



Überblick zu den Datenschutz-Maßnahmen in Einrichtungen

Anforderungen des neuen Kirchlichen Datenschutzgesetzrechtes (KDG)

verantwortlich:

Heinrich Griep

Justitiar des Caritasverbandes für die Diözese Mainz e.V.

Stand: Mai 2018

Inhaltsverzeichnis

A) Betriebsinterne Organisationsmaßnahmen	2
Organisation, Arbeitsabläufe und Technik.....	2
Dokumentationspflichten.....	3
Meldepflichten gegenüber der Datenschutzaufsicht.....	3
B) Betroffene Personen (Einrichtungsnutzer und Klienten).....	4
Prozesse betreffend die Beziehung zu Einrichtungsnutzern/Klienten.....	4
Betroffenen-Informationspflichten (§ 14 KDG).....	4
Anlassbezogene Betroffenen-Mitteilungspflichten.....	5
C) Auftragsverarbeiter (Datendienstleister).....	5
Prozesse betreffend die Auftragsverarbeiter.....	5
D) Prioritäre Maßnahmen	6

A) Betriebsinterne Organisationsmaßnahmen

Organisation, Arbeitsabläufe und Technik

Stichwort	notwendig für	Maßnahme	durchführungsverantwortliche Person
betrieblicher Datenschutzbeauftragten (§ 36 KDG)	Einrichtungsträger/ Organisationen <ul style="list-style-type: none"> mit mindestens 10 Personen in der ständigen Verarbeitung personenbezogener Daten oder Kerntätigkeit liegt in Verarbeitungsvorgängen oder Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) 	Beauftragung eines geeigneten Mitarbeiters oder Beauftragung eines geeigneten externen Datenschutz-Dienstleisters	Verantwortlicher ¹ <ul style="list-style-type: none"> Einstellung oder Beauftragung eines Mitarbeiters oder Dienstleistungsvertrag mit externem Datenschutz-Dienstleister
Verzeichnis der Verarbeitungstätigkeiten (§ 31 KDG)	Einrichtungsträger/ Organisation, wenn sie personenbezogene Daten verarbeiten	Erstellung des Verzeichnisses	Verantwortlicher unterstützt durch betriebl. Datenschutzbeauftragten
Datenschutz-Folgenabschätzung (§ 35 KDG)	Einrichtungen und Organisationen, wenn sie personenbezogene Daten verarbeiten, bei denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bestehen	Durchführung der Folgenabschätzung unter Beteiligung des betrieblichen Datenschutzbeauftragten (§ 35 Abs. 2 KDG)	
Technik + Organisation (§§ 26 – 30 KDG)	Einrichtungsträger/ Organisation, wenn sie personenbezogene Daten verarbeiten	<ul style="list-style-type: none"> Anpassung der Technik und Organisation an Vorgaben des neuen KDG organisatorische Sicherstellung der Melde-, Konsultations- und Dokumentationspflichten² datenschutzfreundliche Voreinstellungen der verwendeten Datenverarbeitungsprogramme und -geräte sicherstellen (§ 7 und § 27 KDG) interne Datenschutzregelungen und Dienstanweisungen³ 	
Schulungen zum neuen Recht	Mitarbeiterinnen + Mitarbeiter, die mit Datenverarbeitung beschäftigt sind	Durchführung von Schulungen	Fobi-Veranstalter ⁴

¹ Geschäftsführungsorgan des Einrichtungsträgers oder der Organisation (Vorstand, Geschäftsführung)

² z.B. durch Dienstanweisungen, verbindliche hausinterne EDV-Ordnung

³ z.B. keine dienstliche Nutzung von Whatsapp

⁴ oder betrieblicher Datenschutzbeauftragter

Dokumentationspflichten

Stichwort	dokumentationspflichtige Daten	durchführungsverantwortliche Person
Datenschutzverpflichtung (§ 5 S.2 KDG)	der mit der Verarbeitung personenbezogener Daten beauftragten Beschäftigten der Einrichtung/Organisation	Verantwortlicher unterstützt durch betrieblichen Datenschutzbeauftragten
Einwilligung (§ 8 KDG)	Einwilligung der von der Verarbeitung der personenbezogenen Personen ⁵ in die Datenverarbeitung	
Verarbeitungsverzeichnis (§ 31 KDG)	Verzeichnis aller Verarbeitungstätigkeiten betreffend personenbezogene Daten in der Zuständigkeit der Einrichtung/Organisation	
Datenschutz-Folgenabschätzung (§ 35 KDG)	personenbezogene Daten der betroffenen Personen ⁶ , deren Verarbeitung einem hohen Risiko der Verletzung von Rechten und Freiheiten ausgesetzt sind (Fallbeispiele in § 35 Abs.4 KDG)	
Datenschutzverletzungen (§ 33 Abs.5 KDG)	Verletzungen des Schutzes personenbezogener Daten, einschließlich aller damit im Zusammenhang stehenden Tatsachen	
Betrieblicher Datenschutzbeauftragter (§ 36 Abs.4 KDG)	Bekanntmachung des betrieblichen Datenschutzbeauftragten	

Meldepflichten gegenüber der Datenschutzaufsicht

Stichwort	Meldepflichtige Tatsachen	durchführungsverantwortliche Person
Verletzung des Datenschutzes (§ 33 Abs.1 KDG)	Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt	Verantwortlicher
betrieblicher Datenschutzbeauftragter (§ 36 Abs.4 S.2 KDG)	Benennung des betrieblichen Datenschutzbeauftragten	

⁵ Einrichtungsnutzer, Klienten

⁶ Einrichtungsnutzer, Klienten

B) Betroffene Personen (Einrichtungsnutzer und Klienten)

Prozesse betreffend die Beziehung zu Einrichtungsnutzern/Klienten

Stichwort	notwendig, wenn	Maßnahme	Durchführungsverantwortung
Einwilligungserklärungen	Einrichtung oder Organisation personenbezogene Daten verarbeitet	Einwilligungserklärungen den Anforderungen nach § 8 KDG anpassen	Verantwortlicher
Verträge mit Einrichtungsnutzern und Klienten ⁷	soweit schriftliche Verträge verwendet werden oder verwendet werden müssen ⁸	Die Verträge sind den Vorgaben des KDG entsprechend anzupassen (siehe z.B. unten Informationspflichten)	

Betroffenen-Informationspflichten (§ 14 KDG)

Stichwort	informationspflichtige Tatsachen		Durchführungsverantwortliche Person
bei der unmittelbaren Erhebung der Daten ⁹ (§ 15 KDG)	<ul style="list-style-type: none"> • Kontaktdaten • Zwecke der Datenverarbeitung • Empfänger der Daten • Speicherdauer • Widerruf der Einwilligung • Beschwerderecht 	z.B. Abschluss von Einrichtungsverträgen (Heimvertrag, Pflegevertrag), Erhebung von Klientendaten beim Beginn eines Beratungsprozesses, Erhebung von Daten persönlicher Mitglieder oder Ehrenamtlicher eines Vereins, Spenderdaten, Internetseite, Beschäftigtendaten	Verantwortlicher
bei der mittelbaren Erhebung der Daten ¹⁰ (§ 16 KDG)	zusätzlich zu den Informationen nach § 15 Abs.1 KDG <ul style="list-style-type: none"> • erhobene Daten • Quelle der Daten 		
für die Ausübung der Rechte der betroffenen Person bei der unmittelbaren und mittelbaren Datenverarbeitung (§ 14 KDG)	<ul style="list-style-type: none"> • Auskunftsrechte (§ 17 KDG) • Recht auf Berichtigung (§ 18 KDG) • Recht auf Löschung (§ 19 KDG) • Recht auf Einschränkung der Verarbeitung (20 KDG) • Recht auf Löschung (§ 19 KDG) • Mitteilungspflichten zur Berichtigung oder Löschung (§ 21 KDG) • Widerspruchsrecht (§ 23 KDG) 		

⁷ Krankenhaus, Pflegeheim, Sozialstation, Kindergarten, Hospiz etc.

⁸ In Pflegeheimen und Pflegediensten sind schriftliche Verträge vom Gesetz vorgeschrieben (§ 6 Abs.1 WBG, § 120 Abs.2 SGB XI)

⁹ z.B. Aufnahme in Einrichtung, Beginn des Beratungsprozesses, aber auch beim Internet-Auftritt, wenn dort personenbezogene Daten erhoben werden (z.B. elektronische Spenden)

¹⁰ d.h. die Daten des Betroffenen werden bei einem Dritten erhoben

Anlassbezogene Betroffenen-Mitteilungspflichten

Stichwort	informationspflichtige Tatsachen	Durchführungsver- antwortliche Person
Berichtigung + Löschung von Daten	Mitteilung der Berichtigung oder Löschung personenbezogener Daten (§ 21 KDG)	Verantwortlicher
Zweckänderung der Datenverarbeitung	Soweit die Datenverarbeitung für einen geänderten Zweck nicht durch Rechtsnormen erlaubt wird, ist eine neue Einwilligung des Betroffenen erforderlich (§ 5 Abs.2 KDG)	
Datenschutz- verletzung	Im Fall einer Datenschutzverletzung ist die betroffene Person zu benachrichtigen (§ 34 KDG)	

C) Auftragsverarbeiter (Datendienstleister)**Prozesse betreffend die Auftragsverarbeiter**

Stichwort	Notwendigkeit	Maßnahme	Durchführungsver- antwortung
Auswahl	Die personenbezogene Daten verarbeitende Einrichtung/Organisation darf nur geeignete Auftragsverarbeiter iSd § 29 KDG auswählen	Auswahlentscheidung des Verantwortlichen	Verantwortlicher
Dienstleistungs- verträge (§§ 29 ff KDG)	Notwendig bei allen Auftragsverarbeitern, die personenbezogene Daten im Auftrag der Einrichtung/Organisation verarbeiten	Anpassung der Verträge an das neue Recht (§ 29 Abs.3 KDG)	Verantwortlicher (i.d.R wird ein professioneller Auftragsverarbeiter von sich aus einen angepassten Vertrag anbieten, der dann aber noch zu prüfen ist)
u.a. ergänzungs- bedürftige Inhalte des Vertrages	Weisungsrecht des Verantwortlichen (§ 29 Abs.4a) KDG		
	Auftragsverarbeiter hat Verzeichnis seiner Verarbeitungstätigkeiten zu erstellen (§ 31 KDG)		
	Unterstützung bei der Ausübung der Betroffenen-Rechte beim Verantwortlichen (§ 29 Abs.4 e) und f) KDG)		
	Genehmigungsvorbehalt bei Weitergabe der Aufträge an Dritte (§ 29 Abs.2 KDG)		
	Weitergabe vertragliche Verpflichtungen an Sub-Auftragsverarbeiter (§ 29 Abs.5 KDG)		
	Tansparenz-Pflichten (§ 29 Abs.4 h) KDG)		
Ausschluss der Datenverarbeitung außerhalb der EU (§ 29 Abs.6 KDG)			

D) Prioritäre Maßnahmen

Folgende der vorgenannten Maßnahmen haben (soweit diese Maßnahmen bisher noch nicht oder nur unzureichend durchgeführt worden sind) Priorität:

Stichwort	Maßnahme	Anmerkungen
Verarbeitungsverzeichnis (§ 31 KDG)	Erstellung eines Verzeichnisses aller Verarbeitungstätigkeiten betreffend personenbezogene Daten in der Zuständigkeit der Einrichtung/Organisation	Dies gewährt den Überblick über alle Aufgabenfelder der Implementierung des neuen Datenschutzrechts und bietet die Grundlage für die Priorisierung der Maßnahmen!
betrieblicher Datenschutzbeauftragter (§ 36 KDG)	Bestellung eines betrieblichen Datenschutzbeauftragten, soweit Voraussetzungen nach § 36 Abs.2 KDG vorliegen	Der betriebliche Datenschutzbeauftragte soll eine wichtige Stütze bei allen Maßnahmen der Umsetzung des neuen Datenschutzrechts sein!
Informationspflichten auf der Internetseite (§§ 14 – 16 KDG)	Auf der Internetseite unter der Überschrift „Datenschutz“ sind Funktionen der Internetseite zu beschreiben, bei denen vom Nutzer der Internetseite personenbezogene Daten erhoben werden.	Internetseiten können u.U. durch automatische Verfahren im Hinblick auf die Anwendung des neuen Rechts auf besonders einfache Weise geprüft werden!

Mainz, den 22.05.2018

Heinrich Griep
Justitiar