Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Gemeinsame Stellungnahme des Beauftragten für den Datenschutz der EKD und des Beauftragten für den Datenschutz der Nordkirche zum Homeoffice im Zusammenhang mit der Corona-Pandemie

27. März 2020

Herausgegeben vom
Beauftragten für den Datenschutz
der Evangelischen Kirche in
Deutschland (BfD EKD)

Lange Laube 20
30159 Hannover

T. +49(511) 768128-0
F. +49(511) 768128-20

info@datenschutz.ekd.de
https://datenschutz.ekd.de

Aufgrund der Corona-Pandemie arbeiten viele Mitarbeitende kurzfristig im Homeoffice.

Wenn Mitarbeitende kurzfristig im Homeoffice arbeiten, ohne dass interne Regelungen – wie etwa eine Dienstvereinbarung – regeln, welche datenschutzrechtlichen Anforderungen zu beachten sind und auch keine dienstliche technische Infrastruktur zur Verfügung steht, haben diese oft nicht im Blick, wie personenbezogene Daten vor unbefugten Zugriffen zu Hause, beim Transport oder bei der Datenübertragung geschützt werden müssen. Dies betrifft das Arbeiten am Computer, mit Papierdokumenten und auch beim Telefonieren.

Zunächst muss allen Beteiligten bewusst sein, dass auch bei der Nutzung von Homeoffice oder Telearbeit die datenschutzrechtlichen Bestimmungen stets zu beachten sind und die datenschutzrechtliche Verantwortung nach wie vor bei der verantwortlichen Stelle – also z.B. dem kirchlichen Verwaltungsamt, der diakonischen Einrichtung – liegt und nicht beim einzelnen Mitarbeitenden. Aus diesem Grund hat der Arbeitgeber auch zu regeln, welche Tätigkeiten im Homeoffice durchgeführt werden dürfen und welche technischen und organisatorischen Maßnahmen hierbei zu beachten sind.

Aufgrund der erhöhten Risiken bei einem kurzfristig eingerichteten Homeoffice-Arbeitsplatz wird daran erinnert, dass interne Regelungen beim Umgang mit Datenpannen getroffen werden müssen. Alle Beschäftigten müssen vor allem wissen, wem in der Einrichtung Datenpannen zu melden sind.

Welche Tätigkeiten dürfen im Homeoffice durchgeführt werden?

Zunächst ist zu prüfen, ob die jeweilige Tätigkeit im Hinblick auf die konkrete Datenverarbeitung im Homeoffice erfolgen kann bzw. welche technischen und organisatorischen Maßnahmen im Hinblick auf die jeweilige Schutzbedürftigkeit zu treffen sind. Besonderer Beachtung bedarf hier die

Verarbeitung von Beschäftigtendaten, Sozialdaten und besonderen Kategorien personenbezogener Daten gemäß § 4 Nr. 2 EKD-Datenschutzgesetz (DSG-EKD).

Des Weiteren können auch Regelungen in Verträgen zur Auftragsverarbeitung (AV) der Verarbeitung personenbezogener Daten im Homeoffice entgegenstehen. So enthält beispielsweise § 5 Abs. 8 Mustervertrag AV BfD EKD ein Verbot der Verarbeitung personenbezogener Daten in Privatwohnungen durch den Auftragsverarbeiter. Ausnahmen bedürfen der vorherigen Zustimmung der kirchlichen Stelle. Es wird empfohlen, die Zustimmung schriftlich einzuholen.

Was ist bei der Einrichtung des Arbeitsplatzes und beim Arbeiten im Homeoffice zu beachten?

Es ist wichtig, dass keine Vermischung privater und dienstlicher Daten stattfindet. Papierdokumente müssen in einem verschlossenen Schreibtisch oder Schrank aufbewahrt werden.

Der Monitor darf nicht ohne weiteres eingesehen werden können. Hierbei kann auch eine Blickschutzfolie genutzt werden. Beim Verlassen des Arbeitsplatzes muss ein Bildschirmschoner mit Kennwortschutz eingeschaltet werden, damit keine unberechtigten Personen auf dienstliche Daten zugreifen können.

An einen dienstlichen Computer darf keine private Hardware (z.B. externe Festplatten oder USB-Sticks) angeschlossen werden. So kann das Risiko verringert werden, dass der Computer von Schadsoftware befallen und personenbezogene Daten kompromittiert werden. Falls der Computer doch infiziert wurde, ist dies schnellstens der verantwortlichen Stelle zu melden. Es muss jedem Mitarbeitenden bekannt sein, wer anzusprechen ist und wie diese Person erreichbar ist. Die nötigen Kontaktinformationen (Telefon/E-Mail) müssen jedem Mitarbeitenden griffbereit zur Verfügung stehen.

Liegt der Arbeitsplatz im Erdgeschoss, dann ist darauf zu achten, dass nach dem Verlassen des Arbeitsplatzes Türen und Fenster geschlossen sind, um eine unbefugte Kenntnisnahme, einen Verlust oder eine Veränderung der personenbezogenen Daten zu verhindern.

Ist die Nutzung privater IT-Infrastruktur (z.B. mobile Endgeräte, WLAN und Drucker) im Homeoffice zulässig?

Normalerweise ist die Nutzung privater IT-Infrastruktur im Homeoffice nicht zulässig.

Da es in der momentanen Situation für einige Arbeitgeber schwierig sein wird für alle Mitarbeitenden eine dienstliche IT-Infrastruktur zur Verfügung zu stellen, erfolgt zurzeit bei Verwendung einer privaten IT-Infrastruktur unter Einhaltung folgender Bedingungen keine Beanstandung durch die Aufsichtsbehörde:

- Bei der Verarbeitung personenbezogener Daten ist nach wie vor das **EKD-Datenschutzgesetz** – vor allem auch die Grundsätze - einzuhalten.
- **Mobile Endgeräte** müssen mindestens durch eine **PIN** oder ein **Passwort** geschützt werden, sodass allein der Mitarbeitende Zugang hat.

- Sobald die Nutzung der privaten IT-Infrastruktur nicht mehr erforderlich ist, sind die damit verarbeiteten personenbezogenen Daten unwiederbringlich zu löschen, insbesondere die zu diesem Zweck gespeicherten Telefonnummern von privaten Endgeräten.
- Mitarbeitende müssen sich in das Netzwerk der verantwortlichen Stelle über eine **sichere Verbindung** (Virtual Private Network, sog. VPN) einwählen. Gegebenenfalls muss der Zugriff auf sensible Bereiche ausgeschlossen werden.
- Mitarbeitende müssen Dokumente oder Arbeitsergebnisse in der IT-Infrastruktur der verantwortlichen Stelle speichern. So kann auch die übliche Datensicherung (Backup) gewährleistet werden.

Was ist bei der Nutzung eines privaten Internetanschlusses/ WLAN zu beachten?

Wenn der private oder dienstliche Computer mit einem privaten Internetanschluss/WLAN genutzt wird, muss dieser mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden sein. Das private WLAN muss in jedem Fall so eingerichtet sein, dass man sich nur mit einem Passwort einwählen kann.

Was ist bei der Nutzung privater Computer zu beachten?

Dienstliche Daten dürfen nicht auf dem privaten Computer gespeichert werden. Für die Speicherung dienstlicher Daten müssen externe Datenträger (z.B. externe Festplatten, USB-Sticks) verwendet werden. Der externe Datenträger ist spätestens mit Beendigung der Corona-Pandemie dem Arbeitgeber zu übergeben, der die personenbezogenen Daten anschließend unwiederbringlich löscht.

Was ist beim Drucken im Homeoffice zu beachten?

Dokumente, die am häuslichen Arbeitsplatz ausgedruckt werden, müssen unverzüglich aus dem privaten Drucker genommen werden, um eine Kenntnisnahme von unberechtigten Personen in dem Haushalt zu verhindern.

Bei der Nutzung von VPN: Es dürfen keine Druckaufträge auf die in den Dienstgebäuden befindlichen Drucker geschickt werden, da ansonsten nicht ausgeschlossen werden kann, dass unberechtigte Personen Einblick in diese Dokumente nehmen können.

Was ist beim Telefonieren im Homeoffice zu beachten?

Dienstliche Telefonate mit privaten oder dienstlichen mobilen Endgeräten sind in einem ungestörten Bereich bzw. bei geschlossener Tür zu führen, damit andere Personen im Haushalt keine Kenntnis von dem Telefonat nehmen können. Gespeicherte Telefonnummern auf privaten mobilen Endgeräten sind zu löschen, sobald sie nicht mehr benötigt werden.

Was ist beim Transport dienstlicher mobiler Endgeräte und dienstlicher Unterlagen zwischen Büro und Homeoffice zu beachten?

Das Laptop muss mit einem sicheren Passwort geschützt und die Festplatte sowie externe Speichermedien müssen verschlüsselt sein. Papierdokumente sind in einem verschließbaren Behälter (z.B. Aktentasche) zu transportieren und dürfen genauso wie elektronische Geräte während des Transports nicht unbeaufsichtigt sein.

Was ist bei der Müllentsorgung im Homeoffice zu beachten?

Dienstliche Papierdokumente dürfen nicht im privaten Papiermüll entsorgt werden. Vielmehr muss der Müll so gelagert werden, dass unberechtigte Dritte keine Kenntnis nehmen können. Eine Entsorgung des Papiermülls erfolgt dann im Büro nach den in der jeweiligen verantwortlichen Stelle geltenden Regeln.

Wird deutlich, dass die Arbeit im Homeoffice aufgrund der Corona-Pandemie länger andauern wird, dann ist es Aufgabe der verantwortlichen Stelle, über mündliche oder per E-Mail durch Vorgesetzte getroffene Anordnungen hinaus interne Regelungen zu treffen. Hierbei wird es notwendig, dass ein schriftliches Konzept erstellt wird. In diesem Konzept müssen insbesondere technische und organisatorische Maßnahmen beschrieben werden, die sicherstellen, dass personenbezogene Daten unter Beachtung der Anforderungen des Datenschutzes und der Datensicherheit im Homeoffice verarbeitet werden können.

Weitere Hinweise zu den Anforderungen an Datenverarbeitung im Homeoffice oder in der Form der Telearbeit finden Sie unter anderem hier:

„Telearbeit und Mobiles Arbeiten“ Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Stand: Januar 2019, 20 Seiten, deutsch
https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

„Home-Office? –Aber sicher!“ Information des Bundesamts für Sicherheit in der Informationstechnik (BSI), Stand: März 2020, 4 Seiten, deutsch
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.htm

Hannover, den 27.03.2020
Der Beauftragte für den Datenschutz der EKD