Praktischer Leitfaden zur Umsetzung der EU-DSGVO

Ziel dieses Dokumentes ist eine vereinfachte Zusammenstellung von To-Do´s, die jeder beim Datenschutz vornehmen sollte, um die EU-DSVGO praktisch umzusetzen und ein gewisses Maß an Rechtssicherheit zu gewährleisten. Hierzu geben wir einen 9-Punkte-Plan an die Hand:

1. Erstelle eine **Datenschutzerklärung** oder überprüfe Deine aktuelle.
2. Passe Deine **Formulare** an, so dass Sie auf die Datenschutzerklärung verweisen.
3. Fasse zusammen, welche **Daten** Du erhebst, und warum. Sammle keine unnötigen Daten.
4. Überlege Dir, wie gut diese Daten **geschützt** sind und wer darauf Zugriff hat.
5. Bedenke die Rechte der **Dateninhaber**. Informiere sie offensiv.
6. Für den Fall, dass Du eine **Homepage** betreibst, passe diese an und schließe entsprechende Verträge ab.
7. **Dokumentiere** Deine Datenschutzmaßnahmen.
8. **Sensibilisiere** alle, die mit diesen Daten arbeiten
9. Überlege Dir, was Du im Falle einer **Datenpanne** tun würdest.

Ein Großteil der Maßnahmen der EU-DSGVO sind ohnehin schon Standard in Deutschland. Auch vor der neuen Verordnung hatten wir das strengste Gesetz innerhalb der EU. Auch da galt der Grundsatz, dass **personenbezogene Daten** nur zweckgebunden gespeichert und verarbeitet werden durften. Die DSGVO schreibt also vor, dass überall da, wo Daten verarbeitet werden, auch erklärt werden muss, zu welchem Zweck **und auf welcher Rechtsgrundlage** dies geschieht und dass man dies ordnungsgemäß dokumentiert.

Neu sind vor allem die erweiterten Sanktionen bei Datenschutzverstößen.

Folgende Punkte sind umzusetzen:

1) Datenschutzerklärung

Zunächst ist es natürlich notwendig, dass man eine Datenschutzerklärung hat bzw. anpasst. Hierzu gibt es im Internet auch Generatoren, die diese Erstellung vereinfachen. Wer sich der vorhandenen Datenschutzerklärung nicht sicher ist, kann ja im Internet mal eine generieren und die mit der aktuellen vergleichen.

https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/
https://datenschutz-generator.de/

Details, was unbedingt enthalten sein muss, unten in Anhang A.

2) Formulare anpassen

Das betrifft alle Formulare, die personenbezogene Daten enthalten, Homepage, Statuten (ggfs.)
Diese müssen mit dem Verweis auf die Datenschutzerklärung versehen sein.
D.h. also mindestens: Anmeldeformular ergänzen und auf Wunsch mit der Datenschutzerklärung aushändigen

Formulare, die zur **Anmeldung oder zur Anmeldung zu Veranstaltungen** usw. gedacht sind, müssen auf den Datenschutz-Abschnitt der Nutzungsordnung/Satzung o.ä. hinweisen. Das könnte in etwa so lauten:

„Wir erheben diese Daten im Einklang mit der Benutzungsordnung / Satzung unseres Vereins / Chores … und den gesetzlichen Bestimmungen, insbesondere dem Gesetz für den Kirchlichen Datenschutz (KDG), damit Sie unsere Bücherei nutzen / unserem Chor beitreten können. Einzelheiten zum Datenschutz entnehmen Sie bitte der Anlage Datenschutz zur Benutzungsordnung, die wir / unsere Mitarbeiter/innen Ihnen gerne aushändigen.“

Des Weiteren muss in die **Speicherung der Daten** eingewilligt werden:

z.B. „Ich erkläre mein Einverständnis für die Speicherung meiner persönlichen Daten in der EDV und den Unterlagen der XX. Die dort gespeicherten Daten dürfen nur im Zusammenhang meiner Mitgliedschaft verwendet werden."

Am besten weist man auch noch darauf hin, dass die Daten verarbeitet werden („zur Pflege des Mitgliederverzeichnisses sowie zum Einzug der Beiträge" o.ä.).

Grundsätzlich bestehen bereits erteilte Einwilligungen fort (sofern bis dato rechtskonform). Sollten aber bestenfalls binnen 2 Jahren erneuert werden.

3) Welche Daten werden erhoben und warum?

Zur Sensibilisierung: Jede Neu-Anmeldung ist eine Datenverarbeitung sowie jede Kontaktaufnahme bzgl. Informationen oder Beiträgen (Mahnung). Eine Mitgliedsnummer ist eine Identifikation usw. Jeder Notizzettel, auf dem persönliche Daten notiert werden. Der Aufruf einer Webseite ebenfalls!

Personenbezogene Daten:

Name, Anschrift, Geburtsdatum, Bankdaten, Telefonnummer, Mitgliedsnummer, IP-Adresse, Familienstand und -zugehörigkeit, Religionszugehörigkeit, Aufenthaltsstatus, Erkrankungen, Status als Schüler, Student, Auszubildender, Beruf oder die Information, dass sich jemand an einem bestimmten Ort aufhält oder Mitglied in einem Verein ist usw.

Sofern diese Informationen nicht von selbst mitgeteilt werden, geht sie einfach niemanden etwas an. Dies ist grundsätzlich. Bei einigen Daten ist es uns sofort einsichtig. Bei den anderen sollten wir es einfach aus Respekt vor der Rechtslage und dem Inhaber der Daten einsehen.

Stellen Sie sich kurz vor, wie es wäre, morgens im Büro alle diese Daten über sich selbst an die Wand gepinnt vorzufinden (selbst wenn ein Großteil den Anwesenden ohnehin bekannt wäre). Wie würden Sie das empfinden? Wie einen Steckbrief? Ein „Profil"?

Jede Organisation müsste kurz zusammenfassen, welche **Informationen** man speichert, in welcher Form, wozu usw.: Also die Anmeldungen in Papierform, digital auf dem Rechner etc. Hat sonst noch jemand ein Verzeichnis? Gibt es einen Email-Verteiler? Welche Daten werden erhoben: Name, Adresse, Telefonnummer, Email, Geburtsdatum…?

Dies alles am besten direkt schriftlich festhalten, man kann es zur Erstellung eines Verfahrensverzeichnisses bzw. zur Dokumentation der Datenschutzorganisation nutzen. (s.u.)

Fotografien:

Wie bei anderen personenbezogenen Daten gilt, dass ein vorher (durch Einvernehmen) erteiltes Einverständnis gültig bleibt. Das betrifft also bereits veröffentlichte Fotos. Im Falle eines Widerrufes sind diese natürlich umgehend zu entfernen, sofern man dies gewährleisten kann.

Die vorherige Rechtslage ist selbstredend nicht außer Kraft gesetzt. Wer also bei **einer öffentlichen Veranstaltung** als Zuschauer auftaucht, muss sich nicht wundern, wenn er ggfs. „als Beiwerk" auf einer Fotografie abgelichtet wird. (§ 23 Absatz 1 KunstUrhG)

Auf der ganz sicheren Seite ist man derzeit nur, wenn man sich eine **schriftliche Einverständniserklärung** zu jeder Veranstaltung von jedem Teilnehmer einholt bzw. sich bei einer Mitgliedschaft direkt bei der Anmeldung die Einverständniserklärung hierzu einholt – als Teil des Anmeldeformulars. Gleiches gilt natürlich für Mitarbeiter.

Diese Einwilligung muss **aktiv** erfolgen, ein Nachweis dieser Einwilligung muss vorliegen und es besteht ein Kopplungsverbot, d.h. der Grund / die Art der Veröffentlichung muss genannt sein und kann nicht auf etwas anderes übertragen werden. (z.B. dürfen Fotos für die Homepage nicht einfach

an eine Zeitung weitergereicht werden).

Für Kinder sollte man grundsätzlich eine Einverständniserklärung des Erziehungsberechtigten einholen.

„Die **Verbreitung und öffentliche Schaustellung** – auch in Sozialen Medien – ist hingegen regelmäßig nur zulässig, wenn die Abgebildeten hierin **eingewilligt** haben. Das Recht am eigenen Bild begründet diesen Schutz.

Es gilt: 1. Grundsätzlich dürfen Sie Fotos und Videos erstellen, auf denen auch andere Personen abgebildet sind. Eine Ausnahme gilt hier, wenn diese dem Vorgang **eindeutig** widersprechen.

2. **Ohne die Einwilligung** der abgebildeten Personen, dürfen Fotos und Videos aber weder verbreitet noch öffentlich zur Schau gestellt werden (§ 22 Satz 1 KunstUrhG).

Überflüssige Daten und unnötige Kopien sind zu löschen.

Welche Daten sind überflüssig? („Linkshänder", „Achtung, nervig!" sind keine für die Arbeitsvorgänge relevanten Daten. Wenn ich meine Mitglieder stets in Briefform kontaktiere, gibt es keinen Grund, die Telefonnummer aufzubewahren.)

Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt) …

Die Rechtsgrundlage sollte in den meisten Fällen damit abgedeckt sein, dass die Daten freiwillig zur Verfügung gestellt wurden und dass der Wunsch nach einer Mitgliedschaft und zur Begleichung der Mitgliedsbeiträge etc. bekundet wurde. Im § 6 des KDG finden sich auch noch weitere Begründungen (siehe **Anhang B** bzw. : https://isidor.bistum-muenster.de/zd/Documents/Gesetz-Kirchlicher-Datenschutz-2017.pdf.)

Die wenigsten werden im Falle einer Datenpanne mit den von Ihnen erhobenen Daten Ihre Mitglieder besonders gefährden. Eine Interessenabwägung sollte nicht notwendig sein. Wer natürlich sehr sensible Daten erhebt (Erkrankungen, Religionszugehörigkeit usw.) sollte sich mit diesem Punkt noch einmal auseinandersetzen und überlegen, ob er besondere Maßnahmen ergreifen muss. Dazu sollte man aber doch noch einmal die Meinung eines Juristen hören oder sich an die Datenschutzbeauftragten des Bistums wenden.

„**Nach Art 35 Abs. 1 DSGVO** muss (… prüfen, ob die Verarbeitung der Daten insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat."

4) Analyse, wie mit personenbezogenen Daten umgegangen wird (Werhat Zugriff, wie gespeichert?)

Wird gewährleistet, dass die Daten nur zur Verarbeitung und nur von den befugten Personen genutzt werden? Abgesehen von der rechtlichen Lage sollte man diese Daten wie Betriebsgeheimnisse behandeln, d.h. für Außenstehende unzugänglich und nicht einsichtig.

Sind normalerweise solche Informationen sicher aufbewahrt? Akten sind im Schrank und nicht lose im Regal, und an den Schrank kann nicht jeder. Bei der Bearbeitung kommt es aber auch immer wieder vor, dass ich Notizen mache, oder etwas mit einem Namen oder einer Kennung versehe, weil es für jemanden bestimmt ist.

Da aber auch dies im weitesten Sinne eine Information über diese Person ist, platziere ich diesen Hinweis so, dass er nur für Befugte sichtbar ist. Die Notiz vernichte ich später.

Im alltäglichen Umgang heißt das auch einfach Ordnung halten. Was nicht mehr gebraucht wird, kommt weg. Wenn ich mich von meinem Arbeitsplatz entferne, sorge ich dafür, dass niemand Einblick nehmen kann, ggfs. schließe ich das entsprechende Programm oder sichere den Rechner.

Bei einem Telefonat in öffentlich zugänglichem Raum kann ich auch höflich und prägnant alles besprechen, ohne Mithörern Informationen zuzuspielen.

Es geht hier nicht um die reine Rechtslage, die sollte formal ohnehin eingehalten werden. Es geht darum, ein Gespür dafür zu vertiefen, was alles nur die betroffenen Personen angeht.

Wenn Daten auf einem PC festgehalten sind: Wie ist der gesichert? Werden regelmäßige Updates ausgeführt? Gibt es einen Virenschutz?

Für viele gilt: Die Daten in elektronischer Form liegen auf den Servern des Bistums, vor Ort sind nur Clients. Die Sicherheit der Server ist Angelegenheit des Bistums. Ich muss nur dokumentieren und gewährleisten, dass ich Unbefugten keinen Zugang gewähre.

5) Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten

Wenn das o.g. umgesetzt ist, kommt man ja seinen Pflichten nach. Die in der Datenschutzerklärung erwähnten **Rechte** (s. Anhang A) werden wir wohl gewähren. Man sollte intern am besten noch klären, wer für die Löschung oder Änderung von Daten verantwortlich ist, wenn mehrere Personen beteiligt sind.

Was noch fehlt, ist ein **Löschkonzept** bzw. eine Angabe der Frist, wie lange die Daten aufbewahrt werden. Selbstredend ist es zunächst einmal logisch, dass die Daten für die Dauer der Mitgliedschaft erhoben werden. Der Rest ist nicht haarklein geregelt, jeder sollte einfach überlegen, wie lange er die Daten noch wirklich braucht.

Bei inaktiven Mitgliedern? Umgehend löschen bzw. schreddern oder gibt es Gründe erst noch eine definierte Frist zu setzen? Am besten ist umgehend zu löschen, eine Frist sollte gut begründet sein.

Adressänderung o. ä. müssen umgehend eingepflegt werden (Grundsatz der Richtigkeit), aber daran hat jeder wohl auch ein Eigeninteresse.

6) Homepage anpassen und evt. Verträge über Auftragsverarbeitung schließen

Wer Fragen hat, kann sich die Homepage der St. Maria Magdalena als Orientierung nehmen. Die Datenschutzerklärung kann sicherlich auch als Formulierungshilfe dienen.

Am einfachsten ist es, keine Produkte von **Drittanbietern** wie Google in die Homepage einzubeziehen bzw. zu hinterfragen, ob diese wirklich einen Nutzen haben.

Für alle noch einmal zusammengefasst:

Jede **Internetseite**, auf der Daten aufgenommen werden, muss diverse **Kriterien** erfüllen:

1. Eine **IP-Adresse** ist quasi der Fingerabdruck des eigenen Computers. Laut Gerichtsurteil ist diese zu den personenbezogenen Daten zu zählen. Die Transparenzpflicht verlangt von Webseitenbetreibern, ausdrücklich darauf hinzuweisen, dass hier Daten ausgetauscht werden (mit Verweis auf § 6 EU-DSGVO).

2. Wer ein **Kontaktformular** hat, über das man angeschrieben werden kann, lässt sich hierüber persönliche Daten zusenden.

3. Wer **Google Maps** bei sich auf der Seite hat, um besser gefunden zu werden, oder andere Angebote von Google nutzt, nimmt auch hier Nutzungsdaten auf und übersendet diese automatisch an Google. Dies gilt auch für andere in die Homepage einbezogenen Produkte von Google.

4. Jede Internetseite, die Daten austauscht, muss mit einer **SSL-Verschlüsselung** versehen sein. Wer oben in seinem Browser „https“ am Anfang stehen hat, kann diesen Punkt als abgehakt betrachten.

5. Jeder muss darauf hinweisen, dass **Cookies** verwendet werden (am einfachsten als Checkbox, man hat sonst stetig das Banner im Bild, wenn man nicht bestätigt).

6. **Bestehender Inhalt einer Website** (Fotos des letzten Festes etc.) darf theoretisch auch erst einmal drin bleiben, aber auch das wird diskutiert. Es ist nicht sicher, wie das mit zukünftigen Beiträgen aussieht. Am besten holt man sich für jede Person, die auf einem Foto zu sehen ist, eine Einverständniserklärung ein.

7. Die **Dienstleistungsbeziehungen** für eine Homepage (Verträge über eine Auftragsdatenverarbeitung) sollten geregelt und somit dokumentiert sein. Das betrifft z.B. Google, aber auch den Provider, über den die Homepage läuft. Bei Google gilt das für jeden Dienst, den man nutzt, GoogleMaps, Googleanalytics usw. Zu jedem dieser Dienste muss dann auch entsprechend auf der Homepage etwas in der Datenschutzerklärung stehen.

   Es muss ein Vertrag zur Auftragsverarbeitung geschlossen werden. Die (meisten) Provider haben entsprechende Formulare zum Download vorbereitet oder schicken sie auf Anfrage zu.
   Bei dieser Gelegenheit kann man auch gleich erfragen, wie lange diese Daten aufbewahrt werden, denn auch darüber muss man Auskunft geben.

Es folgen noch die Maßnahmen, die sich auf die Dokumentationspflichten beziehen. Diese Punkte sind zwar intern, aber auf Verlangen dem Datenschutzbeauftragten oder der Aufsichtsbehörde vorzulegen.

7) Verfahrensverzeichnis (inkl. dazu gehöriger Rechtsgrundlage)

Hier fasst man schriftlich noch einmal zusammen und systematisiert, was man sich erarbeitet hat. Auch hierzu gibt es Vorlagen. Sonst reicht z.B. eine einfache excel-Tabelle.

Folgendes muss enthalten sein:
„Verzeichnis der Verarbeitungstätigkeiten
Namen und Kontaktdaten des Verantwortlichen
Name und Anschrift der Institution
Ansprechpartner
Datenschutzbeauftragter
Verarbeitungstätigkeiten: in jedem Fall "Mitgliederverwaltung"; ...
Kategorien der betroffenen Personen: Nutzer, Mitglieder usw.
Kategorien personenbezogener Daten: Name, Telefonnummer usw.
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden:
z.B. Verbände, Versicherungsgesellschaften, Sozialversicherungsträger usw.
Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien:
z. B. Aufbewahrungsfrist für Zuwendungsbestätigungen“

8) Mitarbeiter informieren und sensibilisieren

Der beste Umgang mit personenbezogenen Daten wird natürlich durch eine entsprechende Information der Mitarbeiter gewährleistet. Nur wer sich der Rechtslage und der Bedeutung von Daten bewusst ist, kann mit dem entsprechenden Feingefühl agieren.

"Die Personen, die mit der Datenverarbeitung befasst sind, müssen auf das Datengeheimnis verpflichtet werden. Dazu sollte jeder ein entsprechendes Merkblatt vorbereiten und per Unterschrift bestätigen lassen."

Also: das Thema mindestens in einer Teamsitzung besprechen, eine Verschwiegenheitserklärung entsprechend unterschreiben lassen und im Zweifel bezüglich Schulungen nachfragen.

9) Datenpanne

Ggfs. dem Datenschutzbeauftragten melden, Betroffene informieren, die Sicherheitslücke schließen.

ANHANG A

Grundsätzlich muss man über Folgendes in der Erklärung (auch auf der Homepage) informieren:

- Wer ist der/die Verantwortliche/r? - Kontaktdaten
- Wer ist der/die Datenschutzbeauftragte/r? - Kontaktdaten (Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht werden.)
- Zweck der Datenverarbeitung
- Rechtsgrundlage
- Werden persönliche Daten weitergegeben?
- Wie lange werden diese Daten gespeichert?
- Betroffenenrechte (Auskunftsrecht, Recht auf Berichtigung und Löschung)
- Widerrufsrecht
- Beschwerderecht
  (z.B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS- GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).

ANHANG B

Grundlage: **§ 6 KDG (1):** Rechtmäßigkeit der Verarbeitung personenbezogener Daten:

„… b) die betroffene Person [also der- oder diejenige, die personenbezogene Daten angeben muss] hat in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt;

c) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; …"