereinbarung zur Verfügung gestellt. Auch auf die Notwendigkeit der Aufzeichnung der Arbeitszeiten wurde bereits hingewiesen.

Dass die Verarbeitung der personenbezogenen Daten, die nun nicht mehr in Präsenz im Büro erfolgt, sondern „remote“ von einem anderen Ort, meist dem Wohnort der Mitarbeiter*Innen durchgeführt wird, nach den grundsätzlich gleichen Regeln abläuft, wie bei Präsenzarbeit (dh auf der gleichen Rechtsgrundlage mit Kunden, Lieferanten oder anderen Mitarbeiter*Innen oder beim Versenden des Newsletters oder Telefonaten), davon wird wohl auszugehen sein.

Zu bedenken ist jedoch, dass sich

1. **Abläufe ändern**, zB vermehrt Telefonkonferenzen oder Video-Konferenzen (intern und mit externen Beteiligten) genutzt werden, Webinare statt Präsenzseminaren angeboten werden, oder

2. im Heim-Büro ni**cht ganz so strenge „Sicherheitsvorkehrungen“** getroffen werden, weil auch andere Personen (Partner, Kinder) den gleichen Raum für eigene Tätigkeiten (Arbeit, Lernen etc..) nutzen.

Was jedoch gibt es aus datenschutzrechtlicher Sicht zu beachten.

Jeder Verantwortliche hat zum Schutz der personenbezogenen Daten **angemessene Sicherheitsmaßnahmen** (TOMs; technische und organisatorische Maßnahmen) iSd Art 32 DSGVO zu setzen.

Die folgende Checkliste nimmt auf ein Paper des BfDI aus dem Jahr 2017 Bezug; aktuell sehen viele Aufsichtsbehörden die Telearbeit und die notwendigen Sicherheitsmaßnahmen nicht ganz so streng, und kann auch davon abgewichen werden (siehe zB Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) mit vorläufiger Gültigkeit bis 11.5.2020; Stand 24.04.2020: Sonderinformation zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie). Hier ein Auszug daraus, wobei bei Gesundheitsdaten strengere Anforderungen gelten müssen:

- Idealerweise sollte **keine Speicherung von sensiblen Daten** auf dem **Privatgerät** erfolgen, ansonsten muss die **Möglichkeit zur unkomplizierten Löschung der Daten** bestehen.
- Die Kommunikation sollte möglichst **datensparsam** erfolgen.
- Mobile Geräte müssen mindestens durch eine **PIN** oder ein **Passwort geschützt** werden.
- Sobald die Nutzung dieser **Dienste nicht mehr erforderlich** ist, sind die damit verarbeiteten personenbezogenen Daten zu löschen, insbesondere die zu diesem Zweck gespeicherten Telefonnummern von privaten Geräten.

Ergänzend dazu ist zu bedenken, dass **private Geräte** oft auch von verschiedenen Personen verwendet werden. Dann sollten für jeden Benutzer des Gerätes ein **eigenes Benutzerkonto** eingerichtet werden, und sichergestellt werden, dass es keine Möglichkeit gibt, auf die Daten eines anderen Benutzers zuzugreifen.

Bitte beachten Sie auch, dass nicht nur die **„elektronischen" Daten**, die auf Geräten gespeichert werden, vertraulich zu behandeln sind, sondern auch Ausdrucke oder sonstige **Papierunterlagen** von

unbefugten Personen (und dazu zählen auch Familienmitglieder) nicht eingesehen werden dürfen, insbes. wenn darin Art 9 Daten (zB Gesundheitsdaten) oder besonders schützenswerte Daten (Kontoverbindungen, Finanzdaten, Ausweise ...) enthalten sind. Eine **„Clean-Desk"-Policy** ist daher mE eine absolute Notwendigkeit.

Der **„sichere" Transport der Daten** (vom Heimbüro zu den Kunden, Lieferanten, Mitarbeiter*Innen oder auch nur ins Büro an sich) ist sicherzustellen, wobei dies **nicht nur die elektronische Datenübermittlung**, sondern auch die Versendung per **Post** oder **Kurierdienst** betrifft. Hier bieten sich **File-Transferysteme** an, und diesen sollte der **Vorzug gegenüber herkömmlichem E-Mail** gegeben werden, insbes. wenn die **Kommunikation vertraulich** sein soll oder es **Art 9 DSGVO-Daten** (zB Gesundheitsdaten) betrifft.

Videokonferenzen, die mit Lieferanten, Kunden, Mitarbeiter*Innen abgehalten werden oder Webinare über Videokonferenztools stellen eine weitere datenschutzrechtliche Herausforderung dar. Hier ist insbes. darauf zu verweisen, dass nicht nur Zoom oder Cisco (Webex) oder Microsoft (Teams) derartige Möglichkeiten bieten, sondern es auch österreichische Anbieter zB eyeson oder faircom gibt, oder auch auf deutsche Provider mit circuit zurückgegriffen werden kann.

Grundsätzliche Informationen zu Videokonferenzen gibt es bereits im dataprotect-blog.

Andere Regelungen für das „Home-Office"

Unfallversicherung

Die Frage der „Unfallversicherung" im Home-Office wurde für die Dauer der COVID-19-Krise (mit einer Befristung) geregelt.

Betriebsvereinbarung

Meines Erachtens bedarf eine Home-Office-Regelung in einem Unternehmen **keiner Betriebsvereinbarung**; es ist auch möglich, die Vereinbarung zum Teleworking auf **individueller vertraglicher Basis** mit den Mitarbeiter*Innen zu treffen.

Zu beachten ist jedoch, dass sämtliche Tätigkeiten des Arbeitgebers, die dazu führen können, dass **technische Systeme** eingesetzt werden, **die das Verhalten der Mitarbeiter*Innen aufzeichnen** („überwachen“), schon dann zu einer Verpflichtung des Abschlusses eine Betriebsvereinbarung führen, wenn diese Möglichkeiten gar nicht genutzt werden, aber die objektive Möglichkeit besteht, die Mitarbeier*Innen zu „überwachen“ bzw. deren Verhalten nachzuvollziehen

Checkliste „Homeoffice“ & Datenschutz

(angelehnt an „Telearbeit – ein Datenschutzwegweiser“; BfDI: Stand 2017)

Datensicherheit beim IT-Einsatz

- Separates, abschließbares Arbeitszimmer
- Trennung zwischen beruflichem und privatem (Internet-Anschluss)
- Zugang des Berechtigten zu den sensiblen personenbezogenen Daten nur mit Benutzer-ID und PIN oder Karte (Einsatz zertifizierter Kartenlesegeräte erforderlich)
- Verbindung über ein „virtual private network“ (VPN)
- Verschlüsselung der Daten (Ende-zu-Ende Sicherheit),
- Zugangsmöglichkeit des Arbeitgebers und dessen Beauftragten für den Datenschutz sowie der zuständigen Datenschutzaufsichtsbehörde zum Telearbeitsplatz und dessen IT-Einrichtungen zu Kontrollzwecken unter Berücksichtigung des Hausrechts
- Sperrung von USB-Zugängen und anderen Anschlüssen
- Falls erforderlich, sichere Anbindung eines lokalen Druckers in unmittelbarer Nähe des Arbeitsplatzes mit Protokollierung von häuslichen Druckvorgängen
- keine private Nutzung der beruflich zur Verfügung gestellten IT-Ausstattung

sicherer Transport und sichere Aufbewahrung

- Datenträger nur verschlüsselt und Papierunterlagen nur in verschlossenen Behältnissen transportieren und aufbewahren
- Datenträger und Unterlagen nie unbeaufsichtigt lassen.

Weitere Empfehlungen

- Verantwortlichkeiten im Umgang mit personenbezogenen Daten sind umfassend vertraglich festzulegen
- Eine private Nutzung der vom Arbeitgeber zur Verfügung gestellten IT-Ausstattung ist nicht zulässig
- Private Hard- und Software darf am Telearbeitsplatz nicht eingesetzt werden
- Berufliche E-Mails und Telefonate dürfen nicht auf private Postfächer oder private Telefonanschlüsse/ Handys der Telearbeiter umgeleitet werden
- Bei der Entscheidung über einen Telearbeitsplatz ist der Beauftragte für den Datenschutz des Arbeitgebers rechtzeitig zu beteiligen;
- Die Datenschutzgrundsätze für Telearbeit sollten in einer Betriebs-/Dienstvereinbarung festgeschrieben werden

BSI IT-Grundschutz

M 2.113 Regelungen für Telearbeit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Für die Ausgestaltung der Rahmenbedingungen für Telearbeit sind verschiedene arbeitsrechtliche und arbeitsschutzrechtliche Aspekte zu beachten. So sollten strittige Punkte entweder durch Betriebsvereinbarungen oder zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen Telearbeiter und Arbeitgeber geklärt werden. In diesen Vereinbarungen sollten beispielsweise die Punkte "Freiwilligkeit der Teilnahme an der Telearbeit", "Mehrarbeit und Zuschläge", "Aufwendungen für Fahrten zwischen Betrieb und häuslicher Wohnung", "Aufwendungen z. B. für Strom und Heizung", "Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)" und "Beendigung der Telearbeit" geklärt bzw. geregelt werden.

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.

Folgende Aspekte sollten beispielsweise in den Regelungen für Telearbeit beachtet 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 CD s, DVD s 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.

Prüffragen:

- Sind alle relevanten Aspekte zur Telearbeit geregelt worden?
- Sind alle für die Telearbeit relevanten Sicherheitsmaßnahmen in einer Sicherheitsrichtlinie zur Telearbeit dokumentiert?
- Sind alle Telearbeiter auf die Einhaltung der Sicherheitsrichtlinie zur Telearbeit verpflichtet worden?
- Wurden den Telearbeitern die Regelungen und die Sicherheitsrichtlinie zur Telearbeit oder ein Merkblatt ausgehändigt, in dem die von ihnen zu beachtenden Sicherheitsmaßnahmen erläutert werden?
- Sind Vertreter für alle Telearbeiter benannt worden?
- Sind Vertretungsfälle für Telearbeiter erprobt worden?