Formulierungshilfe

Verzeichnis von Verarbeitungstätigkeiten

nach dem Gesetz über den kirchlichen Datenschutz (KDG)

Stand 05/2018

Katholisches Datenschutzzentrum

Inhalt

Formulierungshilfe

Verzeichnis von Verarbeitungstätigkeiten

Herausgegeben vom Katholischen Datenschutzzentrum

So erreichen Sie uns:

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Diese Formulierungshilfe des Katholischen Datenschutzzentrums der nordrhein-westfälischen (Erz-)Diözesen (KDSZ) dient als Orientierungshilfe. Die konkrete Ausgestaltung ist an den jeweiligen Sachverhalt anzupassen und sollte daher Schritt für Schritt für den konkreten Anwendungsfall erstellt werden. Dieses Dokument kann dies vereinfachen, aber nicht ersetzen. Diese Formulierungshilfe stellt keine zivilrechtliche Beratung durch das KDSZ und keine Standardvertragsklauseln im Sinne von § 29 Abs. 8 KDG bzw. Art. 28 Abs. 8 DS-GVO dar. Insbesondere ist durch das KDSZ keine Prüfung nach den §§ 307ff. BGB vorgenommen worden.

Revision 2.0 / 09.07.2018

Verzeichnis von Verarbeitungstätigkeiten

Informationen vorab zu dieser Formulierungshilfe

§ 31 KDG verpflichtet den Verantwortlichen, ein Verzeichnis von Verarbeitungstätigkeiten zu führen und dieses dem betrieblichen Datenschutzbeauftragten und auf Anfrage der Datenschutzaufsicht zur Verfügung zu stellen.

Das Katholische Datenschutzzentrum hat ein Muster für ein solches Verzeichnis erstellt, welches inhaltlich über die Minimalanforderungen des § 31 Abs. 1 KDG hinausgeht und so den Verantwortlichen ermöglicht, eine aussagekräftige Übersicht ihrer Verarbeitungstätigkeiten zu erstellen, die auch über die Zwecke des KDG hinaus verwendet werden kann. Das Muster steht als Word-Format in der Infothek des KDSZ zum Download bereit und kann von jedem Verantwortlichen leicht auf die lokalen Erfordernisse angepasst werden.

Die dazu gehörende Anleitung zum Ausfüllen ist auch Bestandteil dieser Formulierungshilfe. Sie erläutert alle Felder des Verzeichnisses und gibt Hinweise auf den Zweck der Angaben.

Im ersten Teil ab Seite 4 dieser Formulierungshilfe ist das Musterverzeichnis abgedruckt, im zweiten Teil finden Sie die Anleitung zum Ausfüllen mit weiteren Erläuterungen.

Formulierungshilfe

Katholisches Datenschutzzentrum

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

Formulierungshilfe

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

Formulierungshilfe

- **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**

Formulierungshilfe

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 Informationspflichten nach § 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 Maßnahmen gemäß § 26 KDG

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

(Hier kann ein Verweis auf ein mitgeltendes Dokument, d.h. eine übergreifende 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

Zweiter Teil

Hinweise zum Ausfüllen und weitere Erläuterungen

A.1 Name, Anschrift und Telefon-/E-Mail-Angaben (optional) des Verantwortlichen.
Der Verantwortliche ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. (§ 4 Abs. 9 KDG). Hier ist die offizielle Bezeichnung unverändert und ungekürzt zu verwenden.

A.2 Angaben zum gesetzlichen Vertreter des Verantwortlichen.
Falls der Verantwortliche keine natürliche Person ist, ist hier (mindestens) eine natürliche Person zu benennen, die den Verantwortlichen gesetzlich vertreten kann. Gibt es Regelungen, dass nur mehrere natürliche Personen zusammen den Verantwortlichen vertreten können, ist darauf hinzuweisen und es ist (mindestens) eine Kombination von natürlichen Personen zu benennen, die zusammen die Vertretungsvollmacht innehaben.

A.3 Angaben zur Person des Datenschutzbeauftragten.
Angaben zum vom Verantwortlichen bestellten Datenschutzbeauftragten. Im Falle einer externen Beauftragung soll zur Erleichterung der Kontaktaufnahme auch das den Datenschutzbeauftragten stellende Unternehmen/Büro benannt werden.

B Beschreibung der Verarbeitung.
Jede Verarbeitung erhält eine Nummerierung nach einer logischen Systematik. Über den Stand (Datum) der Beschreibung wird die Versionierung des Dokumentes unterstützt.

B.1 Bezeichnung.
Jede Verarbeitung erhält eine im Verantwortungsbereich des Verantwortlichen eindeutige Bezeichnung,

B.2 Fachliche Zuständigkeit.
Angaben, wer die fachliche Verantwortung für Spezifikation, Betrieb und Weiterentwicklung des Verfahrens trägt. I.d.R. ist das **nicht** die IT-Abteilung!

B.3 Verarbeitungsablauf.
Eine (kurze) Beschreibung des operativen Ablaufs der Verarbeitung mitihren wichtigsten Schritten. Dabei ist auf unterschiedliche Rollen und ihre Berechtigungen einzuge-hen (siehe auch B.10). Hier kann z.B. auch ein Flussdiagramm oder eine andere Form der Prozess-Vi-sualisierung eingesetzt werden oder ein Verweis auf

eine schon vorhandene IT- oder Prozessdoku-mentation.

B.4 Zwecke der Verarbeitung.

Nach § 6 Abs. 1 KDG ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn mindestens eine der abschließend aufgezählten Bedingungen erfüllt sind. Die zutreffende Bedingung ist in der Verfahrensbeschreibung anzugeben und ggf. näher zu beschreiben.

B.5 Kreis der Betroffenen.

Hier sind die von der Verarbeitung personenbezogener Daten in diesem speziellen Verfahren betroffenen Personen nach ihrer Kategorie aufzuführen. Falls erforderlich ist kurz zu erläutern, wodurch genau die genannten Personenkategorien betroffen werden. Besonders ist die evtl. Betroffenheit von Jugendlichen und Kindern zu prüfen und darzustellen, da in diesen Fällen besondere Regeln für die Einholung einer wirksamen Einwilligung (§ 8 Abs. 8 KDG) und die Erfüllung von Informations-, Auskunfts- und sonstigen Rechten unter Einbeziehung der Personensorgeberechtigten beachtet werden müssen. Auch wenn das Verfahren einem Profiling dient, sind nach § 24 KDG besondere Betroffenenrechte zu beachten, weshalb dieses Verfahrensmerkmal in der Beschreibung dokumentiert werden soll.

B.6 Datenkategorien, Datenherkunft und Löschfristen.

Die im Verfahren verarbeiteten personenbezogenen Daten sind nach ihrer Art in Kategorien zusammenzufassen, zu denen dann Informationen über die Datenherkunft (z.B. Erhebungsart) und Löschfristen abgelegt werden. Je genauer diese Angaben zum Verfahren gemacht werden, desto leichter lassen sich später z.B. Auskunftsbegehren der Betroffenen erfüllen und die ordnungsgemäße Datenverarbeitung z.B. hinsichtlich der regelmäßigen Löschung überprüfen.

B.7 Auftragsverarbeitung.

Falls ein oder mehrere Schritte des Verfahrens durch einen Auftragnehmer in Auftragsverarbeitung durchgeführt werden, sind der oder die Schritte und der jeweilige Auftragsverarbeiter zu benennen. Weiterhin ist für jeden externen Verfahrensschritt das vom Auftragsverarbeiter nach § 31 Abs. 2 KDG zur Verfügung zu stellenden Verarbeitungsverzeichnis für diesen Verfahrensschritt beizufügen.

B.8 Kategorien von Empfängern der Daten.

Hier sind alle internen und/oder externen Kategorien von Empfängern der personenbezogenen Daten zu benennen. Empfänger sind im Gegensatz zu Auftragsverarbeitern solche natürlichen oder juristischen Personen, die die Daten zu einer eigenverantwortlichen Verarbeitung erhalten. Empfänger in Drittländern bzw. in-

ternationale Organisationen, bei denen eine Verarbeitung in einem Drittland nicht ausgeschlossen werden kann, sind besonders aufzuführen.

B.9 Übermittlung in Drittländer oder an internationale Organisationen.
Falls solche Übermittlungen stattfinden, sind sie hier besonders zu beschreiben.

B.10 Rollenkonzept.
Hier werden die Grundzüge des Berechtigungskonzeptes beschrieben.

B.11 Hardware.
Die eingesetzte Hardware und ihre Architektur werden auf konzeptioneller Ebene beschrieben.

B.12 Software.
Bezeichnung der eingesetzten System- und Anwendungssoftware, z.B. Betriebssysteme und Standardsoftware

B.13 Ergebnis der Datenschutz-Folgenabschätzung.
§ 35 KDG beschreibt die Kriterien, nach denen die Notwendigkeit einer Datenschutz-Folgenabschätzung vor Einführung des Verfahrens beurteilt werden muss, wie bei einer solchen Datenschutz-Folgenabschätzung vorzugehen und in welcher Weise das Ergebnis zu dokumentieren ist. Die vorgenommenen Erwägungen und – falls durchgeführt – die Dokumentation der Datenschutz-Folgenabschätzung sind hier (ggf. als Verweis auf ein externes Dokument) einzufügen.

B.14 Technische und organisatorische Maßnahmen

B.14.1 Allgemein gültige technische und organisatorische Maßnahmen.
Für alle oder mehrere Verfahren gültige Maßnahmen, die z.B. im Rahmen der Organisation des Rechenzentrums oder einer zentralen Datenerfassung geregelt wurden.

B14.2 Spezielle technische und organisatorische Maßnahmen.
Besondere, nur für das konkret beschriebene Verfahren gültige Maßnahmen, die über die allgemeinen Maßnahmen hinausgehen, diese (teilweise) invalidieren oder konkretisieren. Die aufgeführten Maßnahmenkategorien dienen als Anhaltspunkte für eine vollständige Beschreibung der Organisation des Verfahrens.

Katholisches
Datenschutzzentrum