EVANGELISCHE KIRCHE
Berlin-Brandenburg-schlesische Oberlausitz

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

An die
Kirchlichen Einrichtungen und Werke in
der EKBO

nachrichtlich
an den Kirchlichen Rechnungshof der
EKBO

nachrichtlich
an den Beauftragten für den Datenschutz
der EKD, Außenstelle Berlin

Konsistorium

Dr. Uta Kleine
Oberkonsistorialrätin

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 18. Mai 2018

Erforderliches nach dem neuen Datenschutzgesetz der EKD

Sehr geehrte Damen und Herren,

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, so beispielsweise der Erforderlichkeitsgrundsatz, die Grundsätze zu Datenvermeidung und Datensparsamkeit und Zweckbindung. Den Betroffenenrechten sowie der Transparenz kommt eine besondere Bedeutung zu. Wichtig ist, dass die Verarbeitung personenbezogener Daten zur Erfüllung der Aufgaben der verantwortlichen kirchlichen Stelle nach wie vor möglich ist, wenn sie erforderlich ist.

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 neu und relevant sind und bitten Sie, hier tätig zu werden.

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 dabei auch auf mehrere verantwortliche Stellen erstrecken (§ 36 Abs. 2 Satz 1 DSG-EKD).

Für viele der Dinge, die nunmehr relevant sind, wurden Muster separat erstellt, über die Sie von der oder dem örtlichen Beauftragten informiert werden, die oder der seinerseits in enger Abstimmung mit dem Beauftragten für den Datenschutz der EKD steht.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung und verbleiben
mit freundlichen Grüßen

Im Auftrag
Dr. Uta Kleine

Übersicht über Erforderliches nach dem neuen Datenschutzgesetz der EKD (Stand: 27.4.2018)

Lfd. Nr.	Erforderliches	
1.	Information über das neue Datenschutzgesetz der EKD und dadurch entstehende neue Anforderungen	Leitung und Mitarbeitende, vgl. auch https://datenschutz.ekd.de/infothek/
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 DSG-EKD)	Gemäß § 5 Abs. 2 DSG-EKD muss die verantwortliche Stelle die Einhaltung der Grundsätze [der Verarbeitung personenbezogener Daten, § 5 Abs. 1 DSG-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 tech-nischen und organisatorischen Maßnahmen dokumentiert sind (vgl. § 27 DSG-EKD).
3.	Führen von Verzeichnissen	
a)	Dokumentation von TOM (technisch organisatorische Maßnahmen), § 27 DSG-EKD	§ 27 DSG-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. Diese Maßnahmen schließen unter anderem ein: - 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 Überprüfung,

		Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
b)	Verzeichnis von Verarbeitungstätigkeiten, § 31 DSG-EKD	Vgl. § 31 Abs. 5 DSG-EKD: „Die […] Pflichten gelten nicht für verantwortliche Stellen, die weniger als 250 Beschäftigte haben. Kirchliche Stellen, die weniger als 250 Beschäftigte haben, erstellen Verzeichnisse nach Absatz 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.“
c)	Verzeichnis von Verarbeitungstätigkeiten für die Videoüberwachung, §§ 52, 55 Abs. 4 DSG-EKD	Gemäß § 55 Abs. 4 Satz 1 DSG-EKD sind Verfahrensverzeichnisse im Fall einer Videoüberwachung gemäß § 52 bis zum 24. Mai 2018 zu erstellen.
d)	Dokumentation bei Datenpannen gemäß § 32 Abs. 5 DSG-EKD	Gemäß § 32 Abs. 5 DSG-EKD 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 DSG-EKD	
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 DSG-EKD	
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 DSG-EKD	
5.	Verwendung von veröffentlichten Mustern für - die Verpflichtung auf das Datengeheimnis (vgl. § 26 Satz 2 DSG-EKD), - Einwilligungserklärungen - Verträge im Hinblick auf die Verarbeitung von personenbezogenen Daten im Auftrag gemäß § 30 DSG-EKD.	Es ist vorgesehen, diese Muster demnächst vom Konsistorium zu veröffentlichen.
6.	Datenschutz-Folgenabschätzung gemäß § 34 Abs. 1 DSG-EKD	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 personenbe-

		zogener Daten durch (§ 34 Abs. 1 Satz 1 DSG-EKD).
7.	Datenschutz durch Technikgestaltung (sollte auch Inhalt des IT-Sicherheitskonzepts sein)	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 Rechte 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 DSG-EKD). Beispielhaft können hier folgende Maßnahmen genannt werden: - Zugriffsverwaltung auf Daten, - Umgang mit gemeinsamen Kalendern und der Abwesenheit von Mitarbeitenden, - Umsetzung eines datenschutzgerechten Standards bei Passwörtern, - Einrichtung von Funktions-Email-Adressen. Diese - nicht abschließenden Themen - finden sich im Übrigen im IT-Sicherheitskonzept einer jeden kirchlichen Einrichtung wieder.
	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	
	Einrichtung von Funktions-Email-Adressen	
	Bestellung einer oder eines IT-Sicherheitsbeauftragten	
	…	
8.	Bestandsaufnahme und Prozessbeschreibungen	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.