

Anhang zur Ersten Änderung der Verwaltungsvorschrift gemäß § 11 IT-Gesetz EKvW des Landeskirchenamtes der Evangelischen Kirche von Westfalen

Stand: 13. September 2022



Muster

Datenklassifizierung der EKvW

	Öffentlich	Vertraulich	Streng vertraulich	Streng geheim
		<div style="border: 1px solid black; padding: 2px;"> Extern Intern </div>		
Beschreibung	<ul style="list-style-type: none"> Informationen werden nicht verschlüsselt, enthalten keine vertraulichen Angaben und sind für den externen oder internen Gebrauch freigegeben. Personenbezogene Daten, die die betroffenen Personen frei zugänglich gemacht haben. 	<ul style="list-style-type: none"> Enthalten vertrauliche Informationen deren Veröffentlichung schutzwürdige Interessen verletzen würde. Personenbezogene Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber die betroffenen Personen nicht frei zugänglich gemacht haben. 	<ul style="list-style-type: none"> Enthalten vertrauliche Informationen, deren Veröffentlichung schutzwürdige Interessen erheblich verletzen würde. Personenbezogene Daten, deren unsachgemäße Handhabung eine betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“). 	<ul style="list-style-type: none"> Enthalten vertrauliche Informationen deren Veröffentlichung schutzwürdige Interessen in einem nicht vertretbaren Ausmaß verletzen könnte. Personenbezogene Daten, deren unsachgemäße Handhabung eine betroffene Person in ihrer gesellschaftlichen Stellung, in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“) o. Gesundheit, Leben oder Freiheit der betroffenen Person beeinträchtigen könnte.
Beispiele	Finale Publikationen (Broschüren, Plakate, Stellenausschreibungen, Newsletter, dienstliche Telefonnummern o. E-Mail-Adressen, etc.)	Intern: Geburtstagslisten, Dienstpläne, Stundenzettel, Einkommensverhältnisse, Sozialleistungen, Publikationen in Vorbereitung, Infos zu Veranstaltungen, Dienstvereinbarungen, Raumbelungspläne, Übersicht der Dienstfahrzeuge, Rundschreiben Extern: Austausch von personenbezogenen Daten z.B. mit Behörden	Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen o. die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten u. Daten zum Sexualleben o. der sexuellen Orientierung einer natürlichen Person (besondere personenbezogene Daten), Meldewesendaten, Schulden und Pfändungen, dienstliche Beurteilungen o. Zielvereinbarungsgespräche, Insolvenzen, RMG, Entwicklungsdokumentation, etc.	Verhandlungen mit Ministerien, Informationen aus Seelsorgegesprächen oder im Zusammenhang mit einem Kirchenasyl, Daten zu Straftaten, zu erzieherischen Maßnahmen, Pflegedaten, Daten von Berufsheimnisträgern gemäß §203 StGB, z.B. in Psychologische/Sucht-Beratungsstellen oder Schwangerschaftsberatungen, Meldewesendaten mit kommunalem Sperrvermerk, etc.
Schutzmaßnahmen	Kein Schutz	Alle vertraulichen Daten werden automatisch verschlüsselt und sind EKvW intern lesbar. Die Berechtigungsvergabe für Externe ist individuell. Das Versenden von internen Informationen an Externe wird unterbunden	Alle streng vertraulichen Daten werden automatisch verschlüsselt und sind EKvW intern lesbar. Das Versenden an Externe wird unterbunden. In den Dokumenten wird automatisch ein Wasserzeichen platziert.	Alle streng geheimen Daten werden automatisch verschlüsselt. Die Berechtigungsvergabe ist individuell und kann nur vom Ersteller verändert werden. Das Versenden an externe wird unterbunden. In den Dokumenten wird automatisch ein Wasserzeichen platziert. Die Verschlüsselung wird mit der höchsten Sicherheitsstufe durchgeführt. Die Daten sind nur über ein internes Netzwerk erreichbar.

Wir klassifizieren unsere Dokumente und schützen damit den Zugriff auf unsere Daten effektiv und effizient und sichern so das Vertrauen in die EKvW!