Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Durchführung einer Vorabkontrolle (Muster)

(MV 604 - Stand: 25. September 2014)

Vorbemerkung:

Die Neufassung der Anordnung über den kirchlichen Datenschutz (KDO) sieht nunmehr nach § 3 Abs. 5 KDO die Durchführung einer Vorabkontrolle für automatisierte Datenverarbeitungen vor, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Diese Voraussetzung ist immer dann gegeben, wenn besondere Arten personenbezogener Daten verarbeitet werden (§ 3 Abs. 5 Nr. 1 KDO) oder die Verarbeitung personenbezogener Daten die Persönlichkeit des Betroffenen bewertet, einschließlich seiner Fähigkeiten, seiner Leistungen oder seines Verhaltens (§ 3 Abs. 5 Nr.2 KDO). Diese Bedingungen sind auch im kirchlichen Bereich häufig erfüllt. So ist zum Beispiel davon auszugehen, dass sämtliche Beratungsstellen im Hinblick auf ihre Verschwiegenheitsverpflichtung nach § 203 StGB ebenso eine Vorabkontrolle durchzuführen haben, wie Krankenhäuser und Institutionen, die Dienstleistungen im Gesundheitsbereich anbieten, wie beispielsweise Pflegestellen oder Therapiestellen. Schulen und Kindergärten gehören sicherlich zu den Institutionen, die die Persönlichkeit ihrer Schüler, einschließlich der Fähigkeiten, Leistungen und des Verhaltens des einzelnen, bewerten müssen. Auch sie sind daher zur Vorabkontrolle bei Einführung automatisierter Datenverarbeitungen verpflichtet.

Zuständig für die Durchführung der Vorabkontrolle ist nach § 3 Abs. 6 KDO der betriebliche Datenschutzbeauftragte. Soweit keiner bestellt worden ist, hat der Diözesandatenschutzbeauftragte die Einführung eines neuen Systems durch sein Mitwirken zu begleiten.

Die Frage wird sich für viele Betriebsbeauftragte stellen, wie eine solche Vorabkontrolle künftig durchzuführen ist. Die hier vorliegende Schrift stellt dafür ein umfassendes Muster zur Verfügung. Es beinhaltet alle Punkte, die im Rahmen einer Vorabkontrolle zu berücksichtigen und zu prüfen sind. Natürlich ist die beschriebene Vorgehensweise nicht verbindlich. Sie stellt eine Empfehlung dar, die man zu Grunde legen oder auch von ihr abweichen kann. Bei der Entscheidung hierüber, sollte sich jeder Dienststellenleiter die Frage stellen:

„Bin ich bereit, eine ordnungsgemäß funktionierende und verlässliche Datenverarbeitung zu installieren oder bevorzuge ich das totale Chaos?“

In dem Fall, dass Sie die Frage mit der ersten Alternative beantworten sollten, ist es mit Nachdruck zu empfehlen, dem Betriebsbeauftragten die Möglichkeit einzuräumen, sich allen Fragen,

die in diesem Muster angesprochen werden, intensiv zuzuwenden. Das gilt auch für die Anmerkungen, die bei vielen Fragestellungen eingefügt worden sind.

Was würde beispielsweise passieren, wenn eine Mitarbeiterin oder ein Mitarbeiter bei den Stammdaten eines Klienten dessen Adresse ändern würde, weil sie von ihm erfahren hat, dass er jetzt nicht mehr bei seinen Eltern zuhause sondern bei seiner Freundin wohnt. Diese Angabe hat Auswirkungen auf andere Bereiche, zum Beispiel auf die Abrechnung der von Ihnen erbrachten Leistungen gegenüber Sozialleistungsträgern. Hier wird dann die neue Anschrift berücksichtigt, die beim Rechnungsempfänger gar nicht bekannt ist. Vielleicht führt es sogar dazu, dass er sich nicht mehr als räumlich zuständig ansieht. Folge ist, dass Ihre Kasse leer bleibt, weil ein Mitarbeiter Änderungen ohne eingehende Nachprüfung vorgenommen hat. Wer in diesem Punkt Chaos verhindern will, gibt klare und nachvollziehbare Anweisungen, wer solche Änderungen vornehmen darf und stellt dies auch technisch sicher. Dies ist nur ein kleines Beispiel für die Schaffung einer ordnungsgemäßen Funktionsweise, die der Einrichtung ebenso nützt wie auch dem Schutz des Persönlichkeitsrechts des Betroffenen.

Datenschutz sieht sich nicht als Verhinderer und Begrenzer von Technik sondern als Begleiter und Helfer bei der Einrichtung ordnungsgemäßer und funktionierender Systeme.

Ich hoffe daher, dass dieses Muster Ihnen hilfreich zur Seite steht.

Hannover, den 25. September 2014

Durchführung einer Vorabkontrolle (Muster)

gemäß § 3 Abs. 5 der Anordnung über den kirchlichen Datenschutz (KDO)

Ziel: Zur Vorabkontrolle gehört zunächst eine Beschreibung des Verfahrens, dessen Einführung geplant ist. Sie ist von der **datenverarbeitenden Stelle** vorzunehmen, um den betrieblichen Datenschutzbeauftragten (künftig „betrDSB“) präzise über das Projekt zu unterrichten.

A. Beschreibung des geplanten Verfahrens

1.	Verantwortliche Stelle[1]:	
2.	Leiter(in) der verantwortlichen Stelle:	
3.	EDV-Verantwortliche(r):	
4.	MAV-Vorsitzende(r)[2]:	
5.	Lieferfirma / Hersteller[3]:	
6.	Name des Verfahrens:	
7.	Einzusetzende Software und dabei verwendete Module[4]:	
8.	Datenverarbeitung erfolgt[5]	☐ intern oder ☐ extern

[1] Zum Begriff siehe die Definition in § 2 Abs. 8 KDO
[2] Nur auszufüllen, wenn ein Mitwirkungsrecht der MAV bei der Einführung des Systems besteht.
[3] Der betrDSB sollte die Möglichkeit haben, sich mit dem Anbieter in Verbindung zu setzen, um einzelne Fragen oder Probleme mit ihm erörtern zu können.
[4] Viele Programme sind heute modular aufgebaut (Stammdaten, Rechnungsdaten, Fallakten, usw.). Für die Vorabprüfung ist es notwendig zu wissen, welche Teile zunächst installiert werden sollen und welche Erweiterungen für die Zukunft noch möglich sind.
[5] Um interne Datenverarbeitung handelt es sich, bei einem System, das allein in der Einrichtung betrieben wird, Server und Arbeitsplatzcomputer also unter alleiniger Kontrolle des Betreibers stehen. Externe Datenverarbeitung liegt dann vor, wenn fremde Server, Speicherplätze und Programmangebote in Anspruch genommen werden (Beispiel: „Cloud Computing“).

9.	Rechtsgrundlage der Datenverarbeitung[6]:	
10.	Von der Datenverarbeitung betroffene Personengruppen:	
11.	Schützenswerte Daten[7]:	
12.	Zweckbestimmung[8]:	
13.	Vorgesehene Übermittlungen an Dritte:	
14.	Zugriffsberechtigte Personengruppen:	
15.	Fristen für die Löschung der Daten[9]:	
	Beigefügte Anlagen: ☐ Abschriften / Kopien der in Bezug genommenen Rechtsgrundlagen ☐ Betriebsvereinbarung ☐ Verfahrensbeschreibungen / Handbücher des Anbieters / Herstellers ☐ Schriftliche Regelungen zur Wartung / Fernwartung ☐ Entwurf eines Vertrages zur Auftragsdatenverarbeitung ☐ Entwurf eines bestehenden Datenschutz- und Datensicherheitskonzepts ☐ Beschreibung der Netzstruktur und der Datenhaltung ☐ Ausfertigung der Anlage zu § 6 KDO (organisatorisch-technische Maßnahmen)	

[6] Eine Datenverarbeitung ist nach § 3 Abs. 1 KDO nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die Betroffenen eingewilligt haben. Es ist daher zwingend notwendig, vor Installation des Systems die Grundlagen hierfür zu klären. Als geeignete Rechtsgrundlagen kommen Gesetze und Verordnungen aber auch (Arbeits-)Verträge und Betriebsvereinbarungen in Betracht. Sollte keine spezielle Rechtsgrundlage bestehen, so ist hier „Einwilligung der Betroffenen“ einzufügen.

[7] Eine Vorabkontrolle ist nach § 3 Abs. 5 KDO nur dann erforderlich, wenn durch die Datenverarbeitung besondere Risiken für die Betroffenen bestehen. Das ist der Fall bei Verarbeitung besonderer Arten personenbezogener Daten (Definition in § 2 Abs. 10 KDO), der Verschwiegenheitspflicht unterliegenden Daten nach § 203 StGB und Daten, die die Persönlichkeit der Betroffenen, ihre Leistungen oder ihr Verhalten bewerten (z.B. Personaldaten, Schülerdaten, etc.). Sie sind daher hier möglichst präzise zu benennen.

[8] Hier sind die Zwecke anzugeben, für die die Daten nach § 10 Abs. 1 KDO erhoben und verarbeitet werden sollen.

[9] Wenn nach Art der verarbeiteten Daten verschiedene Löschungsfristen bestehen, sollte eine gesonderte Aufstellung unter Nennung der Arten der Daten und der für sie jeweils geltenden Löschungsfristen beigefügt werden.

B. Überprüfung der rechtlichen Zulässigkeit der Datenverarbeitung[10]

Ziel: Eine Datenverarbeitung ist nur zulässig, wenn sie den gesetzlichen und sonstigen rechtlichen Anforderungen entspricht oder die Betroffenen eingewilligt haben (§ 3 Abs. 1 KDO). Zu Beginn der Prüfung ist daher zu klären, ob die geplante Maßnahme insoweit auf einem gesicherten ‚Fundament' steht.

1.	Entspricht die Zweckbestimmung der geplanten Datenverarbeitung den Voraussetzungen in der angegebenen Rechtsgrundlage?	☐ ja ☐ nein
2.	Werden nur die in der Rechtsgrundlage genannten Arten personenbezogener Daten erhoben und gespeichert?	☐ ja ☐ nein
3.	Bei einer geplanten Erhebung von besonderen Arten personenbezogener Daten: Liegt eine der Voraussetzungen aus § 9 Abs. 5 KDO vor? Nennen Sie die Gründe aus den Ziff. 1 bis 9, die hier vorliegen:	
4.	Auflistung der Daten, deren Erhebung nicht im Einklang mit § 9 Abs. 5 Nr. 1 – 9 KDO erfolgt und auch nicht in der anzuwendenden Rechtsgrundlage gefordert wird:	
5.	Sind sämtliche Daten im Hinblick auf den Grundsatz der Datenvermeidung und -sparsamkeit (§ 2a KDO) wirklich erforderlich?	☐ ja ☐ nein
6.	Benennung der möglicherweise nicht erforderlichen Daten:	
7.	Sind die gesetzlichen Sperr- und Löschfristen berücksichtigt?	☐ ja ☐ nein
8.	Nennen Sie möglicherweise falsche oder nicht berücksichtigte Sperr- und Löschfristen:	

[10] Die nachfolgenden Abschnitte stellen ein Konzept für die Prüfung des betrDSB dar.

9.	Sind die Zugriffsberechtigungen im Rahmen einer Rechteverwaltung geregelt?	☐ ja ☐ nein
10.	Sind die Zugriffsmöglichkeiten inhaltlich den Aufgaben der jeweiligen Nutzer angepasst?[11]	☐ ja ☐ nein
11.	Erfolgt auch eine Regelung der technischen Zugriffsmöglichkeiten?[12] So zum Beispiel:	
	- für die Neuanlage von Datensätzen	☐ ja ☐ nein
	- für die Gewährung von Leserechten	☐ ja ☐ nein
	- für Bearbeitungs- und Veränderungsmöglichkeiten[13]	☐ ja ☐ nein
	- für die Möglichkeit gespeicherte Daten auszudrucken[14]	☐ ja ☐ nein
	- für den elektronischen Versand von Daten[15]	☐ ja ☐ nein
	- für das Recht Kopien auf andere Datenträger zu fertigen[16]	☐ ja ☐ nein
	- für das Sperren oder Löschen von Dateien[17]	☐ ja ☐ nein
	- für die Archivierung von Altakten	☐ ja ☐ nein
12.	Beschreibung der Kritikpunkte und der damit verbundenen Risiken:	

[11] Es muss eine Übereinstimmung bestehen zwischen den Zugriffsrechten und dem jeweiligen Tätigkeitsprofil der Nutzer.
[12] Eine solche Absicherung dient einer verlässlichen Datenverarbeitung und der Geheimhaltung.
[13] Hier muss darüber nachgedacht werden, ob jeder Nutzer Veränderungen an dem Datenbestand vornehmen kann. Das ist meist wenig angemessen. Bestimmte Aufgaben sollten oder müssen sogar einzelnen Stellen vorbehalten bleiben.
[14] Für sensible Daten und solche, die der Verschwiegenheitspflicht unterliegen ist sicherzustellen, dass nur die Beauftragten und ihre Helfer den Ausdruck von Unterlagen im Rahmen ihrer Berufspflicht veranlassen können.
[15] Hier gilt das Gleiche, wie unter FN 12 ausgeführt.
[16] Hier gilt das Gleiche, wie unter FN 12 ausgeführt.
[17] Das Sperren und Löschen ist nur nach Prüfung der hierfür bestehenden Voraussetzungen zulässig und sollte daher nur von bestimmen Mitarbeitern durchgeführt werden können. So kann eine Klientenakte erst dann von dem Berater gelöscht werden, wenn ihm die Bestätigung der Finanzabteilung über die ordnungsgemäße Abrechnung und Bezahlung vorliegt.

13.	Gibt es eine Regelung zur Übermittlung von Daten an Dritte?[18]	☐ ja ☐ nein
	- Übermittlungsregelung für Auskünfte an Behörden	☐ ja ☐ nein
	- Übermittlungsregelung für andere fachlich beteiligte Stellen	☐ ja ☐ nein
	- Übermittlungsregelung für Auskünfte an Betroffene und	☐ ja ☐ nein
	deren Vertreter (Vormund, Rechtsbeistand, Sorgeberechtigte)	☐ ja ☐ nein
	- Übermittlungsregelung für andere Stellen	☐ ja ☐ nein
14.	Welche Stelle(n) ist (sind) mit der Übermittlung beauftragt?	
15.	Schriftliche Übermittlungsregelungen liegen den betrDSB vor?	☐ ja ☐ nein
16.	Abschließende Bewertung zu Punkt B (Rechtliche Zulässigkeit)	

[18] Soweit Übermittlungsregelungen in schriftlicher Form vorliegen, sollten sie von betrDSB überprüft und zum Prüfungsvorgang genommen werden.

C. Überprüfung der Wahrung der Rechte der Betroffenen[19]

Anwendung der §§ 5, 13, 13a, 14, 15 KDO

Ziel: Bei jeder Verarbeitung personenbezogener Daten steht den Betroffenen eine Reihe von Rechten zu. Die Offenheit Ihnen gegenüber schafft das Vertrauen auf eine korrekte und ihre Interessen wahrende Datenverarbeitung. Das System darf nicht durch technische Gestaltung die Geltendmachung dieser Rechte verhindern oder erschweren.

1.	Besteht die Möglichkeit der Auskunftserteilung über die elektronisch gespeicherten Daten?[20]	☐ ja ☐ nein
2.	Können Berichtigungen auf Verlangen des Betroffenen durchgeführt werden? - § 14 Abs. 1 Satz 1 KDO	☐ ja ☐ nein
3.	Wer ist hierfür zuständig?[21]	
4.	Ermöglicht das System eine Sperrung einzelner Datenfelder?[22]	☐ ja ☐ nein
5.	Wie erfolgt diese?	
6.	Kann eine physikalische Löschung einzelner Daten oder ganzer Akten durchgeführt werden?	☐ ja ☐ nein
7.	Nennen Sie das hierfür zur Verfügung stehende Verfahren/Software:	

[19] Diesem Punkt ist besondere Aufmerksamkeit zu widmen. Jede Datenverarbeitung ist ein Eingriff in das Persönlichkeitsrecht des Betroffenen! Auch wenn die Speicherung und Nutzung dieser Daten rechtmäßig erfolgt, muss der Person die Möglichkeit gegeben sein, zu erfahren, was über ihn gespeichert wird, falsche Informationen berichtigen zu lassen und den Umfang der Speicherung in Frage zu stellen.

[20] Technisch muss die Möglichkeit gegeben sein, sowohl einzelne Dokumente, wie auch ganze Akten auf einen externen Datenträger (Speicherstift, CD) zu übertragen oder für den Mail-Versand in einer ZIP-Datei zum Versand zur Verfügung zu stellen. Das Verfahren hierzu muss in personeller Hinsicht klar geregelt sein.

[21] Die Dienstelle ist auch zur ordnungsgemäßen Speicherung und im Rahmen der Aufbewahrungsfrist zum Erhalt der Daten verpflichtet. Änderungen haben meist in verschiedenen Bereichen Auswirkung. Daher ist eine klare Anweisung nötig, die die Vornahme solcher Berichtigungen vorsieht.

[22] Die Notwendigkeit hierzu ergibt sich in der Regel aus § 14 Abs. 4 KDO. Hier sind einzelne Daten zu sperren, bei denen Streit über deren Richtigkeit/Unrichtigkeit besteht.

8.	Können die Betroffenen ihre Rechte in angemessener und unkomplizierter Weise geltend machen?[23]	☐ ja ☐ nein
9.	Wenn nein, warum nicht?	
10.	Abschließende Bewertung zu Punkt C (Rechte der Betroffenen)	

[23] Kann sich der Betroffene an den betrDSB wenden? Ist dieser innerhalb der Einrichtung bekannt und erreichbar? Sind die Arbeitsstellen über das Verfahren eingehend unterrichtet?

D. Technischer Schutz des Systems

Ziel: Datenschutz durch Technik!

Schaffung von Rahmenbedingungen, die geeignet sind, eine Gefährdung des Systems weitgehend auszuschließen. Aus datenschutzrechtlicher Sicht sind dabei drei Anforderungen zu gewährleisten:

a) Die Vertraulichkeit, die sicherstellt, dass nur autorisierte Personen Zugriff auf die gespeicherten, verarbeiteten und genutzten Daten haben.

b) Die Integrität, die gewährleistet, dass auf einen einheitlichen, zutreffenden Datenbestand Bezug genommen wird.

c) Die Verfügbarkeit, die die notwendige Verwendung und Bearbeitung der Daten jederzeit sicherstellt.

Dabei müssen alle Bereiche der Technikinstallation eingehend geprüft werden.

I. Sicherung der eingesetzten Server[24]

1.	Ist der Serverraum vor unbefugtem Betreten gesichert?[25]	☐ ja ☐ nein
2.	Ist der Serverraum vor Wassereinbrüchen geschützt?[26]	☐ ja ☐ nein
3.	Ist ein ausreichender Feuerschutz installiert?[27]	☐ ja ☐ nein
4.	Besteht eine unterbrechungsfreie Stromversorgung?	☐ ja ☐ nein
5.	Nennen Sie die nach Ihrer Auffassung hier erforderlichen Nachbesserungen:	

[24] Nur auszufüllen, wenn es sich um eigene Server handelt, bei einer Auftragsdatenverarbeitung sind nur die Punkte II und III zu bearbeiten.
[25] Der Serverraum darf nur von hierzu autorisierten Personen betraten werden. Ein unbefugtes Betreten führt zu einer erheblichen Gefahr für den Bestand und die Funktionsfähigkeit der gesamten Anlage. Eine Absicherung muss daher sowohl gegen ein Eindringen von außen, wie auch von inneren Zugängen her gegeben sein.
[26] Hier ist nicht nur die Gefahr von Hochwassereinbrüchen, sondern auch die durch etwa bestehende Wasserleitungen zu berücksichtigen.
[27] Absicherung des Raumes mit feuerfesten Stahltüren, Verzicht auf brennbare Holzteile, Installation eines Rauchmeldesystems, personelle Eingriffsmöglichkeiten.

6.	Gibt es eine regelmäßige laufende Sicherung der Daten?[28]	☐ ja ☐ nein
7.	Auf welchem System erfolgt diese und in welchen zeitlichen Abständen?[29]	
8.	Ist auch eine dauerhafte Sicherung vorgesehen?[30]	☐ ja ☐ nein
9.	Welche zeitlichen Abstände werden bei ihr erfasst? Welche Speichermedien werden hierfür eingesetzt? Wo werden die Datenträger aufbewahrt?	
10.	Besteht eine Vorgabe zur Löschung/Vernichtung einzelner Aufzeichnungen der dauerhaften Sicherung?[31]	☐ ja ☐ nein
11.	Bei Internetzugängen: Ist der Server durch eine Hardware-Firewall gesichert?[32]	☐ ja ☐ nein
12.	Ist zudem ein Viren-Scanner vorhanden?[33]	☐ ja ☐ nein
13.	Besteht eine gerätetechnische Trennung zwischen dem „Terminalserver“ (Verwaltung von Programmen) und dem „Fileserver“ (Verwaltung des Datenbestandes)?	☐ ja ☐ nein
14.	Sind die Daten auf dem Fileserver verschlüsselt?[34]	☐ ja ☐ nein

[28] Bei sensiblen Daten ist eine ausreichende Datensicherung Pflicht! Sie erfolgt meist auf Festplatten, für die die Gefahr besteht, beschädigt zu werden. Daher ist in vielen Fällen eine Sicherung auf mehreren, unabhängigen Platten durch ein RAID-System angezeigt. Wie viele Platten hierbei eingesetzt werden, hängt von der jeweiligen Risikoeinschätzung ab.

[29] Der zeitliche Abstand gibt Auskunft darüber, wie groß der Datenverlust beim Ausfall des Systems sein würde. Er ist so zu wählen, dass die verlorenen Daten in angemessener Zeit durch Neueingabe wiederherstellbar sind.

[30] Unter dauerhafter Sicherung ist die gesamte Aufzeichnung des Datenbestandes zu einem bestimmten Zeitpunkt gemeint, die nicht nachträglich verändert werden kann. So sind auch ältere Datenbestände, die in der laufenden Datensicherung nicht mehr vorhanden sind, wieder herstellbar. Ihre Aufbewahrung sollte außerhalb der EDV-Räume, brand- und diebstalgeschützt erfolgen (Beispiel: Stahltresor).

[31] Aus datenschutzrechtlichen Gründen können diese Sicherungskopien nicht für immer aufbewahrt werden. Sie sind spätestens nach Ablauf der höchsten Aufbewahrungsfrist (30 Jahre), in vielen Fällen aber auch schon früher, physikalisch zu vernichten.

[32] Bei größeren Systemen ist eine ausreichende Sicherheit nicht mit Software-Firewalls möglich. Diese bieten sich nur bei Einzelplatzrechnern und kleineren Netzen an.

[33] Pflichtsoftware für Internetzugänge!

[34] Daten, die der Verschwiegenheitspflicht unterliegen sind auf dem Fileserver zu verschlüsseln, damit nur fachlich zugriffsberechtigte Personen diese lesen und bearbeiten können. Andere Mitarbeiter, die fachlich nicht zuständig sind oder Techniker, die das System verwalten, haben auf diese Daten keinen Zugriff. Einzusetzen ist möglichst eine 256-bit AES-Verschlüsselung.

15.	Welche Software wird hierfür eingesetzt?	
16.	Besteht eine Verschlüsselung für die Datenübertragung vom Arbeitsplatzrechner zum Fileserver?	☐ ja ☐ nein
17.	Welche Software wird hierfür eingesetzt?	
18.	Wie sieht das Gesamtkonzept für die Sicherung des/der Servers aus?	

II. Sicherung der eingesetzten Arbeitsplatzrechner

19.	Werden die Arbeitsplatzcomputer technisch betreut?	☐ ja ☐ nein
20.	Wer ist bei Störungen/Fehlfunktionen der Arbeitsplatzrechner anzusprechen?	
21.	Gibt es einen Systemverwalter im Hause?	☐ ja ☐ nein
22.	Ist beabsichtigt, einen externen Systemverwalter zu bestellen?	☐ ja ☐ nein
23.	Welche Mindestreaktionszeit ist bei Störungen des Systems oder einzelner Teile von ihm zugesichert?	
24.	Wie wird die Durchführung wichtiger Sicherheits-Updates des Betriebssystems gewährleistet?	
25.	Sind die Bildschirme für fremde Personen nicht einsehbar?	☐ ja ☐ nein
26.	Besteht eine Sicherung bei kurzfristigem Verlassen des Arbeitsplatzes?	☐ ja ☐ nein

27.	Kann der Bildschirmschoner gezielt aufgerufen werden?	☐ ja ☐ nein
28.	Ist der Bildschirmschoner nur mit Passwort aufzuheben?	☐ ja ☐ nein
29.	Sind die Arbeitsräume abschließbar?	☐ ja ☐ nein
30.	Arbeiten mehrere Personen in den Arbeitsräumen?	☐ ja ☐ nein
31.	Beurteilen Sie das Gesamtkonzept für die Sicherung der Arbeitsplatzrechner:	
32.	Soll eine Fernwartung für die Nutzung der Software zur Verfügung stehen?	☐ ja ☐ nein
33.	Name des Dienstleisters:	
34.	Unter welchen Bedingungen soll die Fernwartung erfolgen?	
	Erfolgt der Beginn der Fernwartung auf Veranlassung Ihrer Dienststelle und wird die Verbindung zum Dienstleister von Ihnen hergestellt?	☐ ja ☐ nein
	Wird dabei eine verschlüsselte, vertrauliche Verbindung hergestellt?	☐ ja ☐ nein
	Erfolgt ein etwa notwendiger Zugriff auf den Datenbestand nur nach Erlaubnis des eigenen Mitarbeiters?	☐ ja ☐ nein
	Sollen auch Updates der Software auf diese Weise erfolgen?	☐ ja ☐ nein
	Sollen auch Upgrades der Software auf diese Weise erfolgen?	☐ ja ☐ nein
35.	Abschließende Bewertung zu Punkt D (Technischer Schutz des Systems)[35]	

[35] Im Falle einer Auftragsdatenverarbeitung ist Punkt D51 anstelle von D35 auszufüllen.

III. Sicherung der Auftragsdatenverarbeitung

Ziel: Erfüllung der Anforderungen nach § 8 KDO und für den Bereich der Jugendhilfe nach § 80 SGB X

36.	Gegenstand und Dauer des Auftrags (§ 8 Abs. 2 Nr. 1):	
37.	Datenverarbeitende Stelle, Auftragnehmer:	
38.	Gründe, die für die Geeignetheit des Auftragnehmers sprechen (§ 8 Abs. 2 S. 1):	
39.	Liegt ein schriftlicher Nachweis des Auftragnehmers für die getroffenen, technisch-organisatorischen Maßnahmen zum Schutz der Daten vor?[36]	☐ ja ☐ nein
40.	Beauftragtes Rechenzentrum, Unterauftragnehmer[37]:	
41.	Liegt ein schriftlicher Nachweis des Auftragnehmers für die im Rechenzentrum getroffenen, technisch-organisatorischen Maßnahmen zum Schutz der Daten vor?[38]	☐ ja ☐ nein
42.	Wo befindet sich der Server, auf dem Ihre Daten gespeichert werden sollen?	
43.	Bei Auslandsdatenverarbeitung: Handelt es sich um einen sicheren Drittstaat?	☐ ja ☐ nein

[36] Hier ist vor allem die Sicherheit des Rechenzentrums zu belegen.
[37] Wenn der Auftragnehmer ein eigenes Rechenzentrum betreibt und dort die Daten verarbeitet werden, braucht dieser Punkt nicht ausgefüllt zu werden.
[38] siehe Anmerkung Nr. 34

44.	Ist die Einschaltung weiterer Unterauftragnehmer geplant?		☐ ja ☐ nein
45.	Ist die Berechtigung zur Einschaltung von Unterauftragnehmern vertraglich geregelt? (§ 8 Abs. 2 Nr. 6 KDO)		☐ ja ☐ nein
46.	Liegt eine vollständige Beschreibung des vereinbarten technischen Verfahrens vor? (§ 8 Abs. 2 Nr. 2, 3, 4) Diese muss mindestens Ausführungen zu den folgenden Punkten enthalten:		☐ ja ☐ nein
	a)	Speicherung und Verwaltung des Datenbestandes getrennt von anderen Auftraggebern (Mandantenfähigkeit)?	☐ ja ☐ nein
	b)	Verschlüsselung der Daten auf dem Server?[39]	☐ ja ☐ nein
	c)	Passwort zur Entschlüsselung ist nur dem Auftraggeber bekannt, so dass der Auftraggeber keine Einsichtsmöglichkeit hat?[40]	☐ ja ☐ nein
	d)	Bei Erbringung von Arbeiten durch den Auftragnehmer (wie beispielsweise Rechnungserstellung, Zahlungskontrolle, Mahnwesen): Darlegung eines vertraglich garantierten Umfangs eigener Sicherheitsmaßnahmen. - Gezielte Auswahl und Schulung von Mitarbeiterin? - Verpflichtungserklärung (§ 4) der Mitarbeiter liegt vor? - Rechtekonzept für den Zugriff auf Datenbestände? - Betrieblicher Datenschutzbeauftragter wurde bestellt?	☐ ja ☐ nein ☐ ja ☐ nein ☐ ja ☐ nein ☐ ja ☐ nein ☐ ja ☐ nein
	e)	Verbindung zwischen Arbeitsplatzrechner und Server. Sicherung durch verschlüsselte Übertragung?[41]	☐ ja ☐ nein
	f)	Vertragliche Regelung bei Beendigung der Zusammenarbeit: - Rückgabe überlassener Datenträger (§ 8 Abs. 2 Nr. 10)? - Die Übertragung der gespeicherten Daten an eine andere Stelle ist gesichert? - Vollständige Löschung der Daten beim Auftragnehmer?	 ☐ ja ☐ nein ☐ ja ☐ nein ☐ ja ☐ nein
47.	Sind die Weisungsbefugnisse des Auftraggebers vertraglich eindeutig geregelt?		☐ ja ☐ nein

[39] Bei der Vorabkontrolle geht es um besonders schützenswerte Daten! (siehe § 3 Abs. 5 Nr. 1, 2 KDO)

[40] Nur erforderlich, wenn der AN keine eigenen Arbeiten mit den Daten zu erbringen hat (wie z.B. eine „Privatärztliche Verrechnungsstelle“), sondern nur die Speicherlösung und die einzusetzenden Programme zur Verfügung stellt. Bei „Cloud“-Lösungen ist darauf zu achten, dass der Account zur Freigabe der Daten nicht auf dem Rechner des AN gespeichert wird!

[41] Siehe Anm. 36

48.	Sind die Kontrollmöglichkeiten des Auftraggebers vertraglich geregelt? (§ 8 Abs. 2 Nr. 7 KDO) Dabei ist zu berücksichtigen: Ein Recht zur Begehung und Prüfung der Einrichtung durch Mitarbeiter sowie den Diözesandatenschutzbeauftragten?	☐ ja ☐ nein ☐ ja ☐ nein
49.	Pflicht des Auftragnehmers zur Durchführung eigener Kontrollen?	☐ ja ☐ nein
50.	Regelung über die Mitteilung von Verstößen gegen Datenschutzvorschriften oder Weisungen des Auftraggebers?	☐ ja ☐ nein
51.	Abschließende Bewertung zu Punkt D unter Berücksichtigung der geplanten Auftragsdatenverarbeitung	

E. Abschließende Bewertung des Gesamtverfahrens

Ziel: Es muss ein positives Ergebnis der Vorabkontrolle vorliegen!

Alle Ergebnisse, die unter den Punkten B16, C10, D35 und stattdessen gegebenenfalls unter D51 beschrieben worden sind, müssen zu einer Gesamtbewertung des Verfahrens zusammengefasst werden, die eine der Feststellungen rechtfertigt, die unter

einem der Punkte E1- E4 benannt sind. Eine Freigabe des Systems ist nur in den Fällen E1 und E2 möglich. Über diese verbindliche Bewertung hinaus, sollte noch eine schriftliche Begründung vorgenommen werden.

1.	Die Verarbeitung personenbezogener Daten ist in der geplanten Form **zulässig**. Das dabei angewendete Verfahren ist rechtlich zulässig, wahrt die Rechte der Betroffenen und die geplanten Sicherheitsmaßnahmen sind zur Beherrschung der bestehenden Risiken geeignet und angemessen.	☐ ja ☐ nein
2.	Die Verarbeitung personenbezogener Daten ist in der geplanten Form **zulässig**. Das dabei angewendete Verfahren weist nur wenige leichte Mängel auf, die den angestrebten Schutzzweck nicht wesentlich beeinträchtigen.	☐ ja ☐ nein
3.	Die Verarbeitung personenbezogener Daten weist in der geplanten Form eine Reihe von Mängeln auf, deren Schweregrad dazu führt, dass die **Zulässigkeit zum gegenwärtigen Zeitpunkt nicht gegeben** ist. Es besteht jedoch die Möglichkeit diese Mängel durch Nachbesserung des Systems zu beseitigen.	☐ ja ☐ nein
4.	Die Verarbeitung personenbezogener Daten ist in der geplanten Form **unzulässig**. Das Verfahren darf nicht freigeben werden! ☐ Es ist rechtlich nicht zulässig, ☐ verletzt in erheblicher Weise die Rechte der Betroffenen und ☐ die geplanten Sicherheitsmaßnahmen reichen nicht aus, um die bestehenden Risiken in einer angemessenen Form zu beherrschen.	☐ ja ☐ nein

Folgende Mängel des geplanten Verfahrens

liegen der abschließenden Beurteilung zu Grunde: