Datenschutz

Mit diesem Arbeitsblatt wollen wir euch einen Überblick über das Thema Datenschutz verschaffen. Dies stellt keine rechtliche Beratung dar und dient lediglich einer reinen Infoweitergabe.

1. Grundlegendes & Definition von Begriffen

Ziel der Datenschutzregelungen ist es, dass jeder und jede weiß, was mir ihren oder seinen Daten passiert und, dass diese geschützt sind.

Datenschutz kümmert sich um alle Daten, mit denen in irgendeiner Art und Weise gearbeitet wird (z.B. erhoben, gespeichert, weitergegeben, etc.) und diese Arbeit automatisiert und organisiert (digital und analog) ist.
Für uns gelten die **EU-DSGVO** (= Europäische Datenschutzgrundverordnung und das **KDG** (= Gesetz über den kirchlichen Datenschutz). Diese beiden Gesetze gehen konform miteinander, allerdings ist das KDG strengere Regelungen als die DSGVO bereit, an welche wir uns als Verband in der kirchlichen Jugendarbeit halten müssen. Dies bringt teilweise einen erhöhten Arbeitsaufwand mit sich (z.B. schriftliche Einwilligungen), hat aber auch Chancen und Vorteile, bspw. die Diözese (über das DPSG Diözesanbüro) als Ansprechpartner mit deren Datenschutzbeauftragten sowie geringe Strafzahlungen im Fall der Fälle.

Für die Umsetzung des Datenschutzes ist der jeweilige Verantwortliche zuständig.

Grundsätzlich gilt beim Datenschutz, dass Verarbeitungsverbot. D.h. Datenschutz ist ein sogenanntes „Verbot mit Erlaubnisvorbehalten“ was so viel heißt wie, alles ist verboten, außer es ist ausdrücklich erlaubt! Dabei hilft die **3-E Regel**:
Rechtmäßiger Datenverarbeitung geschieht auf Grundlage von

1. Gesetzlicher **Erlaubnis** oder

d.h. wenn es im Gesetz geregelt ist.

2. Einer **Erforderlichkeit** oder

d.h. wenn es notwendig ist. Beispielsweise dürfen die Daten, welche bei der Mitgliedschaft zur DPSG abgegeben werden, wie Name, Anschrift, Mailadresse genutzt werden, wenn es im Sinne des Verbandes und erforderlich ist, z.B. für den Versand von Einladungen zu Aktionen. Aber Achtung: Datensparsamkeit!

3. Einer **Einwilligung**

d.h. wenn 1. Und 2. Nicht greifen, dann brauche ich eine Einwilligung.

Die Datenschutzgesetzte folgen bestimmten **Grundprinzipien**:

- **Transparenz**: Die Datenverarbeitung soll nachvollziehbar sein und jeder hat das Recht seine Daten zu prüfen.
- **Zweckbindung & Erforderlichkeit**: Die Erhebung muss einen festgelegten Zweck haben und ist auch nur für diesen Zweck zu verwenden – keine Sammlung auf Vorrat.
- **Datenminimierung /-sparsamkeit:** Nur die Daten, die erforderlich sind abfragen.

Ihr braucht nicht wissen, ob jemand Schwimmer oder Nicht-Schwimmer ist, wenn ihr im Zeltlager keinen Schwimmbadbesuch plant oder die Teilnehmenden anderweitig (bei Programmpunkten wie Wasserspielen) schwimmen können müssen.

- **Verhältnismäßigkeitsgrundsatz**: Personenbezogene Daten nur abfragen, wenn sie benötigt werden.
- **Richtigkeit**: Personenbezogene Daten müssen sachlich richtig bearbeitet und auch gelöscht werden
- **Integrität & Vertraulichkeit:** Personenbezogene Daten müssen durch geeignete Maßnahmen gesichert werden und man ist zukünftig verpflichtet Verletzungen zu veröffentlichen.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Zum Beispiel: Name, Anschrift, Familienstand, Telefonnummer, Mailadresse, Beruf, Mitgliedschaft, Interessen.

monika.hofer@bistum-regensburg.de ist personenbezogen, da aus dieser Mailadresse hervorgeht, wem sie gehört. buero@dpsg-regensburg.de ist nicht personenbezogen, da keine Person dahinter identifizierbar ist.

Besonders schutzbedürftig sind personenbezogene Daten, wenn folgende Kategorien ersichtlich sind:

- Rassistische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugen
- Gewerkschaftszugehörigkeit
- Verarbeitung von genetischen oder biometrischen Daten
- Gesundheitsdaten
- Daten zum Sexualleben und der sexuellen Orientierung einer natürlichen Person

Bei der Sicherung und Schutz von Daten kann die **3-Z Regel** weiterhelfen. Diese weißt auf technische und organisatorische Maßnahmen zur Sicherung von Daten hin:

1. Zutritt zu den Räumlichkeiten

d.h. wer hat Zugang zu den Räumlichkeiten, wer hat einen Schlüssel zum Gruppenzimmer, ist die Tür verschlossen, gibt es überhaupt die Möglichkeit zuzuschließen?

2. Zugang zu den Datenverarbeitungsanlagen

d.h. wer hat Zugang auf den PC / zum Schrank mit Zeltlageranmeldungen, ist dieser mit einem Passwort geschützt?

3. Zugriff auf gespeicherte Daten

d.h. wer hat auf was genau Zugriff?

Diese Fragen werden im **Verzeichnis von Verarbeitungstätigkeiten** geregelt, welches benötigt wird, wenn man mit Daten arbeitet.

Ein **Datenschutzbeauftragter** wird benötigt, wenn mind. 10 Personen ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind.

Sinnvoll ist es, wenn darauf geachtet wird, dass so wenige Personen wie möglich Zugriff auf Daten haben, dann erübrigt sich ein Datenschutzbeauftragter für die Stämme oder Bezirke von selbst. Wichtig: Nami-Zugänge vor Ort klären! Sinnvoll ist eine Person, welche Namibeauftragter vor Ort ist und / oder jemand, der Anmeldungen zentral verwaltet.

Wenn weniger als 10 Personen damit beschäftigt sind, wird kein Datenschutzbeauftragter benötigt. Dennoch benötigen alle Personen, welche mit Daten arbeiten eine **Unterweisung sowie schriftliche Einwilligung** zum Umgang mit Daten.

Wenn Daten an externe Stellen weitergegeben werden, dann müssten bestimmte Verträge (Vereinbarung zur Auftragsdatenverarbeitung) geschlossen werden. Dies ist der Fall beispielsweise bei gehosteten Websites. Eine interne Weitergabe in der DPSG (bspw. zwischen den Ebenen) ist im Sinne des Verbandszweckes (siehe Satzung und Ordnung) gültig.

Wichtig: Wenn die Weitergabe im Sinne des Verbandszeckes geschieht, beispielsweise bei AEJ oder JBM Anträgen, dann entfällt diese Vereinbarung bzw. Einwilligung der Teilnehmenden, dass ihre Daten weitergegeben werden! AEJ und JBM Anträge dienen der Finanzierung des Verbandes und sind somit im Sinne und zum Zweck des Verbandes.

Außerdem sollte auch hier auf Datensparsamkeit geachtet werden. Nur Daten weitergeben, die wirklich benötigt werden.
Wenn ihr Daten an externe Stellen weitergebt, welche nicht im Sinne des Verbandszweckes sind, dann benötigt ihr dafür die schriftliche Einwilligung der jeweiligen Personen.

2. Ausgewählte Themenbereiche & Aufgabenfelder

Mails:
Mails sollten in Blindkopie versendet werden, wenn es sich um keine geschlossene Gruppe handelt, an welche die Mail geht. Dies ist der Fall bei Sammelmails mit gleichem Inhalt an viele Personen.

Beispiel: Einladung zu Sitzungen, Veranstaltungen sollten in Blindkopie verschickt werden, da die anderen Teilnehmenden die Mailadressen der restlichen Teilnehmenden nicht wissen dürfen (Mailadressen sind personenbezogene Daten!). Ausnahme sind geschlossene Gruppen, welche untereinander kommunizieren.

Facebook & Instagram:
Eigentlich derzeit keine Nutzung laut dem Kirchlichen Datenschutzgesetz. Da die Öffentlichkeitsarbeit ein wichtiger Bestandteil ist, sollte ein sinnvoller Umgang damit gepflegt werden (d.h. Persönlichkeitsrechte achten, Bildrechte im Blick haben, vertretbaren Inhalt posten). Außerdem sollt das Impressum aktualisiert werden und klare Verantwortliche für den Inhalt benannt werden Ungenutzte Seiten und Gruppen löschen.

Whatsapp:
Eigentlich derzeit keine Nutzung laut dem Kirchlichen Datenschutzgesetzt. Egal ob dies Ehren- oder Hauptamtliche nutzen, wenn der Messenger zur Arbeit im Verband genutzt wird, gelten Datenschutzregeln. Grund des Verbotes ist, dass das Unternehmen (aufgrund seines Sitzes) nicht nach gültigen EU-Datenschutzrichtlinien arbeitet. Wichtige Daten sollten hier drüber nie verschickt werden, wie Bankverbindungen, Anmeldungen, etc.

Hinweis: Es gibt auch viele alternative Messengerdienste, wie beispielsweise Threema, Wire, Freemessage, Signal, Telegram, Signal,…

Dropbox:
Ist derzeit kein gültiger Onlinespeicher, da der Betreiber seinen Sitz nicht in Europa hat (siehe Whatsapp).

Hinweis: Es gibt auch viele alternative Onlinespeicher, wie Owncloud, Angebote von Telefondienstanbietern,

Homepage:
Für die Homepages werden ein Datenschutzkonzept und ein aktuelles Impressum benötigt. Dies müssen zwei separate Seiten sein, das Konzept kann nicht in das Impressum eingearbeitet sein.
Außerdem sollen eine verschlüsselte Übertragung (SSL) sowie der Hinweis auf Cookies, z.B. bei der Nutzung von Google Analytics, etc. vorhanden sein.

Hinweis: Wenn ihr externes Material auf der Homepage habt, wie Youtube Videos, Google Maps, Facebook oder Instagram Buttons, dann müssen diese im Datenschutzkonzept auftauchen! Gleiches gilt für Kontaktformulare, Newsletter, Cookies, Werbung, etc.

Mitgliedsantrag:
Der Mitgliedsantrag der DPSG wurde von der Bundesebene überarbeitet und kann auf deren Homepage runtergeladen werden.

Anmeldungen:
Bei Anmeldungen zu Veranstaltungen soll drauf hingewiesen werden, dass Daten erhoben, verarbeitet, gespeichert und zum Zwecke XY genutzt und ggf. weitergegeben werden. Es wird dazu eine Unterschrift der erziehungsberechtigten oder volljährigen Person benötigt. Dies muss schriftlich passieren und ihr als Stamm benötigt das Original.
Ein online Anmeldesystem funktioniert soweit, wenn irgendwann vor Veranstaltungsbeginn diese Unterschrift eingeholt wird. Dies kann beispielsweise durch eine vorab Infomail geschehen an die tatsächlich angemeldeten Teilnehmenden.
Außerdem soll jeder nur die nötigen Teile einer Anmeldeliste wissen, die benötigt werden (Datenerforderlichkeit – und sparksamkeit). Anmeldelisten sollten nie offen rumliegen! Anmeldeabschnitte sollten nach Veranstaltungsende vernichtet werden.

Beispiel: Das Küchenteam benötigt die Anzahl an Vegetariern oder vorhandene Allergien (Gesundheitsdaten!), aber nicht, wer genau vegetarisch isst. Die Referenten, welche vor Ort einen Schnitzworkshop abhalten müssen dies nicht wissen. Der Kassier benötigt die Bankverbindungen der Teilnehmenden, welche allerdings das Küchenteam und der Referent nicht wissen müssen. Den Überblick der Teilnehmendenliste erhält sinnvollerweise eine Person, bspw. die Lagerleitung.

Bilder:
Bilder zählen zu den personenbezogenen Daten. Es sind keine Pauschalabfragen bei der Verwendung von Bildern möglich, sondern müssen anlassbezogen sein, d.h. für das Zeltlager und das Hüttenwochenende werden separate Bildabfragen benötigt. Es ist nicht notwendig, jedes einzelne Bild abzufragen! Dafür wird vor Veranstaltungsbeginn eine schriftliche Einwilligung von den erziehungsberichtigten bzw. volljährigen Personen erfasst (siehe Anmeldungen). Kinder ab 12 Jahren müssen zusätzlich selbst zustimmen. Eine Vorlage findet ihr dazu auf der Bundeshomepage.
Eine Einwilligung bedarf es einer separaten Unterschrift und kann nicht mit einer Unterschrift zur Zustimmung von AGBs oder der Anmeldung kombiniert werden.
Ausnahmen:

- Personen sind nur Beiwerk.
- Teilnahme an öffentlichen Veranstaltungen, die Person darf nicht hervorgehoben werden.
- Personen der Zeitgeschichte.

Wichtig: Achtet grundsätzlich darauf keine peinlichen, ordinären oder sonstige Fotos zu schießen bzw. zu veröffentlichen, welche den abgelichteten Personen peinlich sein könnten.

Letzter Hinweis zum Schluss:
Seht das Datenschutzgesetzt und die damit verbundenen Aufgaben nicht als Last oder Ärger. Es soll den Einzelnen schützen! Geht mit Herz und Verstand an das Thema heran und beachtet grundsätzlich die Persönlichkeitsrechte jedes einzelnen, dann ist der Großteil bereits abgedeckt.

Weiter Links mit Vorlagen oder Tipps unter:
https://dpsg.de/de/fuer-mitglieder/datenschutz-heute.html
https://www.bjr.de/nc/service/neuigkeiten/details/datenschutz-in-der-jugendarbeit-2062.html