2 Kenntnis, was mit diesen Daten geschehen darf – oder eben nicht!

Die Verarbeitung von Daten ist verboten - außer sie dient einem ***Zweck*** und hat eine ***Rechtsgrundlage,***
→ *Z.B.* gesetzliche Grundlagen, Erfüllung eines Vertrages, Wahrung von berechtigten Interessen,
→im kirchlichen Interesse/ im Zusammenhang mit der Verkündigung etc.
→Oder es gibt keine Rechtsgrundlage, aber eine Einwilligung der betroffenen Person.

Zweckgebundenheit: Daten dürfen nur für den benannten Zweck verwendet werden *(d.h. Kommunionkinder-Adressen dürfen nicht für den örtlichen Fußballverein oder Helferlisten nicht für eine Tupperparty-Einladung verwendet werden etc.).* Eine Nutzung über den Zweck hinaus bedarf einer Rechtsgrundlage – oder ein Einverständnis.
Datenvermeidung/Datensparsamkeit: Ziel ist es, so wenig Daten wie möglich zu verarbeiten.
Welche Daten braucht es also wirklich?
Die Weitergabe von Daten, etwa für Fahrgemeinschaften, braucht eine Zustimmung.
Der Schutz von Daten gegenüber Dritten und Unbefugten muss gegeben sein.

3 Daten löschen!

Zweckgebundenheit bedeutet auch die Löschung nach Abschluss & Dokumentationszeitraum. Als Veranstalter noch bedenken, dass die Daten in einem möglichen Haftungsfall später als Beweise dienen können, oder andere Rechtsgrundlagen zur Aufbewahrung (z.B. Rechnungen).
Angemessene Entsorgung beachten! Ggf. Daten schreddern und Datenträger korrekt entsorgen.

4 Wenn man Daten erheben darf…Datenschutzhinweise geben!

Sofern Daten nach einer Rechtsgrundlage erhoben werden dürfen, braucht es kein Einverständnis dazu – aber klare Information, was genau zu welchem Zweck und wie lange gesammelt wird.
Der Datenschutzhinweis sollte dem Betroffenen leicht zugänglich sein, dies kann unterschiedlich – je nach Betroffenengruppe – ausgestaltet sein*, z.B. Aushang, Link auf Homepage, mündlicher Hinweis, den Datenschutzhinweis auf die Einladung dazuschreiben, mit einer anschließenden Post versenden, als Verweis auf die Homepage (dort aber spezifisch zur Veranstaltung, nicht allgemein! Und nur wenn diese Form sinnvoll ist, z.B. Blick auf Alter/Zielgruppe), als Infos zu Fotos in Form eines Türplakates oder bei der Begrüßung auf Großveranstaltungen etc.*
Der Hinweis sollte möglichst ***zeitnah*** sein, offiziell eigentlich VOR der Datenerhebung. Es braucht ***keine Beweispflicht*** für gegebene Datenschutzhinweise!

5 Wenn man keine Daten erheben darf…eine Einwilligung einholen!

Eine Einwilligung der Betroffenen ist **schriftlich** einzuholen. Sie muss **jederzeit widerrufbar** sein und ist **freiwillig** abzugeben.

Form: Entweder geben Personen (bzw. Personensorgeberechtigte) ihr Einverständnis konkret zur Nutzung der Daten für einen bestimmten Zweck durch Bestätigen oder Ablehnen.
Oder es wird beschrieben (separates Blatt oder auf Anmeldung), was mit den Daten im Rahmen einer Anmeldung etc. passiert, die Einwilligung geschieht durch unterschreiben/sich anmelden.

6 Umgang mit Bildern!

Die ***Nutzung „fremder" Bilder*** braucht immer die Zustimmung des/r Urheber*in. Und eigene?

Veröffentlichungen…von Einzelportraits bedürfen grundsätzlich der Einwilligung, außer bei Personen des öffentlichen Interesses (z.B. Pfarrer, Bürgermeister) oder eine Einzelperson ist nur „Beiwerk".
…von Gruppenbildern brauchen ebenfalls die Einwilligung aller abgebildeten Personen, egal wie groß die Gruppe ist. Für „Gruppenbild" gibt es keine klare Definition: Z.B. sind 3 Köpfe eher individuell… 2 Person in einer Handlung eher weniger.

Bei ***allgemeinen Bildern im kirchlichen Zusammenhang*** (z.B. s Gottesdienst-Fotos) braucht es keine Einwilligung, diese dürfen auch im kirchlichen Interesse in kircheneigenen Medien (Homepage, Pfarrbrief etc.) veröffentlicht werden. Darüber ist jedoch in einem Datenschutzhinweis zu informieren.

7 Eigene Rechte kennen – Rechte anderer schützen!

Jeder Mensch hat Rechte bzgl. der ***Darstellung der eigenen Person in der Öffentlichkeit.*** D.h. jeder Mensch hat das Recht auf ***Auskunft***, ***Sperrung*** oder ***Löschung*** der eigenen Daten, dies ist eigenes Recht als Person und Pflicht als Verarbeitender von Daten.
Die ***Grenzen der Persönlichkeitsrechte*** bestehen selbstverständlich da, wo sie Persönlichkeitsrechte anderer einschränken – deshalb gilt es natürlich gleichermaßen, die Rechte andrer zu wahren!

8 Sicherung privater Endgeräte!

Ehrenamt geschieht oft am eigenen Handy und PC – auch hier bitte angemessene Datensicherung:
Zugang zum PC mit einem Passwort sichern. Wer hat alles Zugriff? Ggf. Benutzerkonten einrichten oder Dokumente verschlüsseln.
Passwörter immer wieder neu erstellen, dabei kreativ bleiben und verschiedene nutzen!
Verbindung ins Internet sorgfältig wählen– wenn WLAN, dann abgesichert. Im öffentlichen Raum nur über sichere Verbindungen online gehen.
Mobile Datenträger (Laptops, USB-Sticks, Smartphones usw.) verschlüsseln, damit bei Verlust die Daten nicht in fremde Hände gelangen.
Schutz vor Schad-Software durch angemessene Firewall und Schutz-Software. Besondere Vorsicht bei Mails und deren Anhängen!
Emailadressen fürs Ehrenamt sind im Bestfall passgenau (gemeindeteam@...vorstand @...), oder persönlich (vorname.nachname@...), damit eindeutig ist, wer sie liest. Kritisch sind eher allgemeine Familienadressen.
Mailverteiler und Rundmails mit privaten Mailadressen immer im BCC (blind copy) verdeckt versenden, damit nicht jeder alle Adressen sieht (z.B. Gemeindereferent/in informiert Eltern über Elternabend für Erstkommunion).
Ein offener Verteiler kann bei **Arbeitsgruppen** verwendet werden oder die Einwilligung der Betroffenen, z.B. Eltern, liegt vor.
WhatsApp sammelt nebenbei Daten des Handys… und ist deshalb den kirchlichen Mitarbeitern als Kontaktweg verboten. Alternative wäre Threema.
Eingabe von personenbezogenen Daten, z.B. Login- oder Kontodaten, nur über sichere Verbindungen.
Ausloggen nach einem Login, niemals eine Seite einfach verlassen.

9 Mit offenen Augen durch die Welt!

Jeder verarbeitet heutzutage Daten…angefangen auf dem Handy – bis hin zu Instagram, Bloggs, Facebook etc. Und ***jeder hat Daten zu verbergen***, die nicht jeder kennen muss. Also grundlegend mitdenken und auch mal kritisch nachfragen. Also auch **Protokolle** und sensible Unterlagen nicht offen liegen lassen Zuhause oder bei der Arbeit…

10 Das Datengeheimnis wahren!

Ziel des **Kirchlichen Datenschutz-Gesetzes (KDG)** ist der Schutz von Einzelpersonen und ihrer Daten. Personenbezogene Daten sind vor unbefugter Kenntnisnahme zu schützen, dieser Schutz soll angemessen und verhältnismäßig sein.

Dieser Grundsatz gilt neben den Hauptberuflichen auch für alle Ehrenamtlichen, die regelmäßig personenbezogene Daten verarbeiten: Sie müssen sich in einer kleinen Schulung mit dem Thema auseinandersetzen und sind bei intensivem Datenumgang auf das Datengeheimnis zu verpflichten (Verpflichtungserklärung); diese Verpflichtung besteht auch nach Beendigung der Tätigkeit.

Bei Fragen wenden Sie sich bitte an das Pfarrbüro oder Seelsorgeteam:
*Kirchplatz 9 * 79183 Waldkirch*
Telefon: 07681 7208
Email: buero-waldkirch@ksew.de

10 goldene Regeln für unseren Datenschutz!

1 Wissen, um welche Daten es geht!

Personenbezogene Daten, das sind:
Name, Anschrift, Geburtsdatum/Alter, Mailadresse, Telefonnummern, Kontodaten, Familienstand, Fotos, Kfz-Kennzeichen, Vorstrafen oder Werturteile (z.B. Zeugnisse).
Sensible personenbezogene Daten sind solche zu rassischer oder ethnischer Herkunft, Gesundheitsdaten, politischer Meinung, religiöser oder weltanschaulicher Überzeugung oder Gewerkschaftstätigkeit. Ebenso genetische oder biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten, Daten zu Sexual-leben/ sexueller Orientierung. (Reine Zugehörigkeit zu einer Kirche/ Religionsgemeinschaft gehört nicht dazu.)

„Daten verarbeiten“ bedeutet Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen , Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Abgleichen, Verknüpfen, Löschen, Vernichten…
→Letztendlich ALLES, was man damit macht, egal ob digital oder auf Papier.

Katholische Seelsorgeeinheit Waldkirch
ksew