ABl 6/2019, S. 237-241

Nutzung privater IT-Systeme zu dienstlichen Zwecken - erläuternde Hinweise zur Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz (KDG - DVO) - § 20 KDG-DVO

Der Einsatz privater Rechner zur Erledigung dienstlicher Aufgaben ist aus Gründen des Datenschutzes grundsätzlich nicht zulässig und nur in Ausnahmefällen nach schriftlicher Erlaubnis durch den Dienststellenleiter[1] gestattet. Der Einsatz privater Rechner von Religionslehrern/-innen i.K., von pastoralen Mitarbeitern/-innen, von Ehrenamtlichen in den Kirchenverwaltungen und den pastoralen Gremien sowie von weiteren Ehrenamtlichen auf ortskirchlicher Ebene, soweit sie im Rahmen ihres Ehrenamtes personenbezogene Daten verarbeiten, ist wegen der Besonderheit der Aufgabenwahrnehmung als ein solcher Ausnahmefall anzusehen.

Verantwortlicher/verantwortliche Stelle im Sinne von § 4 Ziffer 9 KDG (Art. 3 Abs.2 BayDSG) ist hierbei für:

- Religionslehrer/-innen i.K., die Schule,
- pastorale Mitarbeiter/-innen in der Kategorialseelsorge, die Diözese,
- pastorale Mitarbeiter/-innen in der Pfarrseelsorge, das jeweilige Pfarramt,
- pastorale Mitarbeiter/-innen mit Wechseleinsatz in der Kategorial- und Pfarrseelsorge, diejenige Dienststelle, an der der/die Mitarbeiter/-in überwiegend tätig ist, bei gleichen Anteilen, die Diözese,
- pastorale Mitarbeiter/-innen mit Wechseleinsatz in der Schule und der Pfarrseelsorge für Schülerdaten die Schule, für Daten aus der Pfarrseelsorge das jeweilige Pfarramt,
- Ehrenamtliche, das jeweilige Pfarramt.

Unabhängig davon, ob vom Dienstgeber ggf. ein Zuschuss zur Beschaffung eines privaten Rechners gewährt wird, oder der Rechner aus Eigenmitteln des/der Mitarbeiters/Mitarbeiterin bzw. des/der Ehrenamtlichen beschafft wird, sind bei der Nutzung von privaten Rechnern aller Art für dienstliche Zwecke nachstehende Richtlinien zu beachten.

1 .) Es dürfen ausschließlich solche Daten verarbeitet werden, die zur Erfüllung der rechtmäßigen Aufgaben des/der Mitarbeiters/-in des/der Ehrenamtlichen erforderlich sind.

2 .) Daten aus einer privaten Nutzung sind durch geeignete Maßnahmen, z.B. durch Speicherung und Verarbeitung auf getrennten Laufwerken, von denen zu trennen, die der dienstlichen Nutzung beziehungsweise dem Verantwortlichen/der verantwortlichen Stelle zuzuordnen sind.

3 .) Daten aus dienstlicher Nutzung dürfen Dritten, auch Familienangehörigen, außerhalb der rechtmäßigen Aufgabenerfüllung, nicht zugänglich gemacht werden. Durch geeignete Schutzmaßnahmen, z.B. Bearbeitung der Daten in einem separaten Raum, Wegsperren des Rechners nach der Bearbeitung der Daten u.a., ist sicherzustellen, dass Dritte auch nicht zufällig Kenntnis von Daten aus dienstlicher Nutzung erlangen.
Eine Datenübermittlung/Offenlegung an Dritte ist nur im Rahmen gesetzlicher Übermittlungsbefugnisse oder mit wirksamer Einwilligung (§ 4 Ziffer 13 KDG, Art. 4 Ziffer 11 DS-GVO) der Betroffenen zulässig (§§ 9 und 10 KDG, Art. 5 BayDSG). Die Regelungen zum Datengeheimnis (§ 5 KDG, Art. 5 BayDSG) zur Wahrung des Betriebs- und Geschäftsgeheimnisses wie zur Verschwiegenheit (ABD, Teil A, § 3 Abs. 1, Art. 12 KiStiftO)

[1] in den Pfarrkirchenstiftungen ist Dienststellenleiter der jeweilige Kirchenverwaltungsvorstand/Pfarrer

finden auch beim Einsatz privater Rechner uneingeschränkt Anwendung[2].

4 .) Die Daten sind passwortgeschützt abzuspeichern. Zudem sind Sicherungsmaßnahmen zu ergreifen, um einen Zugriff auf die Daten über das Internet zu verhindern. Als Mindestschutzmaßnahmen gelten aktivierte Firewall sowie Sicherheitssoftware mit je aktuellen Signaturen und Updates.

5 .) Bei Wartungsarbeiten am privaten Rechner durch externe Firmen oder bei Neu-/Ersatzbeschaffung des Rechners ist sicherzustellen, dass vor Beginn der Wartungsarbeiten bzw. Weitergabe des Rechners alle gespeicherten Daten sicher gelöscht wurden[3].

6 .) Es ist geeignete Vorsorge zu treffen (regelmäßiges Daten-Back- Up auf passwortgesichertem, externem Speichermedium), dass alle gespeicherten Daten auch bei einem Ausfall des Rechners jederzeit zur Verfügung stehen.

7 .) Bei Verlust, Diebstahl oder Zerstörung des Rechners ist unverzüglich die verantwortliche Stelle in Kenntnis zu setzen.

8 .) Bei Beendigung des Dienst-/Beschäftigungsverhältnisses oder auf jederzeitiges Verlangen der verantwortlichen Stelle sind die gespeicherten Daten herauszugeben und dann unverzüglich sicher vom Rechner zur löschen[4]. Die sichere Löschung der Daten ist der verantwortlichen Stelle mittels einer Versicherung an Eides statt zu belegen (Anlage - Muster).

9 .) Bei Schülerinnen und Schülern dürfen deren personenbezogene Daten lediglich dann verarbeitet werden, wenn sie von der bearbeitenden Lehrkraft selbst unterrichtet werden.

9.1) Art und Umfang der zur Bearbeitung auf privaten Rechnern zulässigen Daten von Schülerinnen und Schülern, die nicht überschritten werden dürfen:

- **Personenbezogene Daten der Schülerin oder des Schülers:**
  Familienname, Namensbestandteile, Vorname(n), Rufname, Geschlecht, Geburtsdatum, Geburtsort, Anschrift, Telefonnummer, E-Mail Adresse.
- **Aktuelle Unterrichtsdaten der Schülerin oder des Schülers:**
  Klasse, Klassenart, Unterrichtsart, Schule, Schulart, Jahrgangsstufe, Ausbildungsrichtung/Fachgruppe/Wahlpflichtfächergruppe, besuchter Religions-/Ethikunterricht, Fremdsprachen, Wahlpflichtfächer, Wahlunterricht/ Förderunterricht/ Pluskurse/Arbeitsgemeinschaften, differenzierter Sport einschließlich Sportart, Berufsfeld, Erfüllung der Schulpflicht.
- **Leistungsdaten:**
  Note, Art, Gewichtung, Datum der Leistungsbewertung, Zeugnisbemerkungen, (unentschuldigte) Versäumnisse, Erreichen des Klassenziels.
- **Austritt:**
  Ergänzungsprüfung, Prüfungsende, Eignung für weiterführende Schule, Austrittsdatum, Abschluss.
- **Schuldaten:** Schulart, Schulnummer, amtliche Bezeichnung, Anschrift, Telefonnummer, E-Mail Adresse, Schuljahr, Zeugnisdatum, (Amtsbezeichnung der) Unterzeichnenden, Vorsitz, Klassenleitung.
- **Personenbezogene Daten der Lehrkraft:**

---

[2] die gesetzlichen Grundlagen, Ordnung für kirchliche Stiftungen (KiStiftO) sowie das Gesetz über den kirchlichen Datenschutz (KDG)) mit Ausführungsbestimmungen, sind im Amtsblatt der Diözese Augsburg veröffentlicht.

[3] z.B. mittels qualifizierter Löschsoftware (Software-Überschreibung [wiping Programme]) oder Formatierung der Datenträger auf niedriger Stufe (low level formatting).

[4] siehe Fußnote 3

Familienname, Namensbestandteile, Vorname(n), Rufname, Geschlecht, Amtsbezeichnung.

- **Unterrichtselemente:**
  Information, welche Lehrkraft welche Schülerinnen und Schüler in welchen Fächern unterrichtet; Berücksichtigung der besonderen Gewichtung bei einzelnen Schülerinnen und Schülern (insbesondere wegen Legasthenie).

9.2) Schülerdaten dürfen nur für die Dauer des laufenden Schuljahres bzw. für den jeweiligen Zeugnistermin gespeichert werden und sind anschließend sicher zu löschen.

9.3) Schülerdaten dürfen Dritten nicht zugänglich gemacht werden. Eine Datenübermittlung/Offenlegung an Dritte ist nicht zulässig.

10 .) Diese „erläuternden Hinweise treten zum 1. Mai 2019 in Kraft. Zugleich treten die „Richtlinien zur Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) - KDO- DVO, IV. Anlage 2 zu § 6 KDO, Ziffer 5.1 –„, veröffentlicht in Amtsblatt für die Diözese Augsburg 2017, Nr. 11 vom 07. November 2017, außer Kraft.

Anlage - Muster –

Versicherung an Eides Statt

Ich,_____
_

(Vorname, Name, Anschrift)

versichere durch meine Unterschrift, dass ich sämtliche mir von der verantwortlichen Stelle oder Dritten zu Verarbeitung überlassene dienstliche Software und überlassenen dienstlichen Daten sowie sämtliche von mir erstellten dienstlichen Daten nebst aller Sicherungskopien und Backups unwiederbringlich von meinem Rechner und allen externen Speichermedien gelöscht habe. Ich versichere gleichzeitig, dass ich alle in meinem Besitz befindlichen Ausdrucke aller Art von dienstlichen Daten datenschutzgerecht vernichtet habe.

Ich versichere an Eides Statt, dass ich die vorgenannten Angaben nach bestem Wissen und Gewissen gemacht habe, dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe.

Die Strafbarkeit einer falschen eidesstattlichen Versicherung ist mir bekannt, namentlich die Strafandrohung gemäß § 156 StGB bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei vorsätzlicher Begehung der Tat bzw. gemäß § 163 Abs.1 StGB bis zu einem Jahr Freiheitsstrafe oder Geldstrafe bei fahrlässiger Begehung.

(Ort, Datum, Unterschrift)