Mobiles Arbeiten und Datenschutz in Zeiten der Corona-Pandemie

Dortmund, 26.03.2020: In der aktuellen Corona-Pandemie werden die Unternehmen und Einrichtungen von der Regierung aufgefordert, zur Vermeidung unnötiger sozialer Kontakte den Beschäftigten möglichst eine Erledigung der täglichen Arbeit von zu Hause aus zu ermöglichen.

Normalerweise ist die Einrichtung einer Arbeitsmöglichkeit zu Hause mit einigem organisatorischen Vorlauf verbunden, damit bei der Arbeit zu Hause der Datenschutz im gleichen Maße gewährleistet werden kann wie bei der Arbeit im Büro. In der derzeitigen Situation der Corona-Pandemie findet der Wechsel vom Büro zum heimischen Arbeitsplatz meist ohne lange Vorbereitungszeit statt. Das Katholische Datenschutzzentrum gibt zur Umsetzung des Datenschutzes auch in dieser Situation folgende Hinweise:

Telearbeit – Homeoffice – mobiles Arbeiten
Unter dem Begriff Telearbeit werden häufig alle Arbeitsformen zusammengefasst, bei denen Mitarbeiter einen Teil der Arbeit außerhalb der Gebäude des Arbeitgebers verrichten – unabhängig davon, ob die Arbeit von einem fest eingerichteten Arbeitsplatz oder von unterwegs (mobil) erfolgt. Die gesetzliche Definition unterscheidet jedoch zwischen Telearbeit im engeren Sinne und „mobilem Arbeiten“: Mit der Novellierung der Arbeitsstättenverordnung (ArbStättV) im November 2016 wurde der Begriff der Telearbeit erstmals gesetzlich definiert und damit auch von einer generellen Zulässigkeit ausgegangen. Die Verordnung definiert einen Telearbeitsplatz als einen durch den Arbeitgeber fest eingerichteten Bildschirmarbeitsplatz im Privatbereich des Arbeitnehmers und formuliert arbeitsrechtliche und arbeitssicherheitstechnische Mindeststandards. Erst wenn sowohl die Ausstattung geliefert und installiert als auch die arbeitsrechtliche Vereinbarung geschlossen ist, kann der Telearbeitsplatz in Betrieb gehen.

Im Gegensatz dazu ist mobiles Arbeiten (auch als Remote Work oder Mobile Office bezeichnet) bisher nicht gesetzlich definiert. Das mobile Arbeiten baut zwar – ebenso wie die Telearbeit – auf einer Verbindung zum Betrieb per Informations- und Kommunikationstechnik auf. Diese Arbeitsform zeichnet sich jedoch dadurch aus, dass sie weder an das Büro, noch an den häuslichen Arbeitsplatz gebunden ist. Die Mitarbeiter und Mitarbeiterinnen können von beliebigen anderen Orten mithilfe von Laptop, Tablet oder Smartphone über das mobile Netz ihre Arbeit unabhängig von festen Arbeitszeiten und festen Arbeitsplätzen erledigen. Auch ist nicht unbedingt geregelt, dass die Ausstattung durch den Arbeitgeber gestellt wird.

In der aktuellen Situation wird es also meistens um „temporäres mobiles Arbeiten“ gehen, auch wenn der Begriff „Home Office“ gerne verwendet wird. Die jetzt geschaffenen Möglichkeiten zum Arbeiten zu Hause sollen in der Regel nur einen temporären Charakter haben. Die dauerhafte Einrichtung von Home-Office-Arbeitsplätzen (offiziell: „Telearbeitsplätzen“ nach ArbStättV) kann nur unter erweiterten Voraussetzungen (z.B. Dienstvereinbarung und arbeitsvertragliche Vereinbarungen, Einhaltung der Vorgaben für einen Arbeitsplatz nach der ArbStättV) erfolgen.

Auch unter datenschutzrelevanten Aspekten unterscheiden sich die Anforderungen an einen Telearbeitsplatz von den Voraussetzungen für ein datenschutzkonformes temporäres mobiles Arbeiten.

Einsatz dienstlicher Endgeräte:
Auch beim mobilen Arbeiten muss die kirchliche Einrichtung als Verantwortliche im Sinne des Datenschutzes für die datenschutzkonforme Verarbeitung der personenbezogenen Daten sorgen.

Diesen Schutz wird der Verantwortliche beim Einsatz dienstlicher Endgeräte, die er selbst konfiguriert hat, einfacher sicherstellen können, als beim Einsatz privater Endgeräte.

Der Einsatz privater Geräte zu dienstlichen Zwecken muss nach § 20 KDG-DVO gesondert begründet werden.

In jedem Fall sollte den Beschäftigten eine Ansprechperson für technische Probleme zur Seite stehen. Außerdem müssen auch im häuslichen Umfeld die nötigen Sicherheitsmaßnahmen gewährleistet sein (z. B. sind das System und der Virenschutz mit Updates und Patches auf dem aktuellem Stand zu halten).

Sichere Datenverbindung:
Der Zugriff auf die Firmendaten und evtl. die Firmenanwendungen muss über eine „mithörsichere“ verschlüsselte Verbindung erfolgen. Hierzu bietet sich z.B. eine VPN (Virtual Private Network) – Verbindung an, die auf eine normale unverschlüsselte Internetverbindung aufgesetzt wird. Eine VPN-Verbindung benötigt Einstellungen auf dem Router oder der Firewall des Unternehmens und auf dem Endgerät, welches für das mobile Arbeiten genutzt werden soll. Eine andere Möglichkeit ist das Arbeiten in speziellen webbasierten Oberflächen wie z.B. CITRIX, wobei nicht nur die Daten, sondern auch die Anwendungen zentral auf den Servern des Unternehmens bleiben.

Lokale Daten auf dem Endgerät:
Dokumente in Bearbeitung und Arbeitsergebnisse werden am besten auf Datenträgern im Netz des Unternehmens bzw. der Einrichtung gespeichert So kann auch die regelmäßige Datensicherung (Backup) gewährleistet werden und die Daten sind keinem zusätzlichen Risiko durch alleinige lokale Speicherung ausgesetzt.

Auch wenn eine lokale Ablage von Daten auf dem Endgerät also möglichst vermieden oder reduziert werden sollte, lässt sich diese Ablage der Daten nicht ganz verhindern.

Der Datenspeicher des Endgerätes (z.B. die Festplatte) sind daher zu verschlüsseln, damit die Daten auf dem Gerät auch im Falle des Verlustes des Endgerätes geschützt sind.

Wenn z.B. mit CITRIX unter Einsatz eines privaten Endgerätes gearbeitet wird, muss CITRIX so konfiguriert werden, dass auf lokale Laufwerke (z.B. „C:\“) nicht zugegriffen werden kann. Sollte es aus technischen Gründen nicht möglich sein, den Zugriff zu unterbinden, müssen entsprechende Bestimmungen per Dienstanweisung kommuniziert werden.

Verhinderung des Zugriffs durch Dritte bei dienstlichen Endgeräten:
Das dienstliche Endgerät mit den darauf evtl. befindlichen Daten oder dem Zugang auf die dienstlichen Server ist vor dem Zugriff Dritter zu schützen.

Eine Mitnutzung des Rechners durch Familie oder Freunde, weil z.B. der eigene private Rechner gerade besetzt ist, ist durch eine Anweisung an die Beschäftigten zu untersagen. Auch wenn der Nachwuchs nur mal eben was im Internet nachschauen will, kann nicht sichergestellt werden, dass er bei der Nutzung des Endgerätes nicht doch Kenntnis von schützenswerten dienstlichen Daten erhalten kann.

Vermeiden von Papier:
Der Arbeitsablauf sollte so gestaltet werden, dass keine Ausdrucke durch den Arbeitnehmer zu Hause nötig werden und dass auch keine schriftlichen Unterlagen für die Arbeit benötigt werden. Der notwendige „Dateninput“ kann z.B. über E-Mail oder Intranet verfügbar gemacht werden. Werden dennoch schriftliche Unterlagen mit personenbezogenen Daten bei der mobilen Arbeit benötigt, müssen diese in geeigneter Weise bei Transport und Aufbewahrung im häuslichen Umfeld gesichert werden. Welche Maßnahmen hier im Einzelfall notwendig sind, richtet sich nach der Sensibilität der personenbezogenen Daten.

Telefon- und Videokonferenzen:
Bei der Auswahl von Anbietern von Konferenzdiensten ist auf eine datenschutzkonforme Gestaltung der Systeme zu achten. Auch hier gilt in der Regel der z.B. von Messengerdiensten bekannte Grundsatz, dass die Dienste entweder mit Geld oder mit Daten bezahlt werden. Vor der Nutzung der Dienste sollte daher überprüft werden, inwieweit diese Dienste Zugriff auf die Inhalts- oder Metadaten der Kommunikation haben (wollen). Zur Wahrung der Vertraulichkeit müssen intelligente Lautsprecher (z.B. Amazon-Echo, Google-Assistent oder Cortana), die das gesprochene Wort aus dem Wohnzimmer über das Internet an den Hersteller übertragen, während der Konferenzen ausgeschaltet sein.

Organisation der Arbeit zu Hause
Bei der Arbeit zu Hause sollte der Arbeitsplatz so organisiert sein, dass dienstliche und private Daten nicht gemischt werden. Wird der Arbeitsplatz verlassen, ist der Kennwortschutz zu aktivieren, damit ein unberechtigter Zugriff auf die Daten ausgeschlossen werden kann. Auch Papierakten müssen dann angemessen gesichert werden.

Bei der Arbeit mit dienstlichen Computern sollten keine privaten USB-Sticks oder andere private Hardware genutzt werden, um die Gefahr eines Befalls der dienstlichen Geräte mit Schadsoftware zu verringern. Sofern doch einmal der Verdacht besteht, dass ein Befall mit Schadsoftware vorliegen könnte, ist sofort die Einrichtung zu verständigen.

Werden Ausdrucke oder Notizen nicht mehr benötigt, dürfen diese nicht einfach in den privaten Papiermüll entsorgt werden. Auch bei der Entsorgung ist der Datenschutzeinzuhalten (z.B. durch Vernichtung mit einem privat vorhandenen Aktenvernichter oder durch Sammlung der Dokumente und Entsorgung bei der nächsten Möglichkeit im Büro).

Rückkehr in den Normalbetrieb
Alle Maßnahmen sind unter Beachtung der Schutzziele des Datenschutzes so zu gestalten, dass die temporäre mobile Arbeitsweise jederzeit reibungslos und unterbrechungsfrei in den Normalbetrieb zurückgeführt werden kann.

Diesen Text finden Sie auch hier als Infoblatt.