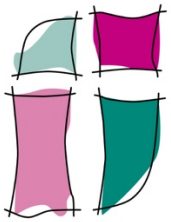

# Erklärungen
# zur
# Datenschutzordnung

**des Mülheimer Verbandes**
**Freikirchlich-Evangelischer Gemeinden e.V. (MV)**

3. Mai 2018

# Inhaltsverzeichnis

# 1. Vorbemerkungen zur Rechtslage

Die EU-Datenschutzgrundverordnung (EU) 2016/679 (DS-GVO) hat ab dem 25.05.2018 unmittelbare Rechtsgeltung in der Europäischen Union (Art. 99 (2) 2 DS-GVO) und damit auch in Deutschland. Sie genießt anders als die Vorgängerregelung, die EG-Datenschutz-Richtlinie 95/46/EG vom 24.10.1995, Anwendungsvorrang gegenüber dem nationalen Bundesdatenschutzgesetz (BDSG). Die Lektüre der DS-GVO ist schwierig, da die 173 Erwägungsgründe (ErwG) integrale Bestandteile der Verordnung sind und nicht nur eine bloße Gesetzesbegründung (Art. 99 (2) 2 DS-GVO: „Diese Verordnung ist in allen ihren Teilen verbindlich." Die Erwägungsgründe sind daher stets zusammen mit den Artikeln zu lesen, auf welche sie sich beziehen.
Die Frage der nun möglichen Sanktionen ist der Faktor, der letztlich alle Unternehmen und auch Vereine aufgeschreckt hat und nun zum Handeln zwingt. Es geht damit nicht nur um mögliche Abmahnungen, wenn Webseiten nicht den gesetzlichen Vorgaben entsprechen, sondern auch um Bußgelder, die in erheblicher und empfindlicher Höhe (so ist es im Gesetz explizit festgehalten worden) bei Datenschutzverstößen verhängt werden können.

Die DS-GVO ist hier zu finden: www.dsgvo-gesetz.de

Ein nationales Ergänzungsgesetz (DSAnpUG-EU, dieses beinhaltet das BDSG 2018) wird die in der DS-GVO für die Einzelstaaten vorgesehenen Regelungsspielräume nutzen, um den bisherigen Regelungsstand in möglichst vielen Bereichen, etwa bei der Videoüberwachung öffentlicher Räume, dem Beschäftigtendatenschutz oder den Schwellenwerten bei der Bestellung eines Datenschutzbeauftragten, zu erhalten. Das BDSG 2018 tritt zeitgleich mit der DS-GVO am 25.05.2018 in Kraft.
Die Datenschutzkonferenz der Datenschutzbehörden des Bundes und der Länder (DSK) gibt regelmäßig sogenannte Kurzpapiere als erste Orientierung zum Verständnis der DS-GVO heraus.

# 2. Warum eine eigene Datenschutzordnung für den MV?

## 2.1 Kirchliches Selbstbestimmungsrecht gilt auch für den MV

Die gesetzliche Regelung des kirchlichen Selbstbestimmungsrechts findet sich heute in Art. 137 Absatz 3 der Weimarer Reichsverfassung (WRV), der gemäß Art. 140 des Grundgesetzes Bestandteil des Grundgesetzes für die Bundesrepublik Deutschland ist:

> *Jede Religionsgesellschaft ordnet und verwaltet ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes. Sie verleiht ihre Ämter ohne Mitwirkung des Staates oder der bürgerlichen Gemeinde.*

Auf das kirchliche Selbstbestimmungsrecht können sich nicht nur Kirchen berufen, sondern alle Religionsgemeinschaften. Es ist auch keineswegs solchen Religionsgemeinschaften vorbehalten, die als Körperschaft des öffentlichen Rechts anerkannt sind, sondern schützt auch privatrechtlich organisierte Gemeinschaften gleich welcher Religion oder Konfession. Der MV versteht sich als Kirche, handelt als Kirche und ist als Kirche anerkannt (siehe Mitgliedschaft in der VEF und der ACK). Deshalb gilt das kirchliche Selbstbestimmungsrecht auch für den MV.

## 2.2 Kirchen dürfen eigene Regelungen schaffen

Deutschland ist der einzige Mitgliedstaat der Europäischen Union mit einem gesonderten kirchlichen Datenschutzrecht. Kirchen dürfen eigene Datenschutzregelungen schaffen und unterliegen damit auch einer eigenen Datenschutzaufsicht. Das gilt auch zukünftig laut Artikel 91 DSGVO:
Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

(1) *Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.*
(2) *Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.*

Weiterhin ist auch „Erwägungsgrund 165 - Achtung des Status von Kirchen und religiösen Vereinigungen“ zu beachten, wo es heißt:

> *Im Einklang mit Artikel 17 AEUV achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren bestehenden verfassungsrechtlichen Vorschriften genießen, und beeinträchtigt ihn nicht.*

Bestehende kirchliche Datenschutzregelungen dürfen danach „weiter angewandt werden, sofern sie mit der DS-GVO in Einklang gebracht werden“ (Art. 91 (1) DS-GVO), also dem Schutzniveau der DS-GVO ab dem 25.05.2018 in allen wesentlichen Punkten zumindest entsprechen.
Deshalb versuchen fast alle Kirchen, die zur VEF gehören und bisher noch keine Datenschutzordnung hatten, vor dem 25.5.2018 eine eigene Ordnung zu verabschieden. Ehrlicherweise muss man feststellen, dass die EU-Richtlinie schon 2016 in Kraft getreten ist. Demnach wäre das nunmehr eigentlich nicht mehr möglich. Allerdings gibt es dazu unterschiedliche Auffassungen in der VEF und den damit befassten Fachanwälten. Falls es so verstanden werden müsste, dürfte keine Religionsgemeinschaft, die nach 2016 entstanden ist (auch keine KdöR) eine eigene Datenschutzordnung verabschieden. Vermutlich muss diese Frage erst noch durch Rechtsprechung endgültig geklärt werden. Aber in der VEF geht man davon aus, dass es möglich und rechtens ist, eine eigene Ordnung zu verabschieden. Außerdem ist davon auszugehen, dass diese Fragestellung grundsätzlich nicht im Vordergrund steht, sondern das Selbstbestimmungsrecht der Kirchen. Jedenfalls versuchen die VEF-Kirchen, noch vor dem 25.5. ihre eigenen Ordnungen zu verabschieden – wir als MV haben dieses jetzt schon getan.

## 2.3 Vorteile einer eigenen Datenschutzordnung (DO)

In der Hauptsache möchte ich drei Vorteile nennen:

(1) Ein Grundsatz des Datenschutzes ist, im Gegenteil zu anderen Rechtsbereichen: „Alles, was nicht explizit erlaubt ist, ist verboten.“ Kirchen dürfen jedoch an bestimmten Stellen Einfügungen machen, die die (frei)kirchliche Arbeit benötigt. Z.B. bei der Frage der besonderen Kategorien personengebundenen Daten (vgl. §5, Absatz 4 (a) DO des MV oder bei der Frage des Seelsorgegeheimnis und der Amtsverschwiegenheit (vgl. §3 DO des MV).

(2) Eine DO für den gesamten MV bedeutet: Alle Gemeinden handeln nach der gleichen Ordnung und unterliegen der gleichen aufsichtsführenden Stelle. Ansonsten würde für jede Gemeinde des MV die EU-Richtlinie, das BDSG und, nicht zu vergessen, auch noch das jeweilige Landesdatenschutzgesetz gelten. Daraus resultieren von Bundesland zu Bundesland im Detail andere Vorgaben. Meldestelle und Beschwerdestelle wäre jeweils das Landesamt für Datenschutz. Das wollen wir gerne vermeiden.

(3) Ein wichtiger Grund liegt tatsächlich darin, dass das Gesetz den Aufbau einer eigenen aufsichtsführenden Stelle erlaubt (unabhängige Aufsichtsbehörde spezifischer Art). Datenschutzverletzungen inklusive der daraus folgenden Konsequenzen werden somit MV-weit gleich gehandhabt (vgl. §35 DO des MV) und an die MV-Stelle gemeldet, nicht an das sonst zuständige Landesamt für Datenschutz. Falls es tatsächlich zu Sanktionen durch Verhängung von Bußgeldern kommen sollte, würden diese Gelder in der aufsichtsführenden Stelle des MV verbleiben und von dieser genutzt werden (vgl. §§ 35 und 37 DO des MV). Ansonsten würden die Landesämter für Datenschutz diese Bußgelder vereinnahmen.

## 2.4 Geltungsbereich der Datenschutzordnung des MV

Zum Geltungsbereich ist unbedingt §2 DO des MV zur Kenntnis zu nehmen.
Bezüglich der Verantwortlichkeit für die Durchführung des Datenschutzes ist §4 DO des MV zur Kenntnis zu nehmen. Dazu unten weiter unten Punkt 3.1.

## 2.5 Datenschutzbeauftragter des MV

Es ist uns gelungen, einen Datenschutzbeauftragten für den gesamten MV zu finden und zu bestellen. Seine Aufgaben und Befugnisse werden in der DO des MV geregelt: §§33 und 34 DO des MV.
Gleichzeitig haben wir die Regelung zur aufsichtsführenden Stelle vom BFP übernommen: Der Datenschutzbeauftragte des MV ist gleichzeitig auch die aufsichtsführende Stelle des MV (vgl. §35 DO des MV).

# 3. Der nächste Schritt für MV-Gemeinden: „Übernahme!“

Während der Mitgliederversammlung des MV am 19.4.2018 wurde ein Beschluss gefasst, der wie folgt lautet:

(1) Der Vorstand des MV wird damit beauftragt, die MV-Datenschutzordnung zu erstellen, aufgrund der geforderten Gesetze laufend zu aktualisieren und zu beschließen. Der Vorstand informiert alle Mitglieder des MV über die von ihm beschlossene und gegebenenfalls aktualisierte MV-Datenschutzordnung.

(2) Die MV-Datenschutzordnung gilt für den Mülheimer Verband Freikirchlich-Evangelischer Gemeinden e.V. mit seinen Einrichtungen, Arbeitsbereichen, für die von ihm eingesetzte Kommissionen und Beauftragungen, für die Mülheimer Verband Freikirchlich-Evangelischer Gemeinden gGmbH, an der der Verein als Gesellschafter beteiligt ist und für die zu ihm gehörenden Mitglieder (rechtsfähige Gemeinden oder andere juristische Personen) mit deren Einrichtungen und Arbeitsbereichen, soweit Letztere die Übernahme dieser Ordnung gegenüber dem MV in Textform und rechtsverbindlich erklärt haben.

(3) Diese Mitglieder des MV verpflichten sich, zusammen mit dem MV (Verein und gGmbH) die Kosten der Umsetzung der MV-Datenschutzordnung (z.B. Datenschutzbeauftragter, verbundene Reisekosten, notwendige Schulungen, etc.) aufgrund eines durch die Mitgliederversammlung des MV mit einfacher Mehrheit verabschiedeten Umlageschlüssels zu tragen. Dieser wird 2019 erstmalig und rückwirkend für 2018 beschlossen.

(4) Eine Beendigung der Übernahme der Datenschutzordnung des MV durch das Mitglied ist der Geschäftsstelle des MV mit Frist von drei Monaten zum Jahresende anzuzeigen. Alle mit der Übernahme der MV-Datenschutzordnung verbundenen Rechte und Pflichten erlöschen damit.

Der Vorstand hat die Datenschutzordnung erstellt und beschlossen. Diese liegt vor. Nun kann diese, wenn gewollt, seitens der Mitglieder des MV übernommen werden. Dazu ist eine Übernahmeerklärung an den MV notwendig. Ein entsprechendes Formblatt liegt vor, welche alle wichtigen Infos enthält. Eine Übernahme ist allerdings nur möglich, wenn die Frage des „Verantwortlichen für Datenschutz des Mitglieds“ vorher gelöst wurde.

## 3.1 Benennung eines Verantwortlichen für Datenschutz des Mitglieds

Die DO des MV gilt nicht automatisch für alle Mitglieder, sondern nur für die, die eine Übernahme rechtsverbindlich angezeigt haben. ***Vor einer Übernahme ist unbedingt Kapitel 5 der Datenschutzordnung des MV (§§ 28 bis 31 DO des MV) zur Kenntnis zu nehmen und umzusetzen.*** Insbesondere geht es um § 28 Absatz (2) bis (3) DO des MV. Der Verantwortliche für Datenschutz ist somit quasi der „verlängerte Arm“ des Datenschutzbeauftragten des MV. Er nimmt an Schulungen des Datenschutzbeauftragten des MV teil (vermutlich 1x pro Jahr) und gibt der Gemeinde Hilfestellung bei der Umsetzung.

Bisher noch nicht bis ins Detail geklärt ist die Frage, wie Mitglieder des MV, die im Innenverhältnis mehr als eine selbständige Gemeinde haben, mit der Bestellung eines Verantwortlichen für Datenschutz umgehen. Das betrifft hauptsächlich den NWB und den Bezirk Nord-Württemberg. Es gibt mehrere Möglichkeiten:

(1) Es wird ein Verantwortlicher für Datenschutz benannt, dem die verschiedenen verantwortlichen Stellen des Mitglieds zugeordnet werden und die dann als „gemeinsam verantwortliche Stellen“ handeln. Dazu siehe §28 Absatz (4) DO des MV. Vermutlich ist diese Lösung für NWB und Bezirk Nord-Württemberg nicht geeignet.

(2) Es wird ein Verantwortlicher für Datenschutz benannt, der sich in Persona um alle verantwortlichen Stellen des Mitglieds in allen Gemeinden jeweils gesondert kümmert.

(3) Es wird ein Verantwortlicher für Datenschutz des Mitglieds benannt, dem wiederum weitere Verantwortliche in den Gemeinden vor Ort untergeordnet sind. Noch nicht endgültig geklärt ist, welche Person davon der MV-Geschäftsstelle und damit dem Datenschutzbeauftragten des MV gemeldet werden soll. Bisher gehen wir davon aus, dass nur der „Hauptverantwortliche“ des Mitglieds genannt wird. Dieser ist dann aber für die anderen Verantwortlichen des Mitglieds in den Gemeinden mitverantwortlich.

## 3.2 Übernahme der Datenschutzordnung des MV durch das Mitglied

Ein Formular „Übernahmeerklärung“ liegt vor. Alle wichtigen Informationen sind darauf zu finden.
Wichtig ist: Ein Verantwortlicher für Datenschutz des Mitglieds muss benannt werden. Falls keiner benannt werden muss (vgl. §28 Absatz (2 a), ist der Vorstand verantwortlich.
Zu beachten ist, dass pro Jahr Kosten in Höhe von 10-15.000€ (geschätzt) für den Datenschutzbeauftragten des MV und die Umsetzung der aufsichtsführenden Stelle anfallen werden. Genau ist dieses

erst nach einem Jahr zu beziffern. Während der Mitgliederversammlung des MV 2019 wird der Vorstand des MV einen Vorschlag für einen Umlageschlüssel machen (Aufteilung der Kosten auf den MV als Dachverband und auf die Mitglieder, die übernommen haben).
***Die Übernahmeerklärung sollte so schnell wie möglich geschickt werden an Mülheimer Verband FEG e.V., Geschäftsstelle, Habenhauser Dorfstraße 27, 28279 Bremen.***
Eine schnelles Handeln ist insbesondere deshalb notwendig, weil nach der Übernahme sehr schnell der zweite Schritt erfolgen muss, der mit der Aktualisierung aller Homepages aufgrund der Übernahme zu tun hat. Das muss auf jeden Fall noch überall vor dem 25.5.2018 geschehen!

# 4. Der zweite Schritt für MV-Gemeinden: „Schotten dicht!“

Es wird allenthalben befürchtet, dass sich diverse Abmahnanwälte darauf vorbereiten, ab dem 25.5.2018 das Internet nach Webseiten abzuscannen, die nicht den neuen Datenschutzgesetzen entsprechen. Keiner kann genau sagen, wie „schlimm“ es werden wird und inwieweit auch Webseiten von Vereinen betroffen sein werden. Wir sollten deshalb auf jeden Fall unter der Maßgabe „Schotten dicht!“ für den Fall der „Gefahr von außen“ vorbereitet sein.
***Folgende Schritte sollten für alle Webseiten, die betrieben werden, bedacht, vorbereitet und umgesetzt werden:***

(1) Webseiten müssen nicht nur ein Impressum haben, welches von jeder Seite aus zugänglich sein muss, sondern neu ist,
   (a) dass daneben auch eine ***Datenschutzerklärung*** zu finden sein muss. Bitte schon einmal alles soweit vorbereiten, so dass später ganz einfach der entsprechende Text eingepflegt werden kann. Dieser hängt auch sehr davon ab, welche Dienste die Webseite nutzt (Google WebFonts, Tracking, Cookies, Youtube, etc.pp.). Das sollte vorab schon einmal geklärt werden. Im Internet finden sich verschiedene Impressums- und Datenschutzerklärungs-Generatoren, die man nutzen kann. Folgend eine Empfehlungsliste ohne Gewähr:
   e-Recht24.de war bisher immer empfehlenswert. Die Seite ist momentan überlastet und die Datenschutzerklärung ist kostenpflichtig.
   Kostenlos ist activemind.de
   Ebenfalls mein-datenschutzbeauftragter.de
   Wir liefern demnächst die Komponenten bezüglich Datenschutzordnung und Datenschutzbeauftragtem.
   (b) Außerdem sollte die ***DO des MV auf den Webseiten zum Download*** angeboten werden.
   (c) Es muss eine ***Kontaktmöglichkeit zum Datenschutzbeauftragten des MV*** eingebaut werden. Unser Vorschlag ist, dass dieses per Formular umgesetzt wird, nicht nur mit Angabe einer Mailadresse.

***(2) Ich (Dieter Stiefelhagen) arbeite zusammen mit dem Datenschutzbeauftragten des MV daran, ein Merkblatt zu erstellen, welches weitere Umsetzungsinfos für die Websites enthält. Dieses wird so schnell wie möglich zur Verfügung gestellt. Spätestens bis 19.5.2018. Dann bleiben im ungünstigsten Fall noch ein paar Tage Zeit bis zum 24.5. Bitte diesen engen Zeitplan vor Ort unbedingt einplanen und vorbereiten.***

# 5. Weitere Schritte folgen: „Das ist erst der Anfang!“

Es ist tatsächlich so: Das ist erst der Anfang. Die neue EU-Richtlinie und damit auch die DO des MV fordern eine Reihe von konkreten Maßnahmen, die nicht ohne Mühe und Zeitaufwand zu bewältigen sind. Das muss ab dem 25.5. dann Zug um Zug umgesetzt werden. Wie gesagt: Das wird uns allen einiges abverlangen an Zeit, Mühe, Geld und Willen.

## 5.1 Warum ist es wichtig, tatsächlich die weiteren Schritte zu tun?

„Gefahr“ droht nicht nur von außen (Webseiten, die der Öffentlichkeit zugänglich sind), sondern auch durch Datenschutzverletzungen der verantwortlichen Stellen bzw. durch Beschwerden von Betroffenen.

(1) Datenverluste und sonstiges Fehlverhalten müssen gemeldet werden. Geschieht das nicht, können im Entdeckungsfall erhebliche Sanktionen fällig werden (auch der MV muss sich daran halten, weil sonst keine Übereinstimmung mit der EU-Richtlinie besteht).
(2) Betroffene haben Rechte, die unter Umständen sehr schnell und nachweisbar umgesetzt werden müssen. Geschieht das nicht bzw. sind bei der verantwortlichen Stelle noch gar keine Grundlagen dafür geschaffen worden, kann Beschwerde eingereicht werden, die dann ebenfalls in erheblichen Sanktionen münden kann/muss.

## 5.2 Was kommt noch auf uns zu?

Es würde an dieser Stelle zu weit gehen, alle Einzelheiten aufzulisten. Viele Erfordernisse können der DO des MV entnommen werden. Folgend nur ein paar Streiflichter auf immer wiederkehrende Fragestellungen:

***(1) Übernahme des Alt-Datenbestandes***

Das Stichwort „Einholung einer Einwilligung“ taucht immer wieder auf. Wenn kein sonstiger Erlaubnistatbestand für die Erhebung der personengebundenen Daten vorliegt, kann die Datenverarbeitung auch durch eine Einwilligung gerechtfertigt sein (Art. 6 (1) a) DS-GVO). Einwilligung ist aber nicht die einzige Bedingungen für die genehmigte Erhebung von Daten. Vgl. dazu §7 Absatz (1) der DO des MV.

Die DS-GVO sagt, dass Alt-Daten nur genutzt werden dürfen, wenn sie rechtlich erhoben wurden. Das Problem: Wer kann das nach langer Zeit noch nachvollziehen? Deshalb wird die Möglichkeit der Interessenabwägung (§7 Absatz (1 f) DO des MV) vermutlich der Punkt sein, auf den wir uns zumeist beziehen, wenn es um die Übernahme des Alt-Datenbestandes geht. Bei der Interessenabwägung ist auf die „vernünftigen Erwartungen einer betroffenen Person" abzustellen. In der Praxis ist die Wahrung berechtigter Interessen des Verantwortlichen wegen der Unbestimmtheit die am schwierigsten nachzuweisende Rechtsgrundlage, aber trotzdem die, auf die die meisten Datenverarbeitungen gestützt werden. Aber auch für diese Daten gilt: Zweckbindung, Richtigkeit, Speicherlänge.

Unverbindlich will ich schon einmal andeuten, was daraus folgen könnte: Daraufhin wäre nicht die Einholung einer neuen Einwilligung notwendig (mit all den Folgen, die diese mit sich bringt), sondern (nur) eine Information an die betroffenen Personen seitens der speichernden Stelle über die Datennutzung verbunden mit der Mitteilung, dass man davon ausgeht, dass die bisherige Einwilligung dafür weiter besteht. Dem könne man allerdings widersprechen.

Aber das ist bisher nur meine persönliche Einschätzung, die noch nicht abgestimmt ist. Es wird dazu seitens der Geschäftsstelle und des Datenschutzbeauftragten des MV ein Merkblatt zur Verfügung gestellt werden, welches nähere Hinweise geben wird.

***(2) Nutzung von Cloud-Services und IT-Sicherheit***

Dazu wird noch ein Merkblatt seitens der Geschäftsstelle und des Datenschutzbeauftragten des MV zur Verfügung gestellt werden.

Für Cloud-Services gilt: Der Server des Cloud-Dienstes muss in der EU stehen. Dropbox, GoogleDrive, iCloud, etc. sind nach unserem bisherigen Kenntnisstand nicht mehr zulässig, um damit personengebundene Daten zu speichern bzw. zu synchronisieren (wie z.B. Mitgliederverzeichnisse, Freizeiten-Anmeldelisten, Personaldaten, Bewerbungsunterlagen, Mitgliederlisten, Buchführungsdaten, etc.pp). Man sollte sich baldmöglichst nach sicheren und erlaubten Alternativen umsehen. Damit ergibt sich zusätzlich die Chance, einem gegebenenfalls entstandenen „Wildwuchs“ von Speicherung auf unterschiedlichen Computern und Clouddiensten Herr zu werden, der hier und da kaum noch zu überblicken ist. Der MV steigt z.B. auf einen eigenen Serverplatz in Deutschland mit Verwendung von Nextcloud als Dropbox-Ersatz um.

***(3) Verarbeitungsverzeichnisse***

Verarbeitungsverzeichnisse müssen erstellt werden, in denen dokumentiert wird, wer, wann, zu welchem Zweck und wie lange personengebundene Daten speichert. Seitens der Geschäftsstelle und des Datenschutzbeauftragten des MV werden dazu Merkblätter und Formulare angefertigt und zur Verfügung gestellt werden.

Die Erstellung dieser Verzeichnisse wird Zeit benötigen. Deshalb wurde in der DO des MV eine Übergangsregelung eingebaut (vgl. §39 DO des MV). Bis Ende Juni 2019 müssen die Verzeichnisse überall fertig sein.

***(4) Rechte der betroffenen Personen***

Siehe die DO des MV. Zug um Zug werden seitens der Geschäftsstelle und des Datenschutzbeauftragten des MV dazu Merkblätter und Formulare angefertigt und zur Verfügung gestellt.

***(5) Pflichten der verantwortlichen Stellen***

Siehe die DO des MV. Zug um Zug werden seitens der Geschäftsstelle und des Datenschutzbeauftragten des MV dazu Merkblätter und Formulare angefertigt und zur Verfügung gestellt.

***(6) Hilfreiche Internet-Adressen***

(a) Die DS-GVO ist hier zu finden: www.dsgvo-gesetz.de

(b) Die Datenschutzkonferenz der Datenschutzbehörden des Bundes und der Länder (DSK) gibt regelmäßig sogenannte Kurzpapiere als erste Orientierung zum Verständnis der DS-GVO heraus.

(c) Der Digitalverband BITKOM hat einen Leitfaden zur Abfassung des Verarbeitungsverzeichnisses herausgegeben. Auch die Datenschutz-Aufsichtsbehörden stellen hierfür eine Mustervorlage bereit.

***(7) Hilfreiche Literatur***

Wir empfehlen das gut 60seitige Helft:

*Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine – das Sofortmaßnahmen-Paket*

Herausgegeben vom Bayrischen Landesamt für Datenschutzaufsicht
Verlag C.H.Beck, www.beck-shop.de, ISBN: 978-3-406-71662-1, Preis: 5,50€.
Das Heft ist auch als eBook erhältlich.

Wir stimmen nicht in jedem einzelnen Punkt mit allen Aussagen überein. Aber es ist ein preiswertes und verständliches Heft, welches einen guten Überblick und Hilfestellungen beinhaltet.

Dieter Stiefelhagen
Sekretär des Mülheimer Verbandes Freikirchlich-Evangelischer Gemeinden e.V.