

Datenschutz

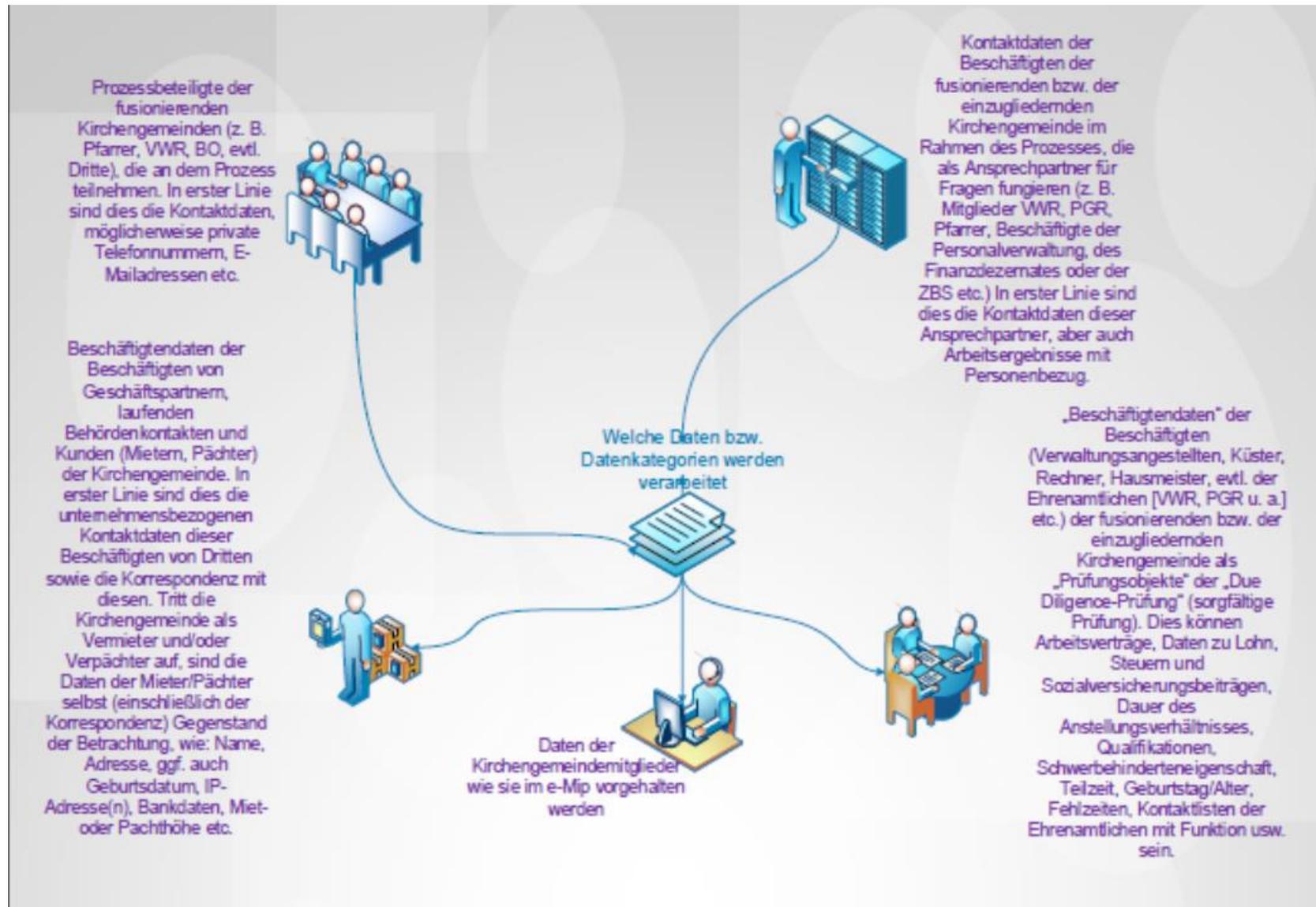
Was ist zu tun?

Grundsätzlich sind im datenschutzrechtlichen Sinne alle Kirchengemeinden zunächst einmal „Verantwortliche“. Dies bedeutet, dass sie jeweils eigenverantwortlich sicherzustellen haben, dass die von ihnen erhobenen, übermittelten oder empfangenen personenbezogenen Daten rechtmäßig verarbeitet wurden bzw. werden.

Welche personenbezogenen Daten werden verarbeitet?

Aus datenschutzrechtlicher Sicht geht es um die Frage, welche Daten (bzw. Datenkategorien) welcher Betroffenen im Zuge eines Fusionsprozesses „verarbeitet“ werden. Dabei spielt es keine Rolle, ob die Daten öffentlich zugänglich sind oder nicht.

Die verarbeiteten Datenkategorien und Betroffenen sind im Wesentlichen folgende:



Jede/r Verantwortliche haftet auch für in der Übermittlungskette „vor“ und „nach“ ihm/ihr begangene Datenschutzverstöße, sofern er/sie nicht alles in seiner/ihrer Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.						
Ziffer	Prozessschritt	Bemerkungen	Realisierung ¹		Wirksamkeitskontrolle ²	
			bis wann	wer	Datum	wer
1	<p>Erstellung einer Übersicht der personenbezogenen Daten und deren Verarbeitung sowie Erstellung und Dokumentation des Verzeichnisses für Verarbeitungstätigkeit (VVT) für Tätigkeiten und Prozesse, bei denen in der Kirchengemeinde personenbezogene Daten erfasst und verarbeitet werden.</p> <p>→ siehe Muster-Datenschutzkonzept der Kirchengemeinden</p> <p>→ Muster VVT der Kirchengemeinden</p> <p>Beides sowie weitere nachfolgend benannte Muster-Dateien finden Sie (zugriffsberechtigt: Leiter, KoordinatorInnen, Verwaltungsleitungen) unter: https://nc.bistum-mainz.de/index.php/s/N7oCw5RSqYcbZAN</p>	<p>Es sollten so wenig wie möglich personenbezogene Daten im Vorfeld des Zusammenschlusses ausgetauscht bzw. offengelegt werden; falls doch notwendig, möglichst anonymisiert, z.B. Anzahl der mitarbeitenden Ehrenamtlichen, Anzahl der Pächter und Mieter und Gesamtmieteinnahmen, ...</p> <ul style="list-style-type: none"> • Liste von PG-Mitgliedern für Bistum (siehe Prozessschritt 2) • MA-Liste für PG Verwaltung, Leiter, MAV, ... (siehe Prozessschritt 3) • Gremienmitglieder über e-Mip geteilt • Kurz vor der Gründung → Info an Geschäftspartner, Firmen, Behörden (siehe Prozessschritte 7 + 8) 				

¹ Umsetzungsplanung durch Gesamtverantwortlichen und durch einzelne Beteiligte

² Controlling durch Gesamtverantwortlichen

Jede/r Verantwortliche haftet auch für in der Übermittlungskette „vor“ und „nach“ ihm/ihr begangene Datenschutzverstöße, sofern er/sie nicht alles in seiner/ihrer Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.						
Ziffer	Prozessschritt	Bemerkungen	Realisierung ³		Wirksamkeitskontrolle ⁴	
2	Einwilligung der prozessbeteiligten Ehrenamtlichen und Hauptberuflichen in die Verarbeitung ihrer personenbezogenen Daten, sofern private Kontaktdaten verwendet werden → siehe Muster Information und Einwilligung Ehrenamtliche →					
3	Information über die Verarbeitung personenbezogener Daten für hauptamtlich Mitarbeitende → siehe Muster Infoschreiben Daten Verwaltungsmitarbeitende für Projektgruppe Verwaltung → siehe Muster Informationsschreiben Mitarbeitende allgemein					

³ Umsetzungsplanung durch Gesamtverantwortlichen und durch einzelne Beteiligte

⁴ Controlling durch Gesamtverantwortlichen

Jede/r Verantwortliche haftet auch für in der Übermittlungskette „vor“ und „nach“ ihm/ihr begangene Datenschutzverstöße, sofern er/sie nicht alles in seiner/ihrer Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.					
Ziffer	Prozessschritt	Bemerkungen	Realisierung ³		Wirksamkeitskontrolle ⁴
4	Prüfung und schriftliche Dokumentation der Rechteverwaltung → siehe Muster Datenschutzkonzept der Kirchengemeinde	Im Vorfeld der Auflösung ist die Rechteverwaltung zu prüfen und schriftlich festzulegen, wer welche Daten sperren, löschen bzw. datenschutzkonform vernichten darf. In diesem Zusammenhang ist die kirchliche Archivordnung strikt einzuhalten. Sollten Dokumente mit personenbezogenen Daten der Vernichtung zugeführt werden, da die Löschfrist erreicht ist oder es sich um Dubletten handelt, sind diese ebenfalls datenschutzkonform zu löschen. Grundsätzlich erfolgen alle Maßnahmen unter Berücksichtigung des KDG und dessen Durchführungsverordnung (KDG-DVO).			
5	Datenschutzkonformer Umgang mit den Kirchenbüchern und sonstigen Archivbüchern (z. B. Protokollbücher des KVR und PGR) auf Grundlage der KAO	Wenn mehrere Pfarreien/Pfarr-Rektorate oder Pfarrkuratien aufgehoben und zu einer neuen Pfarrei vereinigt werden, dann werden die Kirchenbücher/Archivbücher der aufgehobenen Einheiten mit dem Datum der Auflösung geschlossen und von der neuen Pfarrei in datenschutzkonforme Verwahrung genommen. Für die neu errichtete Pfarrei werden neue Kirchenbücher/Archivbücher eröffnet, in die zukünftig alle Handlungen eingetragen werden.			
6	Erstellung und Dokumentation eines Löschkonzeptes → Muster-Löschkonzept (in Arbeit)	Es liegt ein Löschkonzept für die Daten vor, welche auf privaten IT-Systemen (Laptop, Mobilgeräten, ...) zu dienstlichen Zwecken gespeichert sind (vgl. § 20 KDG-DVO). Dies beinhaltet den Zeitpunkt und den/die für die Löschung Verantwortliche/n.			

Jede/r Verantwortliche haftet auch für in der Übermittlungskette „vor“ und „nach“ ihm/ihr begangene Datenschutzverstöße, sofern er/sie nicht alles in seiner/ihrer Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.					
Ziffer	Prozessschritt	Bemerkungen	Realisierung ³		Wirksamkeitskontrolle ⁴
7	Information an die Mitarbeitenden von Geschäftspartnern und Behörden der alten Kirchengemeinde	Da zum Teil konkrete Kontaktdaten von Mitarbeitenden von Fremdfirmen und Dienstleistern (auch private personenbezogene Daten) in Kirchengemeinden vorliegen, sollten diese Fremdfirmen bzw. Dienstleister frühzeitig über eine Neugründung/Fusion informiert werden, so dass diese Firmen ihre Mitarbeitenden informieren können, bevor diese von der neuen Kirchengemeinde kontaktiert werden.			
8	Kunden (Mieter, Pächter, ...) der alten Kirchengemeinde sind zu informieren				
9	Übergabe der vollständigen Datenschutzdokumentation an die neue Kirchengemeinde	Die alte Kirchengemeinde übergibt die vollständige Datenschutzdokumentation (Datenschutzordner) incl. der Verträge zur Auftragsverarbeitung (falls vorhanden) und das Verzeichnis der Verarbeitungstätigkeiten			
10	Datenschutzkonforme Entsorgung bzw. eine datenschutzkonforme Löschung der Festplatten von elektronischen Datenträgern und Papierakten	Nicht mehr benötigte Faxgeräte, Multifunktionsgeräte, IT-Systeme, Kopierer, USB-Sticks, CDs... sind datenschutzkonform zu entsorgen bzw. eine datenschutzkonforme Löschung der Festplatten nach der Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik vorzunehmen. Gleiches gilt für Papierakten, Ordner, Handakten sofern sich nicht ins Archiv nach der Kirchlichen Archivordnung zu verbringen sind.			

Jede/r Verantwortliche haftet auch für in der Übermittlungskette „vor“ und „nach“ ihm/ihr begangene Datenschutzverstöße, sofern er/sie nicht alles in seiner/ihrer Macht Stehende veranlasst, um die Rechtmäßigkeit der Verarbeitung sicherzustellen.					
Ziffer	Prozessschritt	Bemerkungen	Realisierung ³		Wirksamkeitskontrolle ⁴
11	Ggf. Abschluss neuer Verträge zur Auftragsverarbeitung nach § 29 KDG	Die aufnehmende bzw. neue Kirchengemeinde schließt neue Verträge zur Auftragsverarbeitung, wenn nötig, ab und passt das Verzeichnis der Verarbeitungstätigkeiten und das Datenschutzkonzept den neuen Gegebenheiten an.			

Für Rückfragen, wenden sie sich bitte an die

Gemeinsame Betriebliche Datenschutzbeauftragte für die Kirchengemeinden
 Frau Michaela Beiersdorf
 Tel. 06131/253-821, Postfach 1560, 55005 Mainz
 E-Mail: datenschutz@bistum-mainz.de