Nutzungsbedingungen IT-Systeme im Bistum Trier (E-Mail, Cloud-Computing, Intranet, Ingenius, SAP)

1. Geltungsbereich

1.1 Die folgenden NUTZUNGSBEDINGUNGEN regeln die Beziehung zwischen dem Bistum Trier, Mustorstraße 2, 54290 Trier als Anbieter (nachfolgend ANBIETER) der IT-Systeme des Bistums Trier (nachfolgend IT-BISTUM) und den sich registrierenden Nutzerinnen und Nutzern zur Nutzung der IT-BISTUM.

1.2 Diese NUTZUNGSBEDINGUNGEN gelten für alle Nutzerinnen und Nutzer der IT-Systeme im Bistum Trier.
„Interne Nutzerinnen und Nutzer" sind:
Beschäftigte des Bistums Trier im Sinne des § 4 Nr. 24 KDG sowie darüber hinaus auch weitere Beschäftigte mit arbeitsrechtlichen Rechtsverhältnissen zum Bistum Trier. Für sie ist die Nutzung der IT-Systeme des Bistums Trier verpflichtend.
„Externe Nutzerinnen und Nutzer" sind:
Ehrenamtliche Mitarbeiterinnen und Mitarbeiter, Beschäftigte der Kirchengemeinden, Kirchengemeindeverbände und Kirchenstiftungen und weitere Personen, die aufgrund ihrer Tätigkeit für das Bistum Trier und für die Gremien des Bistums Trier einen Zugang zur IT-BISTUM erhalten.
Wenn nur von Nutzerinnen und Nutzern gesprochen wird, sind sowohl die internen als auch die externen Nutzerinnen und Nutzer gemeint.

1.3 Diese NUTZUNGSBEDINGUNGEN gelten für die Dauer der Nutzung der IT-BISTUM.

1.4 Die „Dienstvereinbarung zur Einführung und Anwendung einer Cloud-Computing-Lösung im Rahmen des Einsatzes und der Nutzung privater und dienstlicher Mobilgeräte und privater Endgeräte" findet im Rahmen ihres Geltungsbereichs in der jeweils geltenden Fassung Anwendung.

1.5 Die „Datenschutzerklärung zur Nutzung der IT-BISTUM" gilt gleichermaßen für alle Nutzerinnen und Nutzer.

2. Zweck und Ziele der IT-BISTUM

2.1 Der Zweck der IT-BISTUM ist die Ermöglichung des verwaltungs- und inhaltsbezogenen Arbeitens. Die IT-BISTUM steht den Nutzerinnen und Nutzern ausschließlich als Dienstwerkzeug und/oder zur Erfüllung der kirchlichen Aufgaben zur Verfügung und dient insbesondere dem Austausch von Daten und Dokumenten sowie der internen und externen Kommunikation auf elektronischem Wege.

2.2 Die Verarbeitung von personenbezogenen Daten, die dem Beicht- oder Seelsorgegeheimnis unterliegen, ist in der IT-BISTUM untersagt (vgl. § 14 KDG-DVO).

3. Beantragung eines Zugangs, Prüfung und Anmeldung

3.1 Voraussetzung für die Beantragung eines Zugangs zur IT-BISTUM für interne Nutzerinnen und Nutzer ist die Autorisierung durch den/die Vorgesetzte/n.

3.2 Voraussetzung für die Beantragung eines Zugangs zur IT-BISTUM durch externe Nutzerinnen und Nutzer ist die Autorisierung der Nutzerin/des Nutzers durch „eine/n Weisungsbefugte/n"). Die/der Autorisierende muss interne Nutzerin oder interner Nutzer sein.
Der/die Weisungsbefugte stellt mit seiner/ihrer Unterschrift auf dem Antragsformular fest,

- dass der/die Antragsteller/in mit der Erfüllung kirchlicher Aufgaben beauftragt ist oder kirchliche Aufgaben durch Wahl, Entsendung, Beauftragung oder Einwilligung übernommen hat,
- ob der/die Antragsteller/in zweifelsfrei als solche/r identifiziert wurde,
- dass der/die Antragsteller/in zur Einhaltung des Datengeheimnisses nach §§ 2 und 3 KDG-DVO belehrt und nach § 5 KDG schriftlich verpflichtet wurde (vgl. Arbeitshilfe - Anlage 2)
- dass die Nutzerinnen und Nutzer die Nutzungsbedingungen und die Datenschutzerklärung erhalten und die Nutzungsbedingungen akzeptiert haben. Durch die sich anschließende Anmeldung des/der externen Nutzers/Nutzerin kommt ein Nutzungsvertrag zustande.

3.3 Zur Beantragung sind die realen Klardaten zur Identifizierung des/der Nutzers/in (Vorname, Nachname, Beschäftigungsdienststelle, Personalnummer sowie, sofern Personalnummer nicht vorhanden, Geburtsdatum und Anschrift) erforderlich.
Die Nutzerinnen und Nutzer erklären, dass sämtliche Angaben wahrheitsgemäß sind.

3.4 Mit der Beantragung erklären sich die Nutzerinnen und Nutzer damit einverstanden, dass Name und Vorname sowie E-Mail-Adresse im Nutzerverzeichnis hinterlegt werden. Darüber hinaus werden die persönlichen Angaben nur für die Zwecke der Registrierung gespeichert.

3.5 Zur Beantragung eines Zugangs für eine/n Minderjährige/n im ehrenamtlichen Dienst ist die Einwilligung der Personensorgeberechtigten erforderlich.

3.6 Jede/r Nutzer/in darf nur einen Zugang zur IT-BISTUM beantragen und versichert mit der Beantragung, dass er/sie noch keinen Zugang besitzt bzw. sein/ihr früherer Zugang gelöscht ist.

3.7 Die formale Prüfung des Antrages nimmt der ANBIETER vor. Die Freigabe erfolgt durch den ANBIETER durch die Übersendung der Anmeldedaten/Benutzerkennung und einer personalisierten E-Mail-Adresse.

3.8 Ein Anspruch der Nutzerinnen und Nutzer auf Freigabe besteht nicht. Der ANBIETER kann die Freigabe ablehnen. In diesem Fall werden alle übermittelten Daten der nicht freigeschalteten Nutzerinnen und Nutzer unverzüglich gelöscht.

3.9 Die Nutzerinnen und Nutzer können sich nach der Freigabe in der IT-BISTUM anmelden.
Die Anmeldung zur IT-BISTUM erfolgt durch einen individuellen passwortgeschützten Zugriff.
Bei der ersten Nutzung des Logins muss der/die Nutzer/in sein/ihr Passwort ändern. Benutzerkennung und Passwort dürfen nicht identisch sein. Für ein starkes Passwort braucht es mind. 10 Stellen. Es enthält Groß- und Kleinbuchstaben, mind. zwei Zahlen und mind. ein Sonderzeichen. Passwörter werden kryptographisch gespeichert, so dass niemand das Passwort im Klartext einsehen kann.

3.10 Der ANBIETER kann für den/die Nutzer/in das Passwort zurücksetzen.

3.11 Der Zugriff auf die verschiedenen Systeme der IT-BISTUM erfolgt in abgestufter Form nach dem Rollen-/Berechtigungskonzept in der jeweils aktuellen Fassung. Rollen und Berechtigungen werden durch die Administration im Generalvikariat grundsätzlich nur auf der Grundlage schriftlicher Anträge zugeteilt. Verantwortlich für die Beantragung/Veränderung/Löschung von Rollen und Berechtigungen ist der/die jeweilige Vorgesetzte bzw. der/die Weisungsbefugte. Im Falle des Wechsels eines/einer Vorgesetzten bzw. eines/einer Weisungsbefugten übernimmt der/die Nachfolger/in die Aufgaben. Dies geschieht durch Hinweis an die ausführende Stelle des Anbieters, den ZB 2.7 im Bischöflichen Generalvikariat. Für den Fall, dass die Stelle nicht oder noch nicht nachbesetzt ist, gelten die jeweils aktuell zu fassenden besonderen Vertretungsregelungen. Hierzu stehen den Verantwortlichen/Weisungsbefugten Antragsformulare und jeweils dazu korrespondierende Anleitungen, in welcher Weise die Zugangsberechtigungen zu überprüfen und ggf. anzupassen sind, tagesaktuell im Portal zur Verfügung. (derzeit zu finden unter: >Arbeitsplatz>Bibliothek>Dokumente-Verzeichnis>Informationssysteme).

3.12 Es werden den Vorgesetzten und Weisungsbefugten zur Erfüllung ihrer Aufgaben Arbeitshilfen zur Verfügung gestellt. (vgl. hierzu Pkt. 3.11 Antragsformulare und korrespondierende Anleitungen)

4. Verantwortung und Pflichten der Nutzerinnen und Nutzer

4.1 Sämtliche Daten/Dateien, die Nutzerinnen und Nutzer bei der Nutzung der IT- BISTUM in Umlauf bringen, unterliegen deren alleiniger Verantwortung. Sie erklären sich ausdrücklich damit einverstanden, keine Daten (Texte,

Bilder, Videos, Tonaufnahmen oder Links) einzustellen, die gegen geltendes Recht verstoßen (KDG, UrhG, MarkenG, Grundrechte, etc.). Das Setzen von Hyperlinks auf Webseiten mit illegalen Inhalten ist verboten. Insbesondere vor der Veröffentlichung von Bilddateien (z.B. im Intranet) wird sich jede/r Nutzer/in vergewissern, dass ihm/ihr die Nutzungsrechte hieran zustehen und eine Nutzung nicht gegen Rechte Dritter verstößt.

4.2 Es ist untersagt, ohne Zustimmung des/r Rechteinhabers/in oder einer sonstigen Berechtigung Inhalte zu kopieren, zu verbreiten oder anderweitig öffentlich zugänglich zu machen.

4.3 Die Nutzerinnen und Nutzer pflegen einen höflichen und respektvollen Umgang. Das Suggerieren einer fiktiven Identität ist genauso untersagt wie das Einstellen oder Verbreiten diffamierender, rassistischer, betrügerischer, jugendgefährdender oder sexistischer Inhalte.

4.4 Sämtliche Nachrichten, die Nutzerinnen und Nutzer über die IT-BISTUM versenden, dürfen lediglich aus zweckgerichtetem Interesse an einer kirchlich-gemeinnützigen Tätigkeit heraus erfolgen; ein unsachliches Bewerben von Produkten oder Dienstleistungen ist ausdrücklich untersagt.

4.5 Die Nutzerinnen und Nutzer sind zum vertraulichen Umgang mit sämtlichen Nachrichten und Informationen verpflichtet, die sie/er über die IT-BISTUM erhalten. Speziell sei an dieser Stelle auf die unbedingte Wahrung des Brief- und Telekommunikationsgeheimnisses für systeminterne Nachrichten hingewiesen. Unbeteiligten Dritten dürfen diese Nachrichten oder Teile davon ohne Erlaubnis des/r Absenders/in nicht zugänglich gemacht werden. Selbstverständlich gilt dies auch für übersandtes Bildmaterial, private Daten etc. Vor Aufzeichnungen von Sprach- und Videochats ist die Einwilligung der Beteiligten einzuholen. Die nicht zweckgebundene Nutzung der Daten durch maschinelle oder manuelle Auswertung, Abspeicherung, Editierung etc. ist nicht gestattet. Die Verwendung der personenbezogenen Daten über die Zweckerfüllung und die gültigen Aufbewahrungsfristen hinaus verstößt gegen geltendes Recht.

4.6 Der/die Nutzer/in ist nicht berechtigt, unerwünschte kommerzielle Massen-E-Mails zu erstellen oder bereitzustellen. Die vorsätzliche Verbreitung von Viren, Würmern, trojanischen Pferden, beschädigten Dateien, Viren-Falschmeldungen (sog. Hoaxes) und anderen zerstörerischen oder betrügerischen Elementen ist verboten.

4.7 Die Nutzerinnen und Nutzer sind nicht berechtigt, Änderungen oder Deaktivierungen an der IT-BISTUM vorzunehmen oder Komponenten der IT-BISTUM zu umgehen. Es ist nicht gestattet, die IT-BISTUM nachzukonstruieren, um Beschränkungen und Sicherheitslücken zu ermitteln oder Filterfunktionen zu umgehen.

4.8 Verlassen Inhalte oder Dateien die IT-BISTUM (Entnahme und Speicherung von Dokumenten auf Endgeräten oder Datenträgern, Versand von Mails an Empfänger/innen außerhalb der IT-BISTUM) liegt die Verantwortung für die Einhaltung aller einschlägigen Vorgaben und Gesetze allein beim/bei der Nutzer/in. VDI Arbeitsplätze sind hiervon nicht betroffen.

4.9 Außerhalb des geschützten Netzwerkes werden Daten der Datenschutzklasse II und III (vgl. §§ 12 und 13 KDG-DVO), mit einer aktiven Verschlüsselung versendet. Hierzu beachtet der Nutzer/ die Nutzerin nach erfolgter Anmeldung die Hinweise im Portal unter dem Ordner Datenschutz. Innerhalb des Cloud-Computings stellen die Nutzerinnen und Nutzer im geschützten Netzwerk der IT-BISTUM die Daten dem/der Empfänger/in als Link oder über die Freigabe eines Ablageordners zur Verfügung.

4.10 Die Einrichtung einer automatischen Weiterleitung von dienstlichen Mails an Mailkonten außerhalb der BGV- bzw. Bistums-Domain (= Internetadresse) ist untersagt.

4.11 Der/die Nutzer/in verpflichtet sich, seine/ihre Zugangsdaten zur IT-BISTUM vertraulich zu behandeln und nicht an Dritte weiterzugeben. Es wird darauf hingewiesen, dass der ANBIETER den/die Nutzer/in niemals nach einem Passwort fragen wird. Sollten Anhaltspunkte dafür bestehen, dass die Zugangsdaten von Dritten verwendet werden, wird der/die Nutzer/in den ANBIETER hierüber unverzüglich informieren. Sollte der ANBIETER von einer unzulässigen Weitergabe Kenntnis erlangen, wird er den Zugang umgehend sperren.

4.12 Sollten die Nutzerinnen und Nutzer auf freiwilliger Basis mehr Daten angeben als notwendig, so verpflichten sich die Nutzerinnen und Nutzer, wahrheitsgemäße Angaben zu machen, dies gilt auch für Fotos des/der Nutzers/in selbst.

4.13 Einen Verstoß gegen vorstehende Pflichten (4.1-4.12) meldet der/die Nutzer/in über die Funktionsadresse: problemanzeige@bgv-trier.de zur Einleitung notwendiger Maßnahmen und zur Dokumentation.

4.14 Vor einer planbaren Abwesenheit (z.B. Urlaub) richtet der/die interne Nutzer/in eine automatische Mail/Abwesenheitsnachricht ein, sofern möglich mit Vertretungshinweis und der Auskunft, dass die Mail nicht automatisch an die jeweilige Vertretung weitergeleitet wird. Die Einrichtung und Nutzung einer Funktionsmailadresse trägt dazu bei, dass ein reibungsloser Betrieb gewährleistet werden kann.

4.15 Vor dem planbaren Ausscheiden einer/s internen Nutzerin und Nutzers sind laufende Vorgänge und wichtige dienstliche Inhalte an den jeweiligen Arbeitsbereich abzugeben.

4.16 Es werden unterstützende Maßnahmen zur Einweisung, Direkthilfe und Klärung von Problemanzeigen der IT-Systeme des Bistums Trier vorgehalten.

5. Rechte des Anbieters

5.1 Der Nutzer/die Nutzerin räumt dem ANBIETER mit Einstellen seiner Inhalte in die IT-BISTUM das Recht ein, diese Inhalte in Bezug auf alle Nutzungsarten, dienstlich zu verwenden. Der ANBIETER ist insbesondere berechtigt, die Inhalte dauerhaft in der IT-BISTUM zu speichern.

5.2 Der ANBIETER behält sich das Recht vor z. B. anlassbezogen (vgl. hierzu auch 4.13 und 10.2), die von Nutzerinnen und Nutzern eingestellten Informationen und Dateien dahingehend zu überprüfen, ob obige Pflichten eingehalten wurden.
Sollte eine solche Prüfung negativ ausfallen, so wird der/die Nutzer/in vom ANBIETER auf die Pflichtverletzung hingewiesen und unter Fristsetzung zur Korrektur bzw. Löschung aufgefordert. In dringenden Fällen (etwa bei Rechtsverletzungen) oder im Falle einer ausbleibenden Behebung kann der ANBIETER obige Informationen oder Dateien unverzüglich aus der IT-BISTUM löschen und/oder den Zugang sperren. Rechtliche Konsequenzen bleiben vorbehalten.

5.3 Der ANBIETER hat das Recht, eine vorübergehende Sperrung des Zugangs bereits dann durchzuführen, wenn Beschwerden von anderen Nutzerinnen und Nutzern vorliegen.

5.4 Der ANBIETER behält sich das Recht vor, im Falle eines Ausscheidens oder einer längeren Abwesenheit eines/einer internen Nutzers/Nutzerin, administrativ eine automatische Mail/Abwesenheitsnachricht einzurichten und/oder das E-Mail-Konto auf für den Dienstbetrieb relevante Nachrichten zu durchsuchen. Die Durchsicht erfolgt in der Regel in Absprache mit dem Nutzer/der Nutzerin. Ist dies nicht möglich, erfolgt die Durchsicht unter Aufsicht eines Gremiums bestehend aus dem Vorgesetzten/der Vorgesetzten bzw. der/dem Weisungsbefugten, dem Administrator/der Administratorin, dem/der zuständigen Datenschutzbeauftragten und, sofern der Nutzer durch eine MAV vertreten ist, auch ein Mitglied seiner/ihrer Mitarbeitervertretung (MAV).

6. Deaktivierung und Löschung des Zugangs

6.1 Die Deaktivierung des Zugangs des/r internen Nutzers/in erfolgt durch den ANBIETER nach Änderung oder Beendigung des zugrundeliegenden Rechtsverhältnisses.

6.2 Der/die externe Nutzer/in hat jederzeit die Möglichkeit, die Nutzung ohne Einhaltung von Fristen und Angabe von Gründen zu kündigen. Die Kündigung erfolgt in schriftlicher Form an den ANBIETER und führt zur Deaktivierung des Zugangs.

6.3 Eine Deaktivierung des Zugangs erfolgt zudem nach Ablauf der im Benutzerantrag vordefinierten Nutzungsdauer oder auf Hinweis der verantwortlichen Dienststelle/Einrichtung durch die/den jeweilige/n Vorgesetzte/n oder die/den Weisungsbefugte/n. Der/die externe Nutzer/in wird vor Deaktivierung benachrichtigt und hat die Möglichkeit eine Verlängerung über die/den Weisungsbefugte/n zu erwirken.

6.4 Der ANBIETER wird den Zugang 4 Wochen nach der Deaktivierung löschen, sofern der/die Nutzer/in schriftlich nichts anderes bestimmt hat.

6.5 Die fristlose Kündigung aus wichtigem Grund – insbesondere bei Verletzung der Ziffer 4 dieser Nutzungsbedingungen – bleibt unberührt.

6.6 Die von Nutzerinnen und Nutzern eingestellten Beiträge (z.B. Forumseinträge im Intranet, E-Mails, Dateien in den gemeinsamen Ablagen) bleiben nach der Löschung des Zugangs weiterhin in der IT-BISTUM abrufbar; es erfolgt ein Hinweis auf den gelöschten Zugang eines/r ehemaligen Nutzers/in.

7. Leistungen des ANBIETERS

Der ANBIETER stellt den Nutzerinnen und Nutzern im Rahmen der IT-BISTUM folgende Dienste zur Nutzung zur Verfügung:

- E-Mail
- Cloud-Computing
- Intranet
- Ingenius
- SAP

Der Umfang des Zugriffs auf die einzelnen Dienste richtet sich nach Rollen und Berechtigungen.

Die Leistungen des ANBIETERS beschränken sich grundsätzlich auf den technischen Betrieb der IT-BISTUM. Es wird keine Verantwortung für die von Nutzerinnen und Nutzern eingestellten Inhalte, Daten oder Informationen sowie Inhalte auf verlinkten externen Webseiten übernommen. Zudem wird keine Gewähr dafür übernommen, dass solche Inhalte wahr sind, einen bestimmten Zweck erfüllen oder einem solchen dienen können.

Der ANBIETER stellt für bestimmte Bereiche (z.B. MAV) Funktions-Accounts zur Verfügung. Diese Bereiche unterliegen deren selbstständiger Administration.

Der ANBIETER wird sich bemühen, den technischen Betrieb der IT-BISTUM durchgehend aufrecht zu halten. Dennoch kann es im Einzelfall erforderlich sein, die Leistungen vorübergehend zu beschränken (z.B. für Wartungsarbeiten, Sicherheitsmaßnahmen, Kapazitätsgrenzen etc.). Derartige Einschränkungen werden vom ANBIETER – soweit vorhersehbar – in der IT-BISTUM rechtzeitig angekündigt. Zudem kann es durch fremde Ursachen zu Beeinträchtigungen kommen (z.B. durch Störungen von Kommunikationsnetzen, Stromausfälle). Der ANBIETER übernimmt für derartige Beeinträchtigungen im technischen Betrieb keine Haftung, soweit kein eigenes Verschulden vorliegt und dieser Ausschluss im Einzelfall gesetzlich zulässig ist.

8. Dienste im Rahmen der IT-BISTUM

8.1 Cloud-Computing
Die Cloud-Computing-Lösung des ANBIETERS ermöglicht die Nutzung der freigegebenen Google G Suite Produkte, u.a. Kalender (Termintitel, Beschreibungen, Daten, Zeiten, Häufigkeit, eingeladene Gäste und Orte), Drive (in Google Drive hochgeladene Originaldateiinhalte), Formulare (Text, eingebettete Bilder, Antworten), Gmail (Themen,

Textkörper, Anhänge, Absender und Empfänger von Nachrichten), Google Docs, (Tabellen und Präsentationen, Textkörper der Datei, eingebettete Bilder, eingebettete Zeichnungen, zugehörige vom Endnutzer erstellte Kommentare), Hangouts Chat (Nachrichten, Anhänge), Vault (Exporte).

Grundsätzlich können innerhalb der G Suite auch sensible Inhalte bearbeitet und verarbeitet werden, solange diese die G Suite-Plattform nicht verlassen.
Die gesamte Kommunikation in den Produkten der G Suite erfolgt verschlüsselt, die Ablage der in der G Suite gespeicherten Daten erfolgt gestreut und verschlüsselt.

Die Verwendung der dienstlichen G Suite-Anmeldung zur Identifizierung und Anmeldung zu Diensten, die nicht vom ANBIETER bereitgestellt werden, ist grundsätzlich nicht gestattet. Dazu gehören insbesondere auch Erweiterungen von Drittanwendern für die G Suite.

Mit der Verwendung der G Suite werden keine Rechte an den Inhalten an Google G Suite abgetreten.

8.2 Intranet
Das Intranet dient als Plattform für interne und externe Nutzerinnen und Nutzer zum Austausch von Daten und Dokumenten sowie der Informationsgewinnung auf elektronischem Wege. Das Intranet enthält zudem mit Intrexx-Share auch Elemente eines so genannten „Social Intranets“ mit Werkzeugen für eine digitale

Zusammenarbeit wie Teamräumen, Chat-Funktionen und anderem. Parallel zu diesem Angebot werden Schulung, Direkthilfe, Tutorials und Klärung von Problemanzeigen vorgehalten. Unrechtmäßige, anstößige oder beleidigende Kommentare und Inhalte sowie Verlinkungen auf Webseiten mit derartigen Inhalten können durch jede Nutzerin und jeden Nutzer an den ANBIETER gemeldet und von diesem nach Prüfung ohne weitere Rücksprache entfernt werden.

8.3 Ingenius
Das Programm wird eingesetzt als Pfarrverwaltungssoftware und bietet folgende Funktionen: Termin- und Raumkalender, Liturgischer Kalender, Gottesdienstordnung, Pfarrbrieferstellung, Kollekten- und Zelebrationsplan, Stipendien- und Intentionen-Verwaltung.

Der Zugang zum Programm erfolgt entsprechend des Berechtigungskonzeptes.

Parallel dazu werden unterstützende Maßnahmen zur Schulung, Direkthilfe und Klärung von Problemanzeigen vorgehalten.

8.4 SAP
Die Leistungen des ANBIETERS beinhalten den technischen Betrieb und - soweit vereinbart oder aufgrund rechtlicher Rahmenbedingungen erforderlich - den fachlichen Betrieb und die Fachaufsicht der IT-BISTUM.

Liegt die fachliche Verantwortung nicht beim ANBIETER sondern bei einem eigenen Rechtsträger, ist eine schriftliche Vereinbarung zwischen dem ANBIETER und dem eigenen Rechtsträger erforderlich, in der beschrieben ist, wo die Fachaufsicht für die Nutzerinnen und Nutzern wahrgenommen wird.

Zugriffe auf Teilfunktionen und Inhalte innerhalb von SAP werden über das Rollenkonzept beschrieben. Die Zuteilung von Rollen erfolgt aufgrund schriftlicher Beantragung durch die Nutzerinnen und Nutzer und nach schriftlicher Freigabe durch die jeweils zuständigen Fachabteilungen/die vorgesetzte Fachaufsicht.

9. Datenschutz

Es gilt das Gesetz über den Kirchlichen Datenschutz (KDG) (KA 2018 Nr. 65) sowie die dazu erlassene Durchführungsverordnung KDG-DVO (KA 2019 Nr. 9) in den jeweils geltenden Fassungen.

Jede/r Nutzer/in ist nach § 5 KDG auf die Einhaltung des Datengeheimnisses zu verpflichten.

Der/die Nutzer/in erhält zur Information die „Datenschutzerklärung zur Nutzung der IT-Systeme des Bistums Trier“.

Es werden die Daten erhoben, die zur Bereitstellung der Dienste, der Aufrechterhaltung der Dienste und der Dokumentation der Zugriffe erforderlich sind.

10. Haftung des ANBIETERS gegenüber externen Nutzerinnen und Nutzern

10.1 Die Regelungen dieses Abschnitts 10 gelten ausschließlich für externe Nutzerinnen und Nutzer.
10.2 Der Anbieter ist nach den geltenden Gesetzen nicht dazu verpflichtet, die bei ihm gespeicherten Informationen zu überwachen. Sollte er jedoch Kenntnis von rechtswidrigen Handlungen eines/r Nutzers/in erhalten, so werden die rechtswidrigen Informationen nach Maßgabe von Ziffer 5.2 dieser NUTZUNGSBEDINGUNGEN entfernt oder der betreffende Zugang gesperrt.

10.3 Der ANBIETER übernimmt grundsätzlich keinerlei Gewähr für die Richtigkeit der im IT-System des Bistums Trier eingestellten Inhalte.
10.4 Die Haftung des ANBIETERS ist unbeschränkt bei Verletzung des Lebens, des Körpers oder der Gesundheit. Der ANBIETER haftet darüber hinaus unbeschränkt bei Vorsatz oder grober Fahrlässigkeit, bei einer Verletzung wesentlicher Vertragspflichten (Kardinalpflichten), im Falle der Übernahme von Garantien und wenn die Haftung zwingend gesetzlich vorgeschrieben ist (insb. Produkthaftungsgesetz). Der ANBIETER haftet auch dann, wenn die Verletzung im Sinne der Sätze 1 und 2 durch seine gesetzlichen Vertreter oder Erfüllungsgehilfen erfolgt.

10.5 Liegt kein Fall der Ziffer 10.4 vor, ist eine Haftung des ANBIETERS ausgeschlossen.

10.6 Die Nutzerinnen und Nutzer stellen den ANBIETER von sämtlichen Ansprüchen frei, die Dritte (einschließlich Behörden) infolge einer Verletzung von Rechten oder Rechtsvorschriften durch Handlungen des/der Nutzers/in im IT-System Bistum Trier gegen den ANBIETER geltend machen, soweit der/die Nutzer/in diese Verletzung zu vertreten hat (siehe Ziffer 4.6 und 4.11 dieser NUTZUNGSBEDINGUNGEN). Die Freistellung betrifft auch alle Kosten der anwaltlichen Rechtsverteidigung sowie ggf. anfallende Gerichts- und gegnerische Anwaltskosten, jeweils in gesetzlicher Höhe. Die Nutzerinnen und Nutzer haben die Pflicht, den ANBIETER mit allen notwendigen Informationen zur Rechtsverteidigung auszustatten.

11. Änderung der NUTZUNGSBEDINGUNGEN

11.1 Der ANBIETER behält sich vor, diese NUTZUNGSBEDINGUNGEN jederzeit zu ändern. Jede Änderung wird dem/der Nutzer/in rechtzeitig vor Inkrafttreten mitgeteilt.

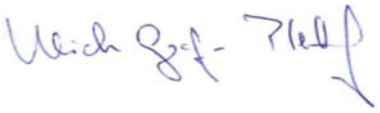
11.2 Der/die externe Nutzer/in hat innerhalb von 14 Tagen die Möglichkeit, gegen die veränderten NUTZUNGSBEDINGUNGEN in Schriftform Widerspruch einzulegen. Geschieht dies nicht, so gelten die veränderten NUTZUNGSBEDINGUNGEN als akzeptiert.
Im Falle eines Widerspruchs gegen die geänderten Nutzungsbedingungen hat der ANBIETER das Recht, den Zugang zu deaktivieren und zu löschen. Zu den eingestellten Beiträgen gilt Ziffer 6.6 dieser NUTZUNGSBEDINGUNGEN. Die Nutzerinnen und Nutzer stellen den ANBIETER von sämtlichen Schadensersatzansprüchen frei, die aus der Löschung des Profils resultieren könnten.

12. Schlussbestimmungen

12.1 Sollten einzelne Bestimmungen dieser NUTZUNGSBEDINGUNGEN unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen dieser NUTZUNGSBEDINGUNGEN hiervon nicht berührt.

12.2 Diese NUTZUNGSBEDINGUNGEN gelten bis zur Einstellung des Betriebs der IT-BISTUM oder bis zur Veröffentlichung neuer Bestimmungen. Bei Einstellung des Betriebs bzw. Einstellung der Dienstleistung werden die Nutzerinnen und Nutzer nach Möglichkeit mindestens 4 Wochen im Voraus vom ANBIETER informiert. Weitere Pflichten hat der ANBIETER bei Einstellung der Dienstleistung nicht.

Trier, den 28. April 2020



Dr. Ulrich Graf von Plettenberg
Bischöflicher Generalvikar

Anlage 1 (Zur Information für jede/n Nutzer/in):
Datenschutzerklärung zur Nutzung der IT-Systeme des Bistums Trier

Anlage 2 (Arbeitshilfe für die Vorgesetzten bzw. Weisungsbefugten):
Belehrung und Verpflichtung der Mitarbeiterinnen und Mitarbeiter aus datenschutzrechtlicher Sicht

- *Muster-Verpflichtungserklärung für Mitarbeiterinnen und Mitarbeiter des Bistums Trier (Zur Info der Gesamt-MAV / Die Organisation der Verpflichtung läuft über BGV, ZB 2.3)*
- *Muster-Verpflichtungserklärung für Mitarbeiterinnen und Mitarbeiter der Kirchengemeinden/Kirchengemeindeverbände (Zur Information der Gesamt-MAV/ Organisation der Neu-Verpflichtung läuft über BGV, ZB 2.3 bzw. im Falle von Neueinstellungen über die Rendanturen)*
- *Muster-Verpflichtungserklärung für ehrenamtliche Mitarbeiterinnen und Mitarbeiter (der Vollständigkeit halber zur Info an die Gesamt-MAV, Organisation wird durch die zuständige verantwortende Einsatzstelle im Sinne § 4 Nr. 9 KDG (z.B. Kirchengemeinde, Bistum) gewährleistet.*

----------Bitte unterzeichnet per Dienstpost senden an:----------

An das

Bischöfliche Generalvikariat Trier
ZB 2.7 Abteilung Informationssysteme
Mustorstraße 2
54292 Trier

oder diese unterzeichnete Seite per E-Mail senden an:
helpdesk@bgv-trier.de

Die Nutzungsbedingungen mit den Anlagen 1 - Datenschutzerklärung und 2 – Belehrung und Verpflichtung

zu den IT-Systemen des Bistums Trier habe ich zur Kenntnis genommen und verstanden:

Name, Vorname:
Pro Person bitte nur einmal ausfüllen, auch wenn mehrere Beschäftigungsverhältnisse vorliegen.

Für interne Nutzerinnen und Nutzer unter Angabe der Personalnummer:

Die Personalnummer finden Sie auf Ihrer Gehaltsabrechnung (über dem Adressfeld im oberen, linken Teil).

Für externe Nutzerinnen und Nutzer die Personalnummer: (falls vorhanden)

oder

im Falle von ehrenamtlichen Mitarbeiterinnen und Mitarbeitern sowie Personen, die aufgrund ihrer Tätigkeit für das Bistum Trier und für die Gremien des Bistums Trier einen Zugang zur IT-Bistum erhalten:

Name Organisationsbereich/Kirchengemeinde/Einrichtung

Geburtsdatum

private Postanschrift

private E-Mail-Adresse

private Mobil-Nr./Tel.-Nr.

Ort, Datum, Unterschrift des/der Nutzers/in

Anlage 1 zu den Nutzungsbedingungen IT-Systeme im Bistum Trier (E-Mail, Cloud-Computing, Intranet, Ingenius, SAP)

Datenschutzerklärung zur Nutzung der IT-Systeme des Bistums Trier

Den Schutz Ihrer Daten nehmen wir sehr ernst; die Einhaltung der datenschutzrechtlichen Anforderungen ist uns ein großes Anliegen. Rechtliche Grundlage ist für uns das Gesetz über den Kirchlichen Datenschutz (KDG) im Bistum Trier (KA 2018 Nr. 65) und die Durchführungsverordnung (KDG-DVO, KA 2019 Nr. 9) in der jeweils geltenden Fassung. Das Gesetz und weitere datenschutzrechtliche Informationen hierzu stehen Ihnen auch unter https://www.bistum-trier.de/datenschutz/ zur Verfügung.

Im Rahmen der Nutzung der IT-Systeme erhebt das Bistum Trier personenbezogene Daten von Ihnen, die für die Bereitstellung der jeweiligen Dienste benötigt werden. Sind Sie Beschäftigte/r des Bistums Trier im Sinne des § 4 Nr. 24 KDG oder Beschäftigte/r mit einem anderen arbeitsrechtlichen Rechtsverhältnis zum Bistum Trier, werden Ihre Daten auf der Rechtsgrundlage des § 53 Abs.1 KDG zur Durchführung Ihres Beschäftigungsverhältnisses verarbeitet. Stehen Sie in keinem Beschäftigungsverhältnis zum Bistum Trier, werden Ihre Daten auf der Grundlage des Nutzungsvertrages, den Sie mit der Anmeldung zu den IT-Systemen schließen (§ 6 Abs.1 c) KDG) verarbeitet.
Sofern die Verarbeitung Ihrer Daten zur Erfüllung einer kirchlichen oder staatlichen Rechtsvorschrift erfolgt oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, dienen darüber hinaus § 6 Abs. 1 a) oder d) KDG als Rechtsgrundlage.
Zur Bereitstellung der IT-Systeme arbeitet das Bistum Trier mit folgenden Auftragsverarbeitern zusammen:

- Für das Cloud-Computing: Google Ireland Limited mit Sitz in Dublin
- Für Ingenius: Compelec Computersysteme GmbH mit Sitz in Wadgassen
- Für SAP:
    1. Atos IT-Dienstleistung und Beratung GmbH mit Sitz in Gelsenkirchen
    2. msg Treorbis GmbH mit Sitz in Hamburg

Mit den Auftragsverarbeitern wurde jeweils ein Auftragsverarbeitungsvertrag entsprechend § 29 KDG geschlossen, der die Rechte und Pflichten zwischen dem Bistum Trier und den Auftragsverarbeitern regelt.
Eine Verarbeitung Ihrer Daten im Rahmen der Nutzung der IT-Systeme erfolgt grundsätzlich in der EU, so dass die strengen Regeln der europäischen Datenschutzgesetze gelten.
Im Rahmen der Nutzung des Cloud-Computings kann es zu einem Datentransfer in Drittländer (Länder außerhalb der EU) kommen. Von einer Datenübermittlung in Drittländer können dabei im Wesentlichen folgende Daten betroffen sein:

- Ihre dienstliche E-Mail-Adresse bestehend aus Vorname.Nachname@bgv-trier.de oder Vorname.Nachname@bistum-trier.de
- die Seite, von der aus die Datei angefordert wurde
- der Name der aufgerufenen Datei
- das Datum und die Uhrzeit der Anforderung
- die übertragene Datenmenge
- der Zugriffsstatus (Datei übertragen, Datei nicht gefunden, etc.)
- die Beschreibung des verwendeten Webbrowsertyps bzw. des verwendeten Betriebssystems
- die verwendete Sprache
- die IP-Adresse des anfordernden Rechners

Die Datenübermittlung erfolgt in diesem Fall auf der Grundlage der Standardvertragsklauseln nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates. Damit ist auch die Datenübermittlung bzw. –verarbeitung in Drittländern vertraglich geregelt.

Bei der Nutzung der IT-Systeme werden folgende Daten verarbeitet:

a) Zwingend erforderliche Stammdaten zur Anlage der Benutzerkonten. Sie dienen Ihrer Identifikation als Nutzer/in der IT-Systeme und dem Zweck der Vergabe von Rollen und Berechtigungen. (Beantragung des Zugangs/Anmeldung siehe Nutzungsbedingungen, Ihre jeweilige persönliche Benutzerkennung, die

individuell durch Sie als Nutzer/in angelegt wird sowie Ihr persönliches Passwort/Kennwort. Anforderungen an die persönliche Benutzerkennung zur Anmeldung im System und das persönliche Passwort/Kennwort siehe Nutzungsbedingungen (vgl. hierzu Pkt. 3.9)

b) Optionale Daten (Zeitzone, Schrift, etc.)
c) Nutzungsdaten = z.B. IP-Adresse, genutzte Dienste (z.B. Dateidownloads), Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung, Protokollierung von Eingaben oder Änderungen
d) Statistische Daten stehen lediglich der Administration zur Gewährleistung und Absicherung des Betriebes bzw. zur Verrechnung zur Verfügung.

Wie bei der Nutzung jeder Internetseite erfolgt eine technische Protokollierung der Zugriffe. Diese Protokollierung erfolgt rein intern beim Auftragsverarbeiter und dient zur Sicherstellung der Funktion und der Sicherheit. Es handelt sich hierbei im Wesentlichen um

- Ihre dienstliche E-Mail-Adresse bestehend aus Vorname.Nachname@bistum-trier.de oder Vorname.Nachname@bgv-trier.de
- die Seite bzw. die Datei, die angefordert wurde
- das Datum und die Uhrzeit der Anforderung
- die übertragene Datenmenge
- der Zugriffsstatus (Seite bzw. Datei übertragen, nicht gefunden, etc.)
- die Beschreibung des verwendeten Webbrowsertyps bzw. des verwendeten Betriebssystems
- die Internet-Adresse, von der der Aufruf erfolgt ist

Im Rahmen der Nutzung des Cloud-Computings können wir nicht ausschließen, dass Ihre personenbezogenen Daten durch unseren Auftragsverarbeiter zu Zwecken der Strafverfolgung an U.S. amerikanische Behörden weitergegeben werden.

Es besteht immer die Gefahr, dass Daten (personenbezogene Daten/Fotos/Videos) in falsche Hände gelangen oder über das Ende ihrer zulässigen Verwendung weiter gespeichert oder genutzt werden. Bei missbräuchlicher Verwendung der personenbezogenen Daten besteht beispielsweise auch die Gefahr eines Betrugs, des Identitätsdiebstahls oder der Diskriminierung/Rufschädigung. Daten könnten auch kopiert, dupliziert oder in anderer Weise verarbeitet werden, ohne dass der Auftraggeber die Möglichkeit besitzt, hierauf Einfluss zu nehmen. Kommen Zahlungsdaten abhanden, kann es zu finanziellen Verlusten kommen.

Ihre Daten werden für die Dauer Ihrer Nutzung der IT-Systeme gespeichert und nach Beendigung des Nutzungsvertrages bzw. des Arbeitsvertrages nach Ablauf der gesetzlichen Aufbewahrungs- und Verjährungsfristen gelöscht oder pseudonymisiert.

Sie können Ihre nachfolgenden Rechte jederzeit bei der **hierfür verantwortlichen Stelle, dem Bistum Trier, Bischöfliches Generalvikariat, ZB 2.7 Abteilung Informationssysteme, Mustorstr. 2, 54290 Trier, E-Mail-Adresse:** helpdesk@bistum-trier.de, geltend machen. Um die Richtigkeit und Aktualität Ihrer Daten zu gewährleisten ist es erforderlich, dass Sie Änderungen unverzüglich an die vorgenannte verantwortliche Stelle schriftlich melden.

Nachfolgend weisen wir Sie auf Ihre Rechte hin:

1. **Recht auf Widerruf der datenschutzrechtlichen Einwilligungserklärung (vgl. § 8 KDG)**
   Für den Fall, dass die Verarbeitung Ihrer Daten auf Ihrer datenschutzrechtlichen Einwilligungserklärung beruht, haben Sie nach § 8 KDG das Recht, diese jederzeit zu widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung wird davon nicht berührt.

2. **Auskunftsrecht (vgl. § 17 KDG)**
   Sie haben das Recht auf eine transparente Information. Auf Verlangen geben wir Ihnen darüber Auskunft, welche Ihrer personenbezogenen Daten zu welchem Zweck verarbeitet werden.

3. **Recht auf Berichtigung (vgl. §18 KDG)**
   Sie haben das Recht auf Berichtigung unrichtiger Daten, die Ihre Person betreffen.

4. **Recht auf Löschung (vgl. § 19 KDG)**
   Unter den in § 19 KDG genannten Voraussetzungen (z. B. falls Sie eine erteilte Einwilligung widerrufen oder die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind) haben Sie das Recht, eine Löschung der Sie betreffenden personenbezogenen Daten zu verlangen.

5. **Recht auf Einschränkung der Verarbeitung (vgl. § 20 KDG)**
   Unter den in § 20 KDG genannten Voraussetzungen haben Sie das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen.

6. **Recht auf Unterrichtung (vgl. § 21 KDG)**
   Haben Sie Ihr Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gegenüber dem Verantwortlichen geltend gemacht, ist dieser verpflichtet, allen Empfängern, denen die Sie betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung oder Löschung der Daten oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Ihnen steht gegenüber dem Verantwortlichen das Recht zu, über diese Empfänger unterrichtet zu werden.

7. **Recht auf Datenübertragbarkeit (vgl. § 22 KDG)**
   Ihnen steht auch das Recht zu, die Sie betreffenden personenbezogenen Daten, die Sie dem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

8. **Widerspruchsrecht (vgl. § 23 KDG)**
   In bestimmten Fällen, die in § 23 KDG näher beschrieben sind, haben Sie jederzeit das Recht, gegen die Verarbeitung der Sie betreffenden personenbezogenen Daten Widerspruch einzulegen.

9. **Automatisierte Entscheidung im Einzelfall (vgl. § 24 KDG)**
   Von der Möglichkeit ausschließlich automatisierter Entscheidungen, die im Einzelfall zulässig wären, machen wir keinen Gebrauch.

10. **Unabdingbare Rechte der betroffenen Person (vgl. § 25 KDG)**
    Diese Rechte können nicht ausgeschlossen oder beschränkt werden. Geltend gemachte Rechte sind in jedem Fall an den zuständigen Verantwortlichen weiterzuleiten.

Daneben stehen Ihnen unterstützend und beratend die Datenschutzbeauftragten zur Verfügung:
Bischöfliches Generalvikariat Trier, Stabsstelle Betrieblicher Datenschutz,
Mustorstraße 2, 54290 Trier, Tel: 0651-7105-0
datenschutz@bgv-trier.de oder datenschutz-pfarreien@bgv-trier.de

Das Bistum Trier tut alles um Ihre Daten zu schützen. Für den Fall, dass Sie sich jedoch im Umgang mit Ihren Daten nicht gut behandelt fühlen, haben Sie auch ein **Recht auf Beschwerde bei einer Aufsichtsbehörde** (vgl. § 48 KDG). Dieses können Sie wahrnehmen über die **Überdiözesane Aufsichtsstelle im Datenschutz der (Erz-) Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier**, ansässig derzeit im Haus am Dom, Domplatz 3, 60311 Frankfurt, Tel: 069-8008718-800, E-Mail: info(at)kdsz-ffm.de

Anlage 2 zu den Nutzungsbedingungen IT-Systeme im Bistum Trier

Zielgruppen:

1. Vorgesetzte und Weisungsbefugte (als Arbeitshilfe)
2. Mitarbeiterinnen/Mitarbeiter – Nutzerinnen/Nutzer der IT-Systeme im Bistum Trier (zur Information)

Belehrung und Verpflichtung der Mitarbeiter/innen aus datenschutzrechtlicher Sicht

Rechtsgrundlagen:

§ 5 KDG - Datengeheimnis
Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 2 KDG-DVO - Belehrung und Verpflichtung auf das Datengeheimnis
(1) Zu den bei der Verarbeitung personenbezogener Daten tätigen Personen im Sinne des § 5 KDG gehören die in den Stellen gemäß § 3 Absatz 1 KDG Beschäftigten im Sinne des § 4 Ziffer 24. KDG sowie die dort ehrenamtlich tätigen Personen (Mitarbeiter im Sinne dieser Durchführungsverordnung, im Folgenden: Mitarbeiter).
(2) Durch geeignete Maßnahmen sind die Mitarbeiter mit den Vorschriften des KDG sowie den anderen für ihre Tätigkeit geltenden Datenschutzvorschriften vertraut zu machen. Dies geschieht im Wesentlichen durch Hinweis auf die für den Aufgabenbereich der Person wesentlichen Grundsätze und Erfordernisse und im Übrigen durch Bekanntgabe der entsprechenden Regelungstexte in der jeweils gültigen Fassung. Das KDG und diese Durchführungsverordnung sowie die sonstigen Datenschutzvorschriften werden zur Einsichtnahme und etwaigen Ausleihe bereitgehalten oder elektronisch zur Verfügung gestellt; dies ist den Mitarbeitern in geeigneter Weise mitzuteilen.
(3) Ferner sind die Mitarbeiter zu belehren über
a) die Verpflichtung zur Beachtung der in Absatz 2 genannten Vorschriften bei der Verarbeitung personenbezogener Daten,
b) mögliche rechtliche Folgen eines Verstoßes gegen das KDG und andere für ihre Tätigkeit geltenden Datenschutzvorschriften,
c) das Fortbestehen des Datengeheimnisses nach Beendigung der Tätigkeit bei der Datenverarbeitung.
(4) Bei einer wesentlichen Änderung des KDG oder anderer für die Tätigkeit der Mitarbeiter geltenden Datenschutzvorschriften sowie bei Aufnahme einer neuen Tätigkeit durch den Mitarbeiter hat insoweit eine erneute Belehrung zu erfolgen.
(5) Die Mitarbeiter haben in nachweisbar dokumentierter Form eine Verpflichtungserklärung gemäß § 3 abzugeben. Diese Verpflichtungserklärung wird zu der Personalakte bzw. den Unterlagen des jeweiligen Mitarbeiters genommen. Dieser erhält eine Ausfertigung der Erklärung.
(6) Die Verpflichtung auf das Datengeheimnis erfolgt durch den Verantwortlichen oder einen von ihm Beauftragten.

§ 3 KDG-DVO - Inhalt der Verpflichtungserklärung
(1) Die gemäß § 2 Absatz 5 nachweisbar zu dokumentierende Verpflichtungserklärung des Mitarbeiters gemäß § 5 Satz 2 KDG hat zum Inhalt:
a) Angaben zur Identifizierung des Mitarbeiters (Vorname, Zuname, Beschäftigungsdienststelle, Personalnummer sowie, sofern Personalnummer nicht vorhanden, Geburtsdatum und Anschrift),
b) die Bestätigung, dass der Mitarbeiter auf die für die Ausübung seiner Tätigkeit spezifisch geltenden Bestimmungen und im Übrigen auf die allgemeinen datenschutzrechtlichen Regelungen in den jeweils geltenden Fassungen sowie auf die Möglichkeit der Einsichtnahme und Ausleihe dieser Texte hingewiesen wurde,
c) die Verpflichtung des Mitarbeiters, das KDG und andere für seine Tätigkeit geltenden Datenschutzvorschriften in den jeweils geltenden Fassungen sorgfältig einzuhalten,
d) die Bestätigung, dass der Mitarbeiter über rechtliche Folgen eines Verstoßes gegen das KDG sowie gegen sonstige für die Ausübung seiner Tätigkeit spezifisch geltenden Bestimmungen belehrt wurde.

(2) Die Verpflichtungserklärung ist von dem Mitarbeiter unter Angabe des Ortes und des Datums der Unterschriftsleistung zu unterzeichnen oder auf eine andere dem Verfahren angemessene Weise zu signieren.
(3) Sofern die zuständige Datenschutzaufsicht ein Muster einer Verpflichtungserklärung zur Verfügung stellt, bildet dieses den Mindeststandard. Bisherige Verpflichtungserklärungen nach § 4 KDO bleiben wirksam.

Empfehlung der Stabsstelle Betrieblicher Datenschutz zum Umgang mit dieser gesetzlichen Anforderung in der Praxis:

Bestenfalls erfolgt die datenschutzrechtliche Belehrung und Verpflichtung im Rahmen der ersten Einweisung, bevor der/die Mitarbeiter/in seine Arbeit aufnimmt. Bei bestehenden Arbeitsverhältnissen erfolgt dies bei wesentlichen Änderungen (die sich z.B. aus der neuen Gesetzgebung und diesen Nutzungsbedingungen ergeben.)
Ziel dieser Belehrung aus datenschutzrechtlicher Sicht ist es, die Mitarbeiterinnen und Mitarbeiter anzuhalten, mit den personenbezogenen Daten die ihr/ihm anvertraut werden, sehr verantwortungsbewusst umzugehen. Kein Dienstgeber kann erwarten, dass ein/e Mitarbeiter/in von alleine weiß, was er von ihm/ihr erwartet und welche datenschutzrechtlichen Anforderungen es durch ihn/sie zu erfüllen gilt.
Der/die Mitarbeiter/in wird auf das Gesetz über den Kirchlichen Datenschutz und seine Verordnungen hingewiesen (z.B. auch auf § 2 KDG-DVO-Belehrung und Verpflichtung auf das Datengeheimnis).
Getroffene Datenschutzmaßnahmen (Technische und organisatorische Maßnahmen=TOMs), wie beispielsweise Zugangskontrollen (z.B. Umgang mit Schlüssel oder Token) und Nutzungsbedingungen (in den IT-Systemen des Bistums), bieten alleine keine hundertprozentige Sicherheit. Entscheidend ist, dass der/die Mitarbeiter/in mit den Daten verantwortungsbewusst und sorgfältig umgeht. Ohne eine (vorherige) Datenschutzunterweisung besteht ein erhöhtes Risiko, dass der/die Mitarbeiter/in, oft unabsichtlich, Datenschutzverstöße begeht.
Die Verpflichtung zur Vermittlung des notwendigen fachspezifische Wissens und der getroffenen Datenschutzmaßnahmen in der jeweils verantwortlichen Stelle/Einrichtung besteht für die/den Vorgesetzten oder für einen von ihr/ihm damit Beauftragten.
Zur Bewältigung dieser Aufgabe stehen derzeit, neben der mündlichen Belehrung durch den Vorgesetzten, folgende Möglichkeiten zur Verfügung:

a) Auf der Rückseite der Verpflichtungserklärungen befindet sich eine Aufstellung über die berufsspezifischen Rechtsgrundlagen (nicht abgeschlossen, wird sich weiterentwickeln und ist jeweils im Intranet abrufbar.)
b) Verpflichtende Schulung (Online Schulung o.ä.) mit Nachweis in der Personalakte
c) Freiwillige Schulungsangebote
d) bedarfsgerechte Beratungen auf Anfrage vor Ort

Zu einer Belehrung aus datenschutzrechtlicher Sicht gehört über § 2 KDG-DVO hinaus auch:

1. **die Frage nach der Teilnahme an der verpflichtenden Datenschutzschulung,** ob das Zertifikat erworben wurde und der Personalverwaltung zur Ablage in der Personalakte (bzw. in der Einrichtung für die ehrenamtlichen Mitarbeiter/innen) vorliegt und ob es darüber hinaus noch datenschutzrechtliche Fragen gibt.

   Die Schulungen werden von den BDSB der Stabsstelle (in Zusammenarbeit mit dem SB 2 bzw. ZB 1.5) vorgenommen. Unabhängig von der ausgeübten Tätigkeit des/der Mitarbeiters/in sollte jeder über ein Basiswissen im Datenschutz verfügen und sich beispielweise mit Fragen auskennen, was Daten mit Personenbezug sind, was unter sensiblen bzw. besonderen Arten von Daten sowie den verschiedenen Datenschutzklassen zu verstehen ist, dass Menschen ein Recht auf Privatsphäre haben und welche Risiken bei Datenschutzverstößen bestehen.

2. **der Hinweis auf weiterführende bereitstehende Datenschutzschulungen in div. Fortbildungsprogrammen (z.B. Stabsstelle in Zusammenarbeit mit dem SB 2, ZB 1.5)**
   a. Es empfiehlt sich, die wichtigsten Inhalte nach einer gewissen Zeitspanne zu wiederholen, damit sie den Mitarbeitern/innen in Erinnerung bleiben.
   b. Kommt es zu datenschutzrechtlichen Neuerungen/Änderungen oder es wird eine neue Software eingeführt, die andere Prozesse im Datenschutz erfordern, so bedarf es einer ergänzenden Datenschutzunterweisung.

3. **der Hinweis auf die Stabsstelle und die zuständigen BDSB.**
    a. Informationen zu relevanten Neuerungen im Datenschutz werden durch die Stabsstelle an die Vorgesetzten gegeben.
    b. Die Vorgesetzten tragen Sorge dafür, dass nicht nur sie selbst sondern auch ihre jeweiligen Mitarbeiter/innen über Neuerungen informiert werden und auch dafür, je nach Erfordernis weiteren Schulungs- oder Beratungsbedarf, bei der Stabsstelle anzumelden.

4. **die Informationen der Vorgesetzten an den Mitarbeiter/in im jeweiligen Zuständigkeitsbereich über die geltenden kirchlichen Datenschutzrichtlinien (KDG und KDG/DVO) und über die fachspezifischen Rechtsgrundlagen, die er/sie zur Erfüllung seiner/ihrer Aufgaben benötigt. Datenschutzunterweisungen müssen auf die Mitarbeiter/innen und auf die jeweiligen Tätigkeitsfelder zugeschnitten sein. Eine Auswahl von fachspezifischen Datenschutzbestimmungen ist auf der Rückseite jeder Verpflichtungserklärung zu finden, denn die datenschutzrechtlichen Herausforderungen, die sich im Berufsalltag stellen, können je nach Aufgabe und Position variieren** (z.B. muss ein/e Lehrer/in nicht nur das KDG sondern auch § 67 des Schulgesetzes RLP kennen. Ein/e Mitarbeiter/in der Lebensberatung die verschiedenen SGB, usw.) Die Aufstellung wird nach Hinweisen durch die Fachabteilungen und bei Bedarf durch die Stabsstelle Betrieblicher Datenschutz aktualisiert und steht jedem/r Mitarbeiter/in im Intranet Portal des Bistums Trier in aktueller Fassung, zusammen mit Verlinkungen zu den aktuellen Gesetzestexten, zur Verfügung.

5. **Der Hinweis auf die TOMs in der jeweiligen Dienststelle/Einrichtung/Fachabteilung insbesondere zum/zur**
    a. Umgang mit Schlüssel/Token
    b. Passwortgestaltung, Verfahren im Zusammenhang mit Vertretung/Krankheit usw.
    c. Umgang mit datenschutzkonformer Verarbeitung, Weitergabe, Aufbewahrung oder Löschung/Entsorgung von personenbezogenen Daten
    d. Rollen- und Berechtigungskonzept incl. der Beantragung oder des Entzuges von Zugangsberechtigungen unter Berücksichtigung der zu erfüllenden Aufgaben des/der Mitarbeiters/in
    e. Einteilung der gängigen Datenarten in die Datenschutzklassen und die unterschiedlichen Schutzniveaus (Stichwort angemessene Sicherheit)
    f. professionellen Umgang zur Informationspflicht und im Umgang mit den Rechten der betroffenen Personen
    g. Umgang mit Datenpannen (Notfallplanung!)
    h. Aushändigung der Broschüre „Daten schützen? Aber sicher!“
    i. …

6. **Die Frage, ob die Verpflichtungserklärung unterzeichnet in der Personalverwaltung ZB 2.3 vorliegt.**