Verzeichnis von Verarbeitungstätigkeiten

eines Verantwortlichen gemäß § 31 Abs.1 KDG

Erstellungsdatum: _____

Version: _____

A. Vorblatt (nur einmal auszufüllen, gilt für alle Verarbeitungen)

A.1 Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person / juristische Person / Behörde / Einrichtung

Name
Anschrift
Telefon, Email-Adresse

Sollten im Sinne des § 28 mehrere Verantwortliche gemeinsam für die Verarbeitung verantwortlich sein, sind alle gemeinsam Verantwortlichen zu benennen.

A.2 Angaben zum gesetzlichen Vertreter (Leitung) des Verantwortlichen

Name, Funktion
Anschrift
Telefon, Email-Adresse

A.3 Angaben zur Person des Datenschutzbeauftragten

Bei externen Datenschutzbeauftragten auch Angaben zum beauftragten Unternehmen

Name
Anschrift
Telefon, Email-Adresse

B. Beschreibung der Verarbeitung

(pro Verfahren auszufüllen)

Laufende Nr.	
Stand	
Version	

B.1 Bezeichnung

Bezeichnung der Verarbeitung
Ggf. Einführungszeitpunkt (wenn bekannt)

B.2 Fachliche Zuständigkeit

Fachabteilung, Ansprechpartner, Funktion
Kontaktdaten

B.3 Verarbeitungsablauf

Kurze Beschreibung der Verarbeitung (operativ) mit den wichtigsten Prozessschritten. Evtl. Verweis auf bestehende Dokumentation/Prozessbeschreibung o.ä. ☐ **Dokumentation ist als Anlage beigefügt**

B.4 Zwecke der Verarbeitung

Zweckbestimmung	
Rechtsgrundlage	
+ kirchliche oder staatliche Rechtsvorschrift	☐Welche?
+ Erlaubnistatbestand des KDG	
- **Vertrag oder Vertragsanbahnung mit dem Betroffenen**	☐Bitte näher bezeichnen

- **Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen**	☐ Welche?
- **Schutz lebenswichtiger Interessen der betroffenen Person**	☐ Welche?
- **Wahrnehmung einer Aufgabe im kirchlichen Interesse**	☐ Welche?
- **Interessensabwägung**	☐Bitte näher beschreiben ☐**Dokumentation ist als Anlage beigefügt**
+ Einwilligung des Betroffenen	☐ In welcher Form? ☐**Muster ist als Anlage beigefügt**

B.5 Kreis der Betroffenen

Kategorien betroffener Personen

z.B. Beschäftigte, Patienten, Angehörige, Interessenten, Kunden, Vertragspartner, Besucher, Lieferanten, Passanten

Sind Jugendliche oder Kinder betroffen? Wenn ja, welche Besonderheiten werden im Verfahren berücksichtigt?

Bitte erläutern!

Dient das Verfahren einem „Profiling“ (d.h. einer automatisierten Bewertung persönlicher Aspekte, insbesondere um z.B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit oder Bewegungsprofile zu analysieren und vorherzusagen)?

Bitte erläutern!

B.6 Datenkategorien,Datenherkunft und Löschfristen

Kategorien der verarbeiteten personenbezogenen Daten

Persönliche Daten:

☐ **Name/Vorname/Anrede/Titel**
☐ **Adresse**
☐ **Kontaktdaten (Tel. Fax, E-Mail)**
☐ **Geburtsdatum**
☐ **Fotos**
☐ **Interessen/Präferenzen**

Abrechnungsdaten:

☐ **Zahlungsdaten**
☐ **Bankverbindungsdaten/Kreditkartendaten**
☐ **Bonitätsdaten**

☐ **Gesundheitsdaten**

Personaldaten:

☐ **Lebenslauf**

☐ **Zeiterfassungsdaten**

☐ **Lohn-und Gehaltsdaten**

☐ **Qualifikationsdaten/Leistungs- und/oder Potenzialbeurteilung**

☐ **Sozialversicherungsdaten**

☐ **Vertragsdaten**

☐ **IT-Nutzungsdaten (Log Daten/Protokolldateien, IP-Adresse...)**

☐ **Standortdaten**

☐ **Sonstige:**

Besondere Kategorien personenbezogener Daten (siehe § 4 Abs. 2 KDG)

Werden besondere Kategorien personenbezogener Daten verarbeitet?
Wenn ja, welche?

☐ **Es werden keine Daten aus besonderen Kategorien personenbezogener Daten verarbeitet.**

☐ **Es werden Daten aus besonderen Kategorien personenbezogener Daten verarbeitet, und zwar:**

Definition und Zuordnung von Datenschutzklassen

Welchen Datenschutzklassen gemäß KDO-DVO werden die Datenkategorien (einschließlich der besonderen Kategorien) zugeordnet?

Datenherkunft nach §§ 15 und 16 KDG

Wie und durch wen werden die Daten unmittelbar oder mittelbar erhoben?

Fristen für die Löschung je Datenkategorie

Erfüllung der Informationspflichtennach § 15 bzw. 16 KDG

Wie werden die Informationspflichten gegenüber dem Betroffenen erfüllt?

☐ **Muster ist als Anlage beigefügt**

B.7 Auftragsverarbeitung

Kurzbeschreibung

Welche Verfahrensschritte werden durch einen Auftragnehmer bearbeitet?

☐ **Keine**

☐ **Die folgenden:**

Auftragnehmer (Name und Kontaktdaten) ☐ **Verzeichnis des Verfahrens nach § 31 Abs. 2 KDG (des Auftragsverarbeiters) ist als Anlage beigefügt**

Diese Angaben für jeden Auftragsverarbeiter im Verfahren einzeln machen!

B.8 Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden

☐ **intern (Zugriffsberechtigte)** **(Abteilung, Funktion)**
☐ **extern** **Empfängerkategorie** **(Kategorien oder konkret), inkl. Empfänger in Drittländern und internationale Organisationen**
☐ **Drittland oder internationale Organisation (Kategorie)**

B.9 Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

☐ **Datenübermittlung findet nicht statt.** ☐ **Datenübermittlung findet wie folgt statt:**
Nennung der konkreten Datenempfänger:
Dokumentation der geeigneten Garantien ☐ **Dokumentation ist beigefügt**

B.10 Rollenkonzept bei der Verarbeitung

Eingerichtete Rollen von Verarbeitern / Kategorien von Zugriffsberechtigungen

☐ **siehe Anlagen**

B.11 Hardware

Eingesetzte Hardware-Kategorien (Arbeitsplatz-PC, mobile Endgeräte, Server) und mitgeltende Benutzungsanweisungen

☐ **siehe Anlagen**

B.12 Software

Eingesetzte System- und Anwendungssoftware, Bezeichnung und Version (wenn relevant)

☐ **siehe Anlagen**

B.13 Ergebnis der Datenschutz-Folgenabschätzung (§ 35 KDG)

☐ **Eine Datenschutz-Folgenabschätzung nach § 35 KDG wurde durchgeführt.**

☐ **Das Verfahren wurde vor Inkrafttreten des KDG eingeführt, deshalb wurde keine Datenschutz-Folgenabschätzung, sondern eine Vorabkontrolle durchgeführt.**

☐ **Es wurde weder eine Datenschutz-Folgenabschätzung noch eine Vorabkontrolle durchgeführt.**

Bitte Erläutern!

☐ **Die Ergebnisdokumentation ist beigefügt.**

B.14 Technische und organisatorische Maßnahmengemäß § 26 KDG

B.14.1 Allgemein (unternehmensweit) gültige technische und organisatorische Maßnahmen

(Hier kann ein Verweis auf ein mitgeltendes Dokument, d.h. eineübergreifende TOM-Beschreibung stehen, die für mehrere/alle Verfahren der Einrichtung gilt)

z.B. Angaben zu

- physikalischem Schutz: Zutrittskontrolle, Zugangskontrolle im Rechenzentrum
- organisatorischem Schutz: Zugriffskontrolle, Eingabekontrolle, Weitergabekontrolle, Auftragskontrolle; Trennungsgebot für alle Verfahren der Einrichtung
- technischem Schutz: Verfügbarkeits- und Backup-Konzept, Wiederherstellungskonzept (Desaster-Recovery) auf Datenbank-Ebene

☐ **Referenzierte Dokumente sind als Anlage beigefügt.**

B.14.2 Spezielle technische und organisatorische Maßnahmen für das spezifische Verfahren, die über die allgemeinen Maßnahmen hinausgehen

Hier können spezielle Maßnahmen benannt werden, die für das Verfahren eingerichtet werden. Die folgende Liste ermöglicht die Zuordnung der Maßnahmen zu den Kategorien des § 26 Abs. 1 KDG und der Anlage 1 zum § 6 KDO. In der Regel werden nicht zu allen Kategorien spezielle Maßnahmen benannt werden.

Pseudonymisierung, Anonymisierung und Verschlüsselung	Welche Maßnahmen werden getroffen? Warum wurde so entschieden? (z.B. unter Berücksichtigung der verarbeiteten Daten-Kategorien bzw. Datenschutzklassen)
Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	Welche besonderen Maßnahmen wurden getroffen? (z.B. wenn besondere Kategorien personenbezogener Daten verarbeitet werden)
Wiederherstellung	Wie wird die verlustfreie Wiederherstellung nach technischen Störungen oder

	Cyberattacken sichergestellt?
Überprüfung, Bewertung und Evaluierung	Wie wird sichergestellt, dass die Sicherheitsmaßnahmen ständig auf Wirksamkeit überprüft und dem Stand der Technik und einer geänderten Bedrohungslage angepasst werden?
Zutrittskontrolle	Welche besonderen, über die allgemeinen Regelungen hinausgehenden Maßnahmen wurden getroffen? (z.B., wenn die Verarbeitung an besonderen Orten erfolgt)
Zugangskontrolle	Wie wird die unbefugte Nutzung der spezifischen Datenverarbeitungsanlage verhindert oder aufgedeckt? (z.B. besondere zusätzliche Identifizierung durch Token oder Passwörter, evtl. in Kombination. Protokollierung des Systemzugangs etc.)
Zugriffskontrolle	Welche besonderen Regeln zum Umgang mit Datenträgern wurden aufgestellt? Wie wird die Einhaltung kontrolliert? Sind die Daten auf den Datenträgern verschlüsselt?
Weitergabekontrolle	Wie ist die Durchführung der Datenübertragung an Dritte bzw. der notwendigen Datenübermittlung an Auftragnehmer geregelt? Gibt es eine Data Loss Prevention (DLP) Policy, die den unberechtigten Abfluss von Daten verhindert oder erschwert? Werden Daten auf dem Transportweg verschlüsselt?
Eingabekontrolle	Wie wird durchgängig nachvollziehbar, ob und von wem Daten eingegeben, verändert oder entfernt wurden? (Gibt es beispielsweise eine Protokollierung?)
Auftragskontrolle	Existieren für alle Auftragsverarbeitungen ausreichende und geprüfte Verträge? Wie werden die Auftragnehmer kontrolliert?

Trennungsgebot	Wie wird sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden? Gibt es eine Mandantentrennung (logisch über Mandantenkennzeichen, physikalisch in getrennten Datenbanken und per Zugriffssteuerung mittels verschiedener Berechtigungen). Ist ein getrennter Testdatenbestand vorgesehen?

…… …… ……

Verantwortlicher Datum Unterschrift