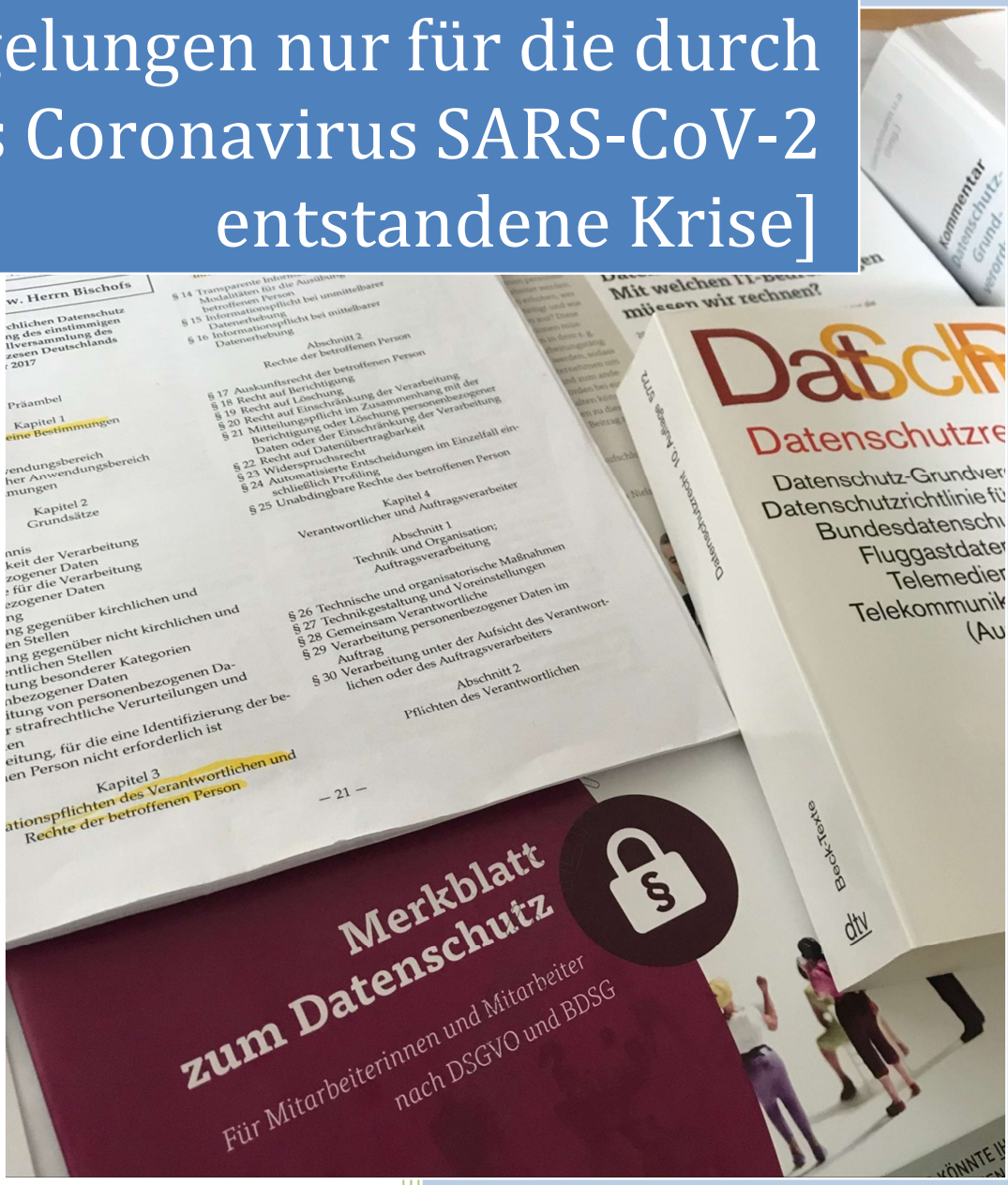
KATHOLISCH
Bistum Mainz

09

[Merkblatt zum Datenschutz im Home-Office. Regelungen nur für die durch das Coronavirus SARS-CoV-2 entstandene Krise]



Betriebliche Datenschutzstelle
im Bistum Mainz

Stand: Juli 2022

Datenschutz im Home-Office.
Regelungen nur für die durch das Coronavirus SARS-CoV-2 entstandene Krise

Vorwort

Aufgrund der rasanten Ausbreitung des Coronavirus (COVID-19) hat der Schutz der Mitarbeitenden und der Bevölkerung höchste Priorität. Daher wurde am 23. März 2020 die Dienstanweisung des Generalvikars: „Regelungen nur für die durch das Coronavirus SARS-CoV-2 entstandene Krise – vorläufig gültig bis zum 19.04.2020" veröffentlicht und unter Punkt 3 das Homeoffice benannt.
Da jedoch die datenschutzrechtliche Verantwortlichkeit (§ 4 Nr. 9 KDG und § 15 KDG-DVO) nicht an der Bürotür endet, folgen im Sinne der Einhaltung des KDG für die Arbeit im Home-Office und von unterwegs jedoch eindeutige und transparente Regeln, um die Rechte und Pflichten beider Seiten zu verdeutlichen.
Auch im Home-Office bzw. bei der Telearbeit müssen die Voraussetzungen zur Einhaltung der bestehenden datenschutzrechtlichen Bestimmungen des Kirchlichen Datenschutzgesetzes und deren Durchführungsverordnung gegeben sein. Die Verantwortlichkeit des Dienstgebers bleibt bestehen – egal wo und auf welchem Endgerät die Mitarbeitenden tätig werden. Darüber hinaus trägt aber auch jede Mitarbeitende nach § 17 KDG-DVO Verantwortung für die datenschutzkonforme Ausübung seiner bzw. ihrer Tätigkeit.

1) Arbeit auf dienstlichen Endgeräten im Home-Office und von unterwegs

Wenn Ihr/e Vorgesetzte/r entschieden hat, dass Sie nicht vom Ordinariat oder dem Pfarrbüro sondern von zu Hause aus arbeiten können, bitte wir um Einhaltung und Beachtung der folgenden Schutzmaßnahmen/Regeln (gilt nur wenn Sie an die Bistumscloud angebunden sind).

2) Schutzmaßnahmen im Home-Office

Beim Home-Office trägt der Arbeitgeber die datenschutzrechtliche Verantwortung. Daher sind folgende Regeln und Schutzmaßnahmen (nicht abschließend) zu beachten, wobei gilt, dass je sensibler und schützenswerter die personenbezogenen Daten sind (unter Beachtung der Schutzklassen I-III und Schutzniveau I-III), umso stärker muss der Schutz sein:

- das Arbeitszimmer sollte separat und abschließbar sein
- dienstliche Unterlagen sollten in einem abschließbaren Schrank aufbewahrt werden
- die dienstliche zur Verfügung gestellte IT-Ausstattung ist nicht privat zu nutzen
- das Betriebssystem ist mit einem Kennwort zu versehen
- Passwörter sind geheim zu halten
- die elektronische Datenübermittlung (also z.B. E-Mail) ausschließlich über die dienstliche Mailadresse
- wenn der Ehegatte/ Kinder oder Dritte (beispielsweise in einer Wohngemeinschaft) mit unter einem Dach wohnen, ist der Computer auch bei kurzzeitigem Verlassen zu sperren
- berufliche E-Mails sind nicht auf private E-Mail Postfächer weiterzuleiten

- Wenn Ihr/e Vorgesetzte/r entschieden hat, dass Sie die zur Arbeit benötigten Akten mit nach Hause nehmen müssen, bedürfen diese einer besonderen Sorgfaltspflicht. Die unberechtigte Kenntnisnahme dieser Akten durch Dritte muss ausgeschlossen werden.
- Transport der Unterlagen in einem geschlossenen Umschlag oder einem anderen Behältnis
- nicht mehr mitnehmen als unbedingt erforderlich
- keine Daten auf USB-Sticks oder tragbaren Festplatten
- im Einzelfall kann es erforderlich sein, dem Arbeitgeber und der zuständigen Datenschutzbehörde zu Kontrollzwecken eine Zugangsmöglichkeit einzuräumen.

3) Datensicherung im Home-Office

Die regelmäßigen Datensicherungen sind immer im Netzwerk (über Bistums-Cloud nach der bisherigen Struktur des Aktenplans bzw. Speicherordnung in der jeweiligen Abteilung) vorzunehmen. Arbeitsergebnisse sind nicht lokal zu speichern, da die Daten dann nicht mehr in die Datensicherung der EDV Abteilung einfließen.

4) Vernichtung von gedruckten Dokumenten

Sollten sie Ausdrucke anfertigen oder solche besitzen und sind diese zu vernichten, dann sind diese datenschutzkonform zu schreddern bzw. der ordnungsgemäßen Vernichtung zu einem späteren Zeitpunkt im Büro zu zuführen, jedoch keinesfalls als Schmier- noch Malpapier für die Kinder zweckentfremden. Grundsätzlich sollte der Ausdruck in dieser Zeit eine Ausnahme darstellen.

5) Meldepflicht bei Verletzung des Schutzes personenbezogener Daten (§ 33 KDG)

Bei der Verarbeitung von besonderen personenbezogenen Daten ist bei der Einrichtung des Heimarbeitsplatzes stets an die Rechtsfolgen des § 33 KDG zu denken.
Beim Auftreten einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche der Datenschutzaufsicht unverzüglich diese Verletzung - wenn sie eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt, binnen 72 Stunden nachdem die Verletzung erfolgte, gemeldet.
Daher hat die/der Mitarbeitende, wenn eine Verletzung bekannt wird, diese unverzüglich dem Verantwortlichen zu melden.

6) Umgehende Verlustmeldungen

Wenn der Fall eintritt, dass mobile Geräte (Laptop, Diensthandy …) oder auch Akten/ Unterlagen abhandengekommen sind, ist eine umgehende Verlustmeldung an den Dienstvorgesetzten notwendig (siehe Meldepflicht nach § 33 KDG).

7) Vorsicht Phishing

Durch COVID-19 können vermehrt Phishing-Mails im Umlauf sein, welche die aktuelle Situation ausnutzen wollen und versuchen werden sensible Daten abzugreifen. Daher auch keine Passwörter in unbekannte Systeme oder fremde LINKs eingeben.
Beantworten Sie keine Anfragen, an fremde Dritte. Löschen Sie lieber eine „Anfrage“ zu viel, wenn Ihnen der Absender oder der Inhalt verdächtig vorkommt.

8) Nutzung privater IT-Systeme zu dienstlichen Zwecken

Vorausgesetzt das bei der Gestaltung des Heimarbeitsplatzes auf die zuvor genannten Anforderungen eingegangen wird und eine schriftliche Zulassung nach § 20 Abs.2 lit a) bis g) KDG-DVO vorliegt, kann ausnahmsweise die dienstliche Nutzung privater Endgeräte aus datenschutzrechtlicher Sicht zugelassen werden.

9)Datenschutzrechtliche Fragen richten Sie bitte gerne an Ihre Betrieblichen Datenschutzbeauftragten:

Leitender Betrieblicher Datenschutzbeauftragter Wolfgang Knauer, Tel. 06131/253-889	
Gemeinsame Betriebliche Datenschutzbeauftragte für die Kirchengemeinden Michaela Beiersdorf, Tel. 06131/253-821	Bischöfliches Ordinariat Mainz Betriebliche Datenschutzstelle Weißliliengasse 2d, 55116 Mainz Postfach 1560, 55005 Mainz datenschutz@bistum-mainz.de
Datenschutzkoordinatorin Alexandra Glinka, Tel. 06131/253-857	

10)Diözesandatenschutzbeauftragte

Zuständigkeit Mittel- und Südwestdeutsche Bistümer

Diözesandatenschutzbeauftragte Ursula Becker-Rathmair	Katholisches Datenschutzzentrum Frankfurt Roßmarkt 23, 60311 Frankfurt am Main Tel.: 069 58 99 755-10 E-Mail: info@kdsz-ffm.de www.kath-datenschutzzentrum-ffm.de

Impressum:

Herausgegeben vom
Bischöflichen Ordinariat Mainz

Betriebliche Datenschutzstelle im Bistum Mainz
☎ 06131-253857
✉ Postfach 1560, 55005 Mainz
datenschutz@bistum-mainz.de

Redaktion: Wolfgang Knauer, Alexandra Glinka