

Evangelische Kirche Berlin-Brandenburg-schlesische Oberlausitz
Konsistorium Postfach 35 09 54 10218 Berlin

Konsistorium

An die Kirchengemeinden
und die Kirchenkreise
in der EKBO

Dr. Uta Kleine
Oberkonsistorialrätin

nachrichtlich

- an die Kirchlichen Verwaltungsämter
in der EKBO
- an den Kirchlichen Rechnungshof der
EKBO
- an den Beauftragten für den
Datenschutz der EKD, Außenstelle
Berlin

Georgenkirchstraße 69
10249 Berlin
Telefon 030 2 43 44 – 279
Fax 030 2 43 44 – 241
u.kleine@ekbo.de
www.ekbo.de

Gz. Referat 1.2
Az. 1626-03:00

Berlin, den 16. Mai 2018

Erforderliches nach dem neuen Datenschutzgesetz der EKD

Sehr geehrte Damen und Herren,
liebe Brüder und Schwestern,

am 24. Mai 2018 tritt das durch die Synode der EKD im Herbst 2017 geänderte Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) in Kraft (Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) vom 15. November 2017 (ABl. EKD S. 353), abrufbar unter <https://www.kirchenrecht-ekd.de/document/39740>).

Die Überarbeitung des DSG-EKD war geboten, weil es in Einklang mit der ab 25. Mai 2018 geltenden EU-Datenschutz-Grundverordnung (DSGVO) zu bringen war. Wesentliche Grundsätze des alten Rechts gelten nach dem neuen Recht fort.

Die stärksten Veränderungen betreffen den technischen und organisatorischen Datenschutz. Rechenschafts- und Meldepflichten, Pflichten zur Führung bestimmter Verzeichnisse nehmen großen Raum ein.

Wir haben in der Anlage eine Übersicht zusammengestellt mit den Dingen, die für Sie als Kirchengemeinde und Kirchenkreis besonders relevant sind und haben diese dort, wo es sinnvoll erschien, um Hinweise ergänzt. Bitte werden Sie im Hinblick auf die Umsetzung der für Sie erforderlichen genannten Dinge tätig.

Eine große Hilfe dabei ist eine örtlich Beauftragte oder ein örtlich Beauftragter für den Datenschutz, zu dessen Bestellung Sie gemäß § 36 Abs. 1 Satz 1 DSG-EKD verpflichtet sind, wenn bei Ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind. Die Zehn-Personen-Grenze ist eine „Kopfzahl“, unabhängig davon, ob Vollzeit, Teilzeit, haupt- oder ehrenamtlich mit den personenbezogenen Daten gearbeitet wird. Die Bestellung kann sich auf mehrere verantwortliche Stellen, also mehrere Kirchengemeinden bzw. zusätzlich auch auf den Kirchenkreis erstrecken (§ 36 Abs. 2 Satz 1 DSG-EKD). Die oder der örtlich Beauftragte für den Datenschutz wird Kontakt zur Aufsichtsbehörde des Beauftragten, Außenstelle Berlin, für den Datenschutz der EKD haben und auch von dort beraten und geschult werden.

Bitte beachten Sie, dass Sie als Leitung für die Erfüllung der Verpflichtungen des DSGVO-EKD verantwortlich sind. Dies gilt unabhängig davon, ob Sie verpflichtet sind, eine oder einen örtlich Beauftragten für den Datenschutz zu bestellen (vgl. §§ 36, 37 DSGVO-EKD). Die Voraussetzungen und Erfordernisse zur Bestellung haben wir Ihnen mit Rundschreiben vom 27.2.2014 bzw. auch vom 26.3.2015 mitgeteilt.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung:

- zu Fragen des rechtlichen Datenschutzes: Frau Dr. Kleine, u.kleine@ekbo.de, Tel.: -279
- zu Fragen des technischen Datenschutzes: Herr Kraetschmer, f.kraetschmer@ekbo.de, Tel: -329
- zu Fragen des organisatorischen Datenschutzes: Herr Kellner, j.kellner@ekbo.de, Tel.: -510

Mit freundlichen Grüßen,

Im Auftrag
Dr. Uta Kleine

Übersicht über Erforderliches für die Kirchengemeinden und Kirchenkreise
nach dem neuen Datenschutzgesetz der EKD (Stand: 16.05.2018)

Lfd. Nr.	Erforderliches	Hinweise
1.	Behandlung des Schreibens des Konsistoriums vom 24.4.2018 im GKR bzw. KKR	
2.	Erstellen und regelmäßiges Aktualisieren eines Datenschutzkonzeptes inkl. technischer und organisatorischer Maßnahmen (TOM) zum Nachweis der Einhaltung der Grundsätze, nach denen personenbezogene Daten zu verarbeiten sind (§ 5 Abs. 2 DSGVO-EKD)	Gemäß § 5 Abs. 2 DSGVO-EKD muss die verantwortliche Stelle die Einhaltung der Grundsätze [der Verarbeitung personenbezogener Daten, § 5 Abs. 1 DSGVO-EKD] nachweisen können (Rechenschaftspflicht). Dazu, wie dieser Nachweis erbracht werden soll, ist nichts gesagt. Daher ist davon auszugehen, dass spezifische Anforderungen hierzu bisher nicht bestehen und dieser Pflicht auf vielerlei Weise Rechnung getragen werden kann, beispielsweise durch einschlägige Verwaltungsbestimmungen, Dienstvereinbarungen, Dokumentationen. Hilfreich wird jedoch sein, dies mittelfristig mittels eines Datenschutzkonzeptes nachzuweisen, in dem auch die technischen und organisatorischen Maßnahmen dokumentiert sind (vgl. § 27 DSGVO-EKD).
3.	Führen von Verzeichnissen	
a)	Dokumentation von TOM (technisch organisatorische Maßnahmen), § 27 DSGVO-EKD	<p>§ 27 DSGVO-EKD sieht vor, dass die verantwortliche Stelle unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und einen Nachweis hierüber führen zu können.</p> <p>Diese Maßnahmen schließen unter anderem ein:</p> <ul style="list-style-type: none"> - die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten; - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall unverzüglich wiederherzustellen; - ein Verfahren zur regelmäßigen Über-

		prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
b)	Verzeichnis von Verarbeitungstätigkeiten für die Videoüberwachung, §§ 52, 55 Abs. 4 DSGVO	Gemäß § 55 Abs. 4 Satz 1 DSGVO sind Verzeichnisse im Fall einer Videoüberwachung gemäß § 52 bis zum 24. Mai 2018 zu erstellen.
c)	Dokumentation bei Datenpannen gemäß § 32 Abs. 5 DSGVO	Gemäß § 32 Abs. 5 DSGVO hat die verantwortliche Stelle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.
4.	Informations-/ Meldepflichten	
a)	gegenüber Betroffenen, §§ 17, 18, 19 DSGVO	
b)	Meldepflicht im Fall einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt, an die Aufsichtsbehörde, § 32 Abs. 1 und 2 DSGVO	
c)	Benachrichtigungspflicht im Fall einer Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich ein hohes Risiko für die persönlichen Rechte natürlicher Personen zur Folge hat, gegenüber der betroffenen Person, § 33 DSGVO	
5.	Verwendung von veröffentlichten Mustern für <ul style="list-style-type: none"> - die Verpflichtung auf das Datengeheimnis (vgl. § 26 Satz 2 DSGVO), - Einwilligungserklärungen - Verträge im Hinblick auf die Verarbeitung von personenbezogenen Daten im Auftrag gemäß § 30 DSGVO 	Es ist vorgesehen, diese Muster demnächst vom Konsistorium zu veröffentlichen.
6.	Datenschutz-Folgenabschätzung gemäß § 34 Abs. 1 DSGVO	Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge, so führt die verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (§ 34 Abs. 1 Satz 1 DSGVO).
7.	Datenschutz durch Technikgestaltung	Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rech-
	Festlegung von möglichen Zugriffen auf Email-Konten der Mitarbeitenden	
	Umgang mit gemeinsamen Kalendern	
	Umgang mit der Abwesenheit von Mitarbeitenden	

	Umsetzung von datenschutzgerechten Standards bei Passwörtern	<p>te natürlicher Personen trifft die verantwortliche Stelle sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen, die geeignet sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieses Kirchengesetzes zu genügen und die Rechte der betroffenen Personen zu schützen (§ 28 Abs. 1 DSGVO-EKD).</p> <p>Beispielhaft können hier folgende Maßnahmen genannt werden:</p> <ul style="list-style-type: none"> - Zugriffsverwaltung auf Daten, - Umgang mit gemeinsamen Kalendern und der Abwesenheit von Mitarbeitern, - Umsetzung eines datenschutzgerechten Standards bei Passwörtern, - Einrichtung von Funktions-Email-Adressen. <p>Diese - nicht abschließenden Themen - finden sich im Übrigen im IT-Sicherheitskonzept einer jeden kirchlichen Einrichtung wieder.</p>
	Einrichtung von Funktions-Email-Adressen	
	...	
8.	Bestandsaufnahme/ Prozessbeschreibungen	<p>Für viele der oben genannten Verpflichtungen wird es zunächst sinnvoll sein, eine Bestandsaufnahme der bereits vorhandenen Maßnahmen vorzunehmen. Sodann sollten Prozessbeschreibungen erfolgen, die u.a. die Zuständigkeiten und die zu beteiligenden Personen oder Ausschüsse definieren sowie für die Umsetzung und das notwendige Controlling sorgen.</p>