Verpflichtungserklärung

zum Datengeheimnis und zur Einhaltung der datenschutzrechtlichen Anforderungen
des Gesetzes über den Kirchlichen Datenschutz (KDG)

Name, Vorname
geboren am
Dienststelle

I. Für alle Mitarbeitenden, die mit personenbezogenen Daten zu tun haben.

(1) Ich verpflichte mich, zur Einhaltung des Datengeheimnisses (§ 5 KDG) und zur Einhaltung des kirchlichen Datenschutzgesetzes und der dazu erlassenden Verordnung in der jeweils gültigen Fassung.

Ich versichere, dass ich alle personenbezogenen Daten, die ich im Rahmen meiner Tätigkeit verarbeite oder die mir zur Kenntnis gelangen, vertraulich behandele. Das Datengeheimnis besteht auch nach Beendigung meiner Tätigkeit fort.

(2) Mir ist bekannt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist (§ 6 KDG). Die Grundsätze des kirchlichen Rechts für die Verarbeitung personenbezogener Daten (§ 7 Abs.1 KDG) habe ich zur Kenntnis genommen. Sie beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden *(„Rechtmäßigkeit, Transparenz“)*;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden *(„Zweckbindung“)*;
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein *(„Datenminimierung“)*;
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden *(„Richtigkeit“)*;
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist *(„Speicherbegrenzung“)*;
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen *(„Integrität und Vertraulichkeit“)*.

Weitere sich aus dem Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtungen werden durch diese Erklärung nicht berührt.

Ich bin darüber belehrt worden, dass ein Verstoß gegen die Vorschriften des KDG und die anderen für meine Tätigkeit geltenden Datenschutzvorschriften ein Verstoß gegen arbeitsrechtliche Pflichten darstellt, der rechtliche Folgen haben kann, wie sie im beigefügten Merkblatt beschrieben sind.

II. Für Mitarbeitende, die personenbezogene Daten zusätzlich digital verarbeiten:

Ich bin auf die in Abschnitt II Ziff. 1 und 2 des anschließenden Merkblatts enthaltenen Regelungen zur Nutzung dienstlicher und privater digitaler Medien hingewiesen worden.

III. Bestätigung der Verpflichtung

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung und das Merkblatt Datenschutz habe ich erhalten.

....., …….....	....., …….....
Ort, Datum	Ort, Datum
.....	.....
Unterschrift der/des Verpflichteten	Unterschrift der/des Verantwortlichen

Original: Personalakte
1 Kopie: Verpflichtete(r)

Merkblatt Datenschutz

I. Für alle Mitarbeitende, die mit personenbezogene Daten zu tun haben

Im Rahmen Ihrer Tätigkeit arbeiten Sie mit personenbezogenen Daten z. B. unserer Mitglieder, Mitarbeitenden und Geschäftspartnerinnen und -partner oder es gibt für Sie die Möglichkeit des Zugriffs auf solche Daten. Deshalb müssen Sie sich mit den wichtigsten Grundsätzen des Datenschutzes vertraut machen.

(1) Die wichtigste Grundlage für den Datenschutz bei uns ist das KDG. Das kirchliche Datenschutzgesetz schützt **personenbezogene Daten.** Das sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen („natürliche Person") beziehen, wie z.B. Geburtsdatum, Anschrift. Anonyme Daten fallen nicht unter die Datenschutzgesetze.

(2) **Geschützt wird das informationelle Selbstbestimmungsrechts jedes Einzelnen**: Jeder soll grundsätzlich selbst darüber bestimmen dürfen, wer welche Daten über ihn kennt und verarbeitet. Deshalb dürfen personenbezogene Daten nur verarbeitet werden, wenn hierfür eine Einwilligung der betroffenen Person vorliegt oder eine Erlaubnis im Gesetz oder einem Vertrag vorhanden ist.

Besonders schützenswerte „sensible" **Daten** (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheit, Sexualleben, strafrechtliche Verurteilungen, Straftaten oder damit verbundene Sicherungsmaßnahmen) dürfen regelmäßig nicht verarbeitet werden. Für das Beschäftigungsverhältnis gibt es aber für erforderliche Verarbeitungen gesetzliche Ausnahmen. Außerdem besteht die Möglichkeit einer ausdrücklich auf diese Daten bezogenen Einwilligung.

(3) Häufig verwendete **Rechtsgrundlagen für die Datenverarbeitung** sind:
- zur Erfüllung eines Gesetzes, z.B. 10-jährige Aufbewahrungsfrist von Rechnungen gemäß AO.
- zur Erfüllung eines Vertrags, z. B. Arbeitsvertrag;
- zur Erfüllung einer Aufgabe, die im kirchlichen Interesse liegt, z.B. Vorbereitung Erstkommunion, Personalverwaltung pastorales Personal.

oder
- die **Einwilligung** der betroffenen Person, z.B. Einwilligung zum Erhalt eines Newsletters, Einwilligung für die Veröffentlichung eines Porträtfotos. Die Erteilung der Einwilligung ist immer freiwillig. Der Betroffene darf nicht benachteiligt werden und kann die Einwilligung jederzeit widerrufen.

(4) Die Transparenz der Datenverarbeitung ist eine wichtige Voraussetzung für das informationelle Selbstbestimmungsrecht. Es besteht eine Informationspflicht gegenüber der betroffenen Person. Bei Erhebung der Daten oder beim erstmaligen Kontakt muss die Person umfassend mit einem **Datenschutzhinweis** informiert werden.

(5) Bei Vorliegen der gesetzlichen Voraussetzungen stehen jeder betroffenen Person außerdem die **Betroffenenrechte** zu. Diese sind die Rechte auf Auskunft, Berichtigung, Löschung, Beschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und Datenübertragbarkeit, sowie ein Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde.

(6) Verarbeitete Daten, wie z.B. wie z.B. Adresslisten, Email-Verteiler, Vertragsunterlagen, sind zu **löschen**, sobald der Zweck erfüllt ist. Längere Aufbewahrungsfristen aufgrund von gesetzlichen Regelungen sind zu beachten.

(7) Schließlich müssen unsere Mitglieder, Beschäftigten und Vertragspartnerinnen und -partner darauf vertrauen können, dass ihre personenbezogenen Daten bei uns sicher sind. Datenschutz und Datensicherheit haben zwei wichtige Grundlagen: eine persönliche und eine technische.

Persönlich müssen Sie als Mitarbeitende/r die Vertraulichkeit der Verarbeitung beachten, zu der Sie sich umseitig verpflichtet haben.

Bitte beachten Sie, dass ein **Verstoß gegen die datenschutzrechtlichen Bestimmungen** ein Verstoß gegen arbeitsrechtliche Pflichten darstellt, der entsprechend geahndet werden kann. Dies kann ggf. Geldbußen, Geldstrafen oder gar Freiheitsstrafe bis zu einem Jahr bedeuten. Entsteht der betroffenen Person durch die unbefugte Verarbeitung ein Schaden, kann ebenfalls ein Schadensersatzanspruch entstehen.

Technisch und organisatorisch muss die Datensicherheit durch geeignete und angemessene Maßnahmen **(TOM)** sichergestellt werden, um personenbezogenen Daten gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen und den Schutz der Rechte der betroffenen Personen und die Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen zu gewährleisten.

(8) Helfen Sie dabei, die Ihnen anvertrauten personenbezogenen Daten zu schützen. Gehen Sie weisungsgemäß und sorgfältig damit um. Melden Sie verdächtige Beobachtungen und Datenschutz- oder Datensicherheitsverletzungen Ihren Vorgesetzen.

(9) **Schulungsangebote**, gesetzliche Grundlagen (KDG, KDG-DVO), Mustervorlagen und weiterführende Informationen finden Sie unter www.ebfr.de/datenschutz oder wenden Sie sich an Ihre/n betriebliche/n Datenschutzbeauftragte/n.

II. Hinweis zur Verwendung privater Geräte oder Privatnutzung dienstlicher Geräte:

(1) Die Nutzung von Telefax, E-Mail, Internet/Intranet sowie sonstiger im Rahmen meines Auftrages zur Verfügung gestellter dienstlicher Hard- und Software für private Zwecke ist nicht zulässig.

(2) Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen ist grundsätzlich unzulässig. Sie kann gem. § 20 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

III. Praktische Hinweise im Umgang mit der Verarbeitung von personenbezogenen Daten im Alltag:

Diese praktischen Hinweise dienen der allgemeinen Unterstützung im Umgang mit der Verarbeitung von personenbezogenen Daten im Alltag für Mitarbeitende. Die Hinweise können nicht vollständig sein, geben jedoch einen grundlegenden Rahmen.
Bei allen Fragen rund um IT-Sicherheit wenden Sie sich bitte an die diözesane IT.

(1) Zweckbindung
- Die Datenverarbeitung ist zweckgebunden. Eine Zweckänderung bedarf im Einzelfall einer neuen Rechtsgrundlage.
- Personenbezogene Daten dürfen nur in besonderen Fällen für andere Zwecke verarbeitet werden (§ 6 Abs. 2 KDG).

(2) Zugang zu PC / Laptop
- Der Zugang zu den PCs oder Laptops muss über ein Passwort geschützt sein. Bitte beachten Sie die jeweils aktuelle Empfehlung der Diözesanen IT.
- Speichern Sie keine Passwörter in Ihrem Browser ab.
- Passwörter dürfen nicht auf Notizzetteln oder ähnlichem aufgeschrieben werden.
- Wird der PC von mehreren Personen oder Gruppen benutzt, ist darauf zu achten, dass jeder nur die Programme und Daten benutzen kann, die für seine Arbeit erforderlich sind.
- Nach Möglichkeit sollten sich Monitore nach einer bestimmten voreingestellten Zeit abschalten (Bildschirmschoner).

(3) E-Mail
- Vor dem Versenden Adressat prüfen.
- Bcc nutzen, wo immer möglich.
- E-Mails mit Daten der Datenschutzklassen II (z.B. Daten über Mietverhältnisse und Geburts- und Jubiläumsdaten) und III dürfen nur mit einer Ende-zu–Ende-Verschlüsselung übertragen werden.

(4) Telefon
- Schutz vor Mithören sicherstellen.

(5) Datenverwaltung
- Akten und Datenträger (USB-Sticks, CD's, externe Festplatten und andere Speichermedien), die personenbezogene Daten beinhalten, sind in verschließbaren Räumen, Schränken, Behältern aufzubewahren.
- Unbefugte dürfen keine Einsicht in Akten und Datenträger nehmen.
- Mobile Datenträger sind zu verschlüsseln.

(6) Schriftgutverwaltung
- Papierakten mit personenbezogenen Daten nie im normalen Müll entsorgen.
- Geheimhaltungsbedürftige Dokumente verschlüsseln oder per Post senden.

(7) WLAN-Nutzung /Gäste WLAN
- Sollte ein WLAN-Netz vorhanden sein, so ist dieses entsprechend „dem Stand der Technik" gesichert zu betreiben. Insbesondere ist zu regeln, ob und wie Gastnutzern Zugang zum WLAN gewährt wird.

(8) Schreibtisch/ Arbeitsplatz (clean-desk)
- Das Aufräumen vor Verlassen des Arbeitsplatzes - insbesondere vor dem Feierabend, so dass keine Akten, sensible Dokumente etc. offen auf dem Tisch liegen bleiben – schützt vor unbefugter Kenntnisnahme.

(9) Schlüsselliste
- Es ist eine Schlüsselliste zu führen. Jederzeit ist somit nachvollziehbar, wer Schlüssel zum Gebäude oder zu Schränken hat.