Katholisches Datenschutzzentrum

Hinweise zum Ablauf von Prüfungen durch das Katholische Datenschutzzentrum

Vorbemerkung

Das Katholische Datenschutzzentrum überzeugt sich auch durch Kontrollen vor Ort vom Stand der Umsetzung des Datenschutzes in den kirchlichen Einrichtungen. Diese Prüfungen können auf Grund einer Beschwerde (anlassbezogen) oder anlasslos zum Beispiel zur Evaluierung des grundsätzlichen Umsetzungsstandes des Datenschutzes in dem Einrichtungstyp angesetzt werden.

Der typische Ablauf einer solchen Prüfung gestaltet sich wie folgt:

1. Information an die Einrichtung

Vier bis sechs Wochen vor dem geplanten Prüfungstermin wird die Einrichtung mit einem Schreiben über die bevorstehende Prüfung informiert. In dem Schreiben werden Unterlagen angefordert, um die Vorbereitung des Katholischen Datenschutzzentrums auf die Gegebenheiten der speziellen Einrichtung zu erleichtern. Eventuelle Wünsche für Terminänderungen sollten frühzeitig mit dem Katholischen Datenschutzzentrum abgesprochen werden.
Innerhalb einer Woche nach Versand des Anschreibens wird eine Terminbestätigung telefonisch bei der Einrichtung eingeholt. Dabei werden auch erste Fragen zum Ablauf und zu den angeforderten Unterlagen geklärt.

2. Welche Unterlagen werden typischerweise angefordert?

Damit das Katholische Datenschutzzentrum sich bezüglich der Verarbeitung der personenbezogenen Daten auf die konkrete Situation vor Ort bestmöglich vorbereiten kann, werden in der Regel folgende Unterlagen von der Einrichtung erbeten:

- Verzeichnis von Verarbeitungstätigkeiten
  Das Verzeichnis nach § 31 KDG gibt einen Überblick über die Datenverarbeitung der Einrichtung und ist eines der zentralen Dokumentationspapiere.
- Auflistung der Verträge mit Auftragsverarbeitung
  Die Auflistung dieser Verträge nach § 29 KDG erlaubt Einblicke in die Struktur der Datenverarbeitung und die Auslagerung einzelner Teile der Verarbeitung auf Dienstleister.
- Konzept und Prozess zu Mitarbeiterschulungen zum Datenschutz
  Übersicht über die Maßnahmen zur Sensibilisierung der Beschäftigten als wichtige Grundlage für die Umsetzung des Datenschutzes vor Ort.
- Musterformulare zu Einwilligungen und Verschwiegenheitserklärungen
  Übersicht über die Muster, die Beschäftigten, Kunden und Vertragspartnern zur Einhaltung datenschutzrechtlicher Vorgaben vorgelegt werden.
- Kontaktdaten des betrieblichen Datenschutzbeauftragten und IT-Sicherheitsbeauftragten
  Klärung der fachlichen Ansprechpartner.
- Datenschutz- oder Qualitätsmanagementhandbuch
  Diese Dokumente geben Einblicke in die Prozesse der Einrichtung.
- IT-Dokumentation
  Die Dokumentation der technischen Systeme und Anwendungen gibt einen Überblick über die IT-Landschaft.
- Prozesslandkarte
  Dieses Dokument zeigt die Prozesse der Verarbeitung der Daten und deren Verbindung untereinander auf.

Sofern die Erstellung der Dokumente nach KDG nicht ohnehin vorgesehen ist, müssen die Papiere (wie z. B. ein Qualitätsmanagementhandbuch oder eine Prozesslandkarte) für die Prüfung nicht extra geschaffen werden. Je nach Gegenstand der Prüfung können weitere Dokumente hinzukommen.

3. Ablauf der Prüfung vor Ort

Die Begehung vor Ort wird in der Regel von zwei Personen des Katholischen Datenschutzzentrums durchgeführt. In einem Einführungsgespräch wird der weitere Ablauf besprochen.
Anhand eines Fragenkatalogs und auf Grundlage der eingereichten Unterlagen wird in einem Gespräch mit der Einrichtungsleitung, dem betrieblichen Datenschutzbeauftragten und weiteren Personen über die allgemeine Umsetzung des Datenschutzes innerhalb der Einrichtung gesprochen. Dabei wird im Rahmen dieses Gespräches eruiert, wie z. B. Mitarbeiterschulungen konzipiert und durchgeführt werden, wie die Benennung des betrieblichen Datenschutzbeauftragten umgesetzt wurde, welche Auftragsverarbeitungen in den Prozessen der Einrichtung integriert sind oder welche Muster für Einwilligungen vorliegen und wie die Erstellung und Führung der Verarbeitungsverzeichnisse durchgeführt wird.
Nach dem allgemeinen Teil wird in gleicher Weise die Umsetzung der technischen und organisatorischen Maßnahmen nach § 26 KDG evaluiert. Dies schließt auch die Begehung von Teilen der Einrichtung, wie z.B. dem Serverraum oder von Fachabteilungen ein.
Die Prüfung schließt mit einem Abschlussgespräch ab, an dem die Einrichtungsleitung beteiligt sein sollte. Hierbei werden die ersten Ergebnisse vorgetragen und der weitere Ablauf besprochen. So werden auch erste Maßnahmen und eine zeitliche Abfolge vereinbart.

4. Dokumentation der Ergebnisse

Nach dem Vor-Ort-Termin wird ein Bericht durch das Katholische Datenschutzzentrum erstellt.
Der Bericht enthält allgemeine Feststellungen zur geprüften Einrichtung, zum Prüfungsgegenstand und zum Prüfungsumfang. Der Teil des Berichtes, der die eigentlichen Feststellungen der Prüfung enthält, stellt zunächst den festgestellten Sachverhalt zum Tag der Prüfung dar (Ist-Zustand). Zu dieser Darstellung wird die einschlägige datenschutzrechtliche Vorgabe genannt (Soll-Zustand) und die Abweichung von Soll- und Ist-Zustand benannt. Komplettiert wird die Darstellung durch einen Vorschlag zur Behebung der Soll-Ist-Abweichung verbunden mit einer Umsetzungsfrist.
Die im Bericht genannten Fristen zur Bearbeitung der Maßnahmen sowie die Maßnahmen selbst richten sich nach der Kritikalität der gefundenen Sachverhalte und den in der Einrichtung umsetzbaren Möglichkeiten. Der Bericht wird an die geprüfte Stelle versandt.
Nach dem Versand des Prüfberichtes wird die Einrichtung erneut kontaktiert, um den Prüfbericht zu besprechen. Dabei können Fragen geklärt werden und die in dem Prüfbericht aufgeführten Fristen erläutert und eventuell verändert werden.

5. Maßnahmenverfolgung

Innerhalb der vereinbarten Zeiträume trifft die geprüfte Stelle geeignete technische und organisatorische Maßnahmen, um die festgestellten datenschutzrechtlichen Mängel zu beheben. Zum Ende der Frist berichtet die geprüfte Stelle über die getroffenen Maßnahmen und liefert entsprechende Dokumente oder andere Nachweise zu den durchgeführten Änderungen.
Sollten vereinbarte Zeiträume aus nachvollziehbaren Gründen nicht eingehalten werden können, so kann im Einzelfall durch das Katholische Datenschutzzentrum der Zeitraum angepasst werden. Hierzu sollte die geprüfte Stelle rechtzeitig vor Ablauf des Zeitraums Kontakt mit dem Katholischen Datenschutzzentrum aufnehmen. Eine Darstellung der schon ergriffenen Maßnahmen und eine Begründung, welche Teile sich aus welchen Gründen nicht innerhalb des Zeitraums umsetzen lassen, helfen bei der Diskussion über eine Verlängerung des Umsetzungszeitraums.