Psychologische Hochschule Berlin

Datenschutzkonzept für die Befragung von Betroffenen und kirchlichen Funktionsträgern

(einschließlich Datenschutzfolgeabschätzung)

im Rahmen des Forschungsprojekts „Aufarbeitung sexuellen Missbrauchs in der Erzdiözese Bamberg“ (ASMEB)

Inhalt

1 Kurzbeschreibung des Projekts 1

2 Datenschutzbezogene Vereinbarungen im Kooperationsvertrag 2

3 Verantwortliche 3

4 Rechtsgrundlagen der Verarbeitung 4

5 Informationspflicht 4

6 Datengeheimnis 4

7 Sicherung gegen unbefugte Kenntnisnahme 5

8 Anonymisierung und Aufbewahrungsfristen 8

9 Veröffentlichung personenbezogener Forschungsergebnisse 9

10 Datenschutzfolgeabschätzung 10

1 Kurzbeschreibung des Projekts

In der am 22.06.2020 von dem Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) und der Deutschen Bischofskonferenz (DBK) unterzeichneten „Gemeinsamen Erklärung über verbindliche Kriterien für eine unabhängige Aufarbeitung sexuellen Missbrauchs in der katholischen Kirche in Deutschland“ haben sich die Diözesen verpflichtet, den sexuellen Missbrauch im Kontext der katholischen Kirche weiter aufzuklären.

In der Erzdiözese Bamberg (EB) wurde eine unabhängige Kommission zur Aufarbeitung des sexuellen Missbrauchs (UKSM) eingesetzt, die zusammen mit der Universität Greifswald (UG) und der Psychologischen Hochschule Berlin (PHB) in dem Projekt „Aufarbeitung sexuellen Missbrauchs in der Erzdiözese Bamberg“ (ASMEB) das Ziel verfolgt, im Nachgang zur sog. MHG-Studie das quantitative Ausmaß des im Zeitraum von Anfang 1946 bis Ende 2022 durch Kleriker an Kindern, Jugendlichen und Schutzbedürftigen begangenen sexuellen Missbrauchs und den administrativen Umgang mit Betroffenen und Beschuldigten in ihrem Verantwortungsbereich weiter zu ermitteln. Dabei soll neben der notwendigen Analyse der jeweiligen Einzelfälle und der Identifikation von Verantwortlichkeiten und etwaigem Fehlverhalten von Führungspersonal der Erzdiözese ein besonderes Augenmerk vor allem auf der Identifikation übergreifender begünstigender Einflussfaktoren für sexuellen Missbrauch in institutionellen Kontexten, insbesondere der katholischen Kirche, und den Möglichkeiten zu Prävention und Intervention liegen.

Die Ziele der Untersuchung ergeben sich vorrangig aus der Projektskizze, die dem Kooperationsvertrag zwischen den Projektpartnerinnen zugrunde liegt. Diese nimmt Bezug auf die bereits erwähnte „Gemeinsame Erklärung“ und berücksichtigt sowohl die Erkenntnisse der „MHG-Studie“ als auch die bereits laufenden oder schon abgeschlossenen diözesanen Aufarbeitungsprojekte. Der Kooperationsvertrag (KV) regelt die Zusammenarbeit der Kooperationspartnerinnen.

Zur Erreichung der Projekt- und Forschungsziele sind in der PHB Befragungen der Betroffenen und kirchlicher Funktionsträger vorgesehen. Auf diese bezieht sich das vorliegende Datenschutzkonzept. In der UG finden Auswertungen von aktuell geführten oder archivierten Personal-, Bezüge- und Gestellungsakten bereits identifizierter Täter bzw. Beschuldigter statt sowie eine Sichtung und Auswertung aller weiteren relevanten Akten und Unterlagen, die durch die EB und ihre Einrichtungen mit Blick auf die vorab bekannten oder im Verlauf der Studie bekanntgewordenen Täter bzw. Beschuldigten geführt werden oder archiviert sind. Für die Beantwortung der Forschungsfragen findet eine Übermittlung von Datenbeständen von und zur UG statt. Um eine unabhängige Aufklärung ohne jegliche Einflussnahme auf die Ergebnisse des Forschungsprojektes zu gewährleisten, nimmt die UKSM die Aufgaben, Rechte und Pflichten der EB wahr.

In den durch die PHB durchgeführten Befragungen der Betroffenen geht es zum einen um die unmittelbaren und mittelbaren Folgen der Viktimisierung. Zum anderen steht der institutionelle Umgang mit den Betroffenen im Zentrum, wobei insbesondere deren eigene Sicht von großer Bedeutung ist. Beleuchtet werden soll, in welchem Maße und auf welche Weise die zuständigen Personen in der Diözese helfend oder hindernd mit den Betroffenen umgegangen sind. Zudem soll es um die von der Diözese getroffenen Maßnahmen zur Intervention gegen und Prävention von sexuellem Missbrauch gehen.

In den Befragungen der Funktionsträger soll in Ergänzung zu den durch die UG durchgeführten Aktenanalysen der frühere Umgang der EB mit sexuellen Missbrauchsbeschuldigungen erfasst werden. Zudem sollen in diesen Befragungen die konkrete Umsetzung der aktuellen Präventions- und Interventionsmaßnahmen erfasst und der etwaige weitere aktuelle Handlungsbedarf identifiziert werden.

Bei beiden Befragungen geht es um die Konsequenzen, die die Diözese aus den Taten gezogen hat und die Maßnahmen, die gegenüber den Beschuldigten ergriffen wurden. Dabei soll insbesondere auch geprüft werden, ob und ggf. inwieweit, warum und durch wen Beschuldigte geschützt und deren Verhalten verschleiert wurde. Schließlich sollen auch etwaige Beschuldigtennetzwerke und institutionelle Verstrickungen – ggf. auch über die EB hinaus – aufgedeckt werden. Der UKSM Bamberg ist es dabei ein zentrales Anliegen, dass die Studie auch im Einzelnen aufzeigt, welche konkreten und persönlich zu benennenden Personen aus der obersten Leitungsebene des Bistums (Bischöfe, Generalvikare etc.) in welcher Weise in Bezug auf die Behandlung von Fällen sexuellen Missbrauchs durch Kleriker unangemessen bzw. fehlerhaft gehandelt haben, wobei noch lebende Personen der obersten Führungsebene, denen entsprechendes Fehlverhalten zugerechnet werden kann, Gelegenheit zur Stellungnahme erhalten sollen.

2 Datenschutzbezogene Vereinbarungen im Kooperationsvertrag

Gemäß §6 der Kooperationsvereinbarung verpflichten sich die PHB und die UG, für ihre jeweiligen Forschungstätigkeiten Datenschutzkonzepte zu erstellen. Ein Datenschutzkonzept für die Analyse von Akten und Unterlagen im Zuständigkeitsbereich von Einrichtungen der Erzdiözese Bamberg wurde seitens der UG bereits erstellt. Neben dem vorliegenden Datenschutzkonzept für die Befragungen von Betroffenen und kirchlichen Funktionsträgern sind weitere Datenschutzkonzepte für die Analysen von Strafakten und Bundeszentralregisterauszügen durch die UG zu erstellen.

Die Billigung des vorliegenden Datenschutzkonzeptes durch die EB stellt dabei laut §6 Abs. 2 der Kooperationsvereinbarung die Voraussetzung für die Übermittlung personenbezogener Daten dar.

Darüber hinaus enthält die Kooperationsvereinbarung in § 3 Abs. 4 und § 6 Abs. 1 bis 3 bereits weitreichende datenschutzrechtliche Vorgaben, welche im Folgenden wiedergegeben werden:

§3 Durchführung der Arbeiten
(4) Jeder Partner wird die ihm obliegenden Aufgaben in eigener Verantwortung realisieren. Über etwaige Verzögerungen sind die anderen Partner unverzüglich zu unterrichten. Die datenschutzrechtliche Verantwortlichkeit nach der DSGVO bleibt hiervon unberührt. Für Verarbeitungstätigkeiten personenbezogener Daten in gemeinsamer Verantwortlichkeit wird zwischen den betreffenden Partnern eine Vereinbarung nach Art. 26 DSGVO abgeschlossen.

§6 Vertraulichkeit und Publikationen
(1) Für die im Rahmen der Durchführung des vorliegenden Forschungsprojektes vorgesehene Auswertung von (Personal-) Akten und sonstiger Unterlagen sowie die schriftliche und mündliche Befragung von Betroffenen und kirchlichen Funktionsträgern erstellen die UG und die PHB auf der Grundlage

(a) der jeweils gültigen Bestimmungen des Gesetzes über den kirchlichen Datenschutz (KDG),
(b) der Durchführungsverordnung zum Kirchlichen Datenschutzgesetz (KDG-DVO),
(c) der Kirchlichen Archivordnung (KAO),

(d) des Gesetzes über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG),
(e) der Kirchlichen Datenschutzgerichtsordnung (DSGO),
(f) der Normen zur Aufarbeitung von sexuellem Missbrauch Minderjähriger und schutz- und hilfebedürftiger Erwachsener in Bezug auf Personalaktendaten von Klerikern und Kirchenbeamten für die Unabhängige Kommission und für alle wissenschaftlichen oder rechtsanwaltlichen Aufarbeitungsprojekte in der Erzdiözese Bamberg (Amtsblatt für das Erzbistum Bamberg 11/2021 vom 16.12.2021, S. 445-447),
(g) der Ordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- und hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung (Amtsblatt für das Erzbistum Bamberg 3//2024 vom 19.03.2024, S. 74-83),
(h) der jeweils geltenden Fassung der Datenschutzgrundverordnung (DSGVO) und
(i) der ggf. einschlägigen Landesdatenschutzgesetze

ein Datenschutzkonzept sowie einen Ethikantrag (vgl. Ziffer 3 lit. b) aa) Arbeitspaket 1.2 der Projektskizze – S. 7).

(2) Das Datenschutzkonzept und der Ethikantrag werden der EB unverzüglich nach Erstellung zur Prüfung vorgelegt. Die für die Datenerhebung erforderlichen personenbezogenen Daten werden erst dann an die UG und die PHB übermittelt, wenn das Datenschutzkonzept sowie der Ethikantrag von der EB gebilligt wurden und der Ethikantrag von den zuständigen Stellen positiv beschieden wurde.

(3) Die PHB und die UG verpflichten sich, zur Projektdurchführung von der EB übermittelte personenbezogene Daten nach Maßgabe der geltenden Datenschutzbestimmungen und unter Beachtung des im Projekt erstellten Datenschutzkonzeptes vertraulich zu behandeln, insbesondere nur durch berechtigte, zur Verschwiegenheit verpflichtete Personen auswerten zu lassen, sicher zu verwahren, sobald wie möglich zu anonymisieren und nicht mehr für die Projektdurchführung erforderliche, personenbezogene Daten sicher zu vernichten. Hiervon ausgenommen sind Sicherheitskopien und Backups, die sich auf den IT-Systemen der UG und/oder der PHB befinden. Die hiernach von der Löschpflicht ausgenommenen Daten sind so zu sperren, dass ein Zugang zu diesen Daten organisatorisch ausgeschlossen ist. Eine Übermittlung nicht anonymisierter personenbezogener Daten an Dritte findet nicht statt, es sei denn, dies ist im Rahmen der Transkription der Interviews unumgänglich. Auch dann erfolgt eine Übermittlung nur zum Zwecke der Transkription und nur dann, wenn sichergestellt ist, dass der die Transkriptionen durchführende Dritte die geltenden Datenschutzbestimmungen einhält und sich auch zur Einhaltung des im Projekt zu erstellenden Datenschutzkonzepts verpflichtet. Mit dem zur Transkription beauftragten Dritten ist ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zu schließen. Die in diesem Absatz niedergelegten Pflichten gelten auch nach Ende der Projektlaufzeit unbefristet fort. Die Möglichkeit einer Veröffentlichung personenbezogener Daten gemäß Absatz 8 dieser Regelung bleibt unberührt.

3 Verantwortliche

Eigenständig verantwortlich für die Verarbeitung personenbezogener Daten aus Befragungen von Betroffenen und kirchlichen Funktionsträgern, insbesondere auch für deren Offenlegung gegenüber dem Forschungsteam der UG zur Durchführung der genannten Studie ist die Psychologische Hochschule Berlin gGmbH, Am Köllnischen Park 2, 10179 Berlin, Telefon: 030 209166200. Projektverantwortliche innerhalb der PHB ist Prof. Dr. Renate Volbert (Projektleiterin), Psychologische Hochschule Berlin gGmbH, Am Köllnischen Park 2, 10179 Berlin, Telefon: 030 209166-290, Telefax 030 209166-17, E-Mail: r.volbert@phb.de. Datenschutzbeauftragter der PHB ist Marko Walther, Psychologische Hochschule Berlin gGmbH, Am Köllnischen Park 2, 10179 Berlin, Telefon: 030 209166-192, Telefax 030 209166-17, E-Mail: datenschutz@phb.de.

4 Rechtsgrundlagen der Verarbeitung

Die Datenverarbeitung der in den Befragungen von Betroffenen und kirchlichen Funktionsträgern erhobenen Daten erfolgt zum Zweck der eingangs genannten Forschungsfragen. Personenbezogene Daten werden nur nach Einwilligung durch die von der Datenverarbeitung Betroffenen (Art. 6 Abs. 1 lit. a), Art. 9 Abs. 2 lit. a) DSGVO, §27 Abs. 1 BDSG) verarbeitet. Es wird jeweils sowohl eine Einwilligung zur Verarbeitung der Daten im Rahmen der mündlichen und schriftlichen Befragungen eingeholt, als auch für die Zusammenführung der Daten aus den Befragungen mit Daten aus Aktenanalysen.

Insofern zur Erreichung der Forschungsziele Daten aus dem Projektteil der UG genutzt werden, ist das kirchliche Datenschutzgesetz zu berücksichtigen, welches allerdings DSGVO-konform auszugestalten und anzuwenden ist (Art. 91 Abs. 1 DSGVO).

5 Informationspflicht

Die an den Befragungen Teilnehmenden werden nach Art. 13 DSGVO informiert. Das beinhaltet Information zu ihren Auskunftsrechten (Art. 15 DSGVO), ihr Recht auf Berichtigung unrichtiger personenbezogener Daten (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO).

Für die Erfüllung der Informationspflichten von Dritten (in den durchzuführenden Befragungen genannten Beschuldigte, Angehörige etc.) wird auf den Ausnahmetatbestand des Art. 14 Abs. 5 Nr. a) und b) DSGVO verwiesen, der für die Verarbeitung im öffentlichen Interesse liegende wissenschaftliche Zwecke vorbehaltlich der Garantien des Art. 89 Abs. 1 DSGVO Anwendung findet. Für die Betroffenenrechte nach Art. 15, 16, 18 und 21 DSGVO wird auf die Ausnahmevorschrift des §27 Abs. 2 BDSG i.V.m. Art. 89 Abs. 2 DSGVO hingewiesen.

Die entsprechend in den genannten Ausnahmevorschriften geforderten Maßnahmen (z.B. Art 89 Abs. 1 DSGVO i.V.m §22 Abs. 2 BDSG) zur Wahrung der berechtigten Interessen der betroffenen Personen wird ausreichend Rechnung getragen, dokumentiert in den nachfolgenden Ausführungen dieses Datenschutzkonzeptes.

6 Datengeheimnis

Die PHB stellt innerhalb ihres Verantwortlichkeitsbereichs sicher, dass alle mit der Datenverarbeitung befassten Mitarbeitenden die Vertraulichkeit der Daten gemäß den Artikeln 29 und 32 DSGVO sowie § 5 KDG für die Zeit ihrer Tätigkeit sowie auch nach Beendigung des Beschäftigungsverhältnisses wahren. Soweit eine Übermittlung im Rahmen des Projektes zur Erfüllung der Projektziele notwendig ist, geschieht diese Sicherstellung gemeinsam mit der UG. Alle Mitarbeitenden der PHB werden nach der „Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)“ schriftlich verpflichtet. Somit kann das geforderte Datengeheimnis sowohl im Sinne der DSGVO als auch hinsichtlich des § 5 KDG in vollem Umfang gewahrt werden. Auch die UG stellt dies für an sie übermittelte Daten entsprechend sicher. Damit sind die Vorgaben des § 5 Abs. 3 der „Ordnung zur Regelung von Einsichts- und Auskunftsrechten“ und von Abs. 3 der „Normen zur Aufarbeitung“ erfüllt.

7 Sicherung gegen unbefugte Kenntnisnahme

Art. 5 Abs. 1 lit. f DSGVO und § 7 Abs. 1 lit. f KDG legen fest, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen vor unbefugtem Zugriff, Verlust oder Zerstörung zu schützten sind. Art. 32 DSGVO nennt beispielhaft verschiedene Maßnahmen zur Gewährleistung eines ausreichenden Schutzniveaus.

7.1 Kontaktdaten

Alle Kontaktdaten werden getrennt von den Forschungsdaten in einem mit VeraCrypt verschlüsselten Container auf dem PHB-Server gespeichert und nach Abschluss des Forschungsprojekts datenschutzkonform gelöscht. Dazu gehören die durch die UKSM übermittelten Kontaktdaten von bekannten Betroffenen, Kontaktdaten von Betroffenen, die sich bereits eigeninitiativ bei der Projektleiterin gemeldet und ihr Interesse an einer Studienteilnahme bekundet haben, sowie Kontaktdaten, die durch Interviews oder andere Quellen erhalten wurden (bspw. Kontaktdaten von Funktionsträgern).

Sollten die interviewten Personen den Wunsch äußern, auf die veröffentlichten Ergebnisse aufmerksam gemacht zu werden, werden die betreffenden Kontaktdaten notiert und in eine Liste eingetragen. In dieser Liste werden ebenso sämtliche andere Interessenten vermerkt. Die Liste wird vollständig getrennt von den Interviewdaten aufbewahrt, sodass diese nicht mit den Kontaktdaten in Verbindung gebracht werden können. Nachdem interessierte Personen über die Studienergebnisse informiert wurden, wird die Liste mit den Kontaktdaten gelöscht.

7.2 Betroffeneninterviews

Die Betroffeneninterviews werden audioaufgezeichnet und die dadurch aufgenommenen Stimmen der Teilnehmenden gelten zusätzlich zu potenziell vermittelten Inhalten als personenbezogene Daten. Die Audioaufzeichnung erfolgt mittels zweier externer Audioaufnahmegeräte, auf die ausschließlich an der Teilstudie beteiligten Personen Zugriff haben werden. Nach Abschluss des jeweiligen Interviews wird die Audioaufzeichnung umgehend mittels einer Virtual Private Network (VPN)-Verbindung (256 Bit Verschlüsselung) mit Zwei-Faktor-Authentifizierung auf einen von der PHB auf dem PHB-Server bereitgestellten und für die Daten freigegebenen Ordner übertragen und dort mit Hilfe der Verschlüsselungssoftware VeraCrypt verschlüsselt gespeichert. Auf diesen PHB-Server-Ordner können auch die PCs der Mitarbeitenden in der PHB über das interne PHB-Netzwerk zugreifen. Bei VeraCrypt handelt es sich um eine Open-Source-Software zur Datenverschlüsselung. Zwecks verschlüsselter Speicherung wird mittels des AES(Twofish)-Verschlüsselungsalgorithmus und SHA-512-Hash-Algorithmus ein Container erstellt, in dem die Forschungsdaten gesichert werden. Bei der Zwei-Faktor-Authentifizierung erfolgt neben einer Anmeldung am Netzwerk mit einem gesicherten Passwort die Zusendung eines Codes auf ein anderes Endgerät (Smartphone). Die VPN-Verbindung wird auf den passwortgeschützten Laptops der am Teilprojekt beteiligten und interviewenden Mitarbeitenden eingerichtet, so dass die Audiodaten bereits während der interviewbedingten Reisetätigkeit gesichert werden können. Sollte eine Zwei-Faktor-Authentifizierung nicht ausführbar sein, wird die Audioaufzeichnung nach Anschluss des Interviews auf einem passwortgeschützten Laptop der PHB, der von den beiden Interviewerinnen ausschließlich für das Projekt ASMEB genutzt wird, gesichert und dort mit Hilfe der Verschlüsselungssoftware VeraCrypt verschlüsselt temporär gespeichert, bis eine Übertragung auf den PHB-Server-Ordner am PC der jeweiligen Mitarbeitenden in der PHB möglich ist. Diese Übertragung der Audioaufnahme vom Laptop auf den PHB-Server-Ordner erfolgt mittels eines

USB-Sticks am PC der Mitarbeitenden. Die Kopie der Datei auf dem USB-Stick sowie die Datei auf dem Laptop werden direkt nach der erfolgreichen Übertragung mittels der Software „Eraser“ durch mehrfaches Löschen und Überschreiben gelöscht. Lediglich die an der Teilstudie beteiligten Projektmitarbeitenden werden über ihre Laptops und PCs in den Gebäuden der PHB Zugang zu den verschlüsselten Audioaufnahmen haben. Direkt im Anschluss an die überprüfte erfolgreiche Übertragung wird die Audioaufzeichnung von dem externen Audioaufnahmegerät gelöscht.

Für die Auswertung der Interviews müssen die Audioaufnahmen transkribiert werden. Hierzu werden die Audioaufzeichnungen an ein Schreibbüro weitergegeben. Mit dem Schreibbüro wurde ein Auftragsverarbeitungsvertrag (Art. 28 DSGVO) geschlossen. Der Datenaustausch (Audioaufnahmen und Transkripte) mit dem Schreibbüro findet cloudbasiert über HiDrive (SSL256, AES128 verschlüsselt) statt. Dort wird durch das Schreibbüro für das Projekt ein passwortgeschützter Ordner eingerichtet und der zugehörige Link per E-Mail an die Projektmitarbeitenden übersandt. Das Passwort wird telefonisch übermittelt. Die Audioaufnahmen und Transkripte werden jeweils umgehend nach der Transkription bzw. dem Herunterladen aus dem HiDrive-Projekt-Ordner sicher gelöscht. Hierfür wird die Software Eraser verwendet, die sensible Dateien durch mehrfaches Überschreiben unwiderruflich entfernt. Die Mitarbeitenden des Schreibbüros werden zur Verschwiegenheit verpflichtet.

Die Audioaufnahmen der Interviews, welche auf dem Server der PHB verschlüsselt gespeichert wurden, werden direkt nach der Überprüfung der Richtigkeit des Transkripts gelöscht. Während der Datenverarbeitung werden die Transkripte ebenfalls in verschlüsselter Form (VeraCrypt-Container) auf dem Server der PHB gespeichert.

7.3 Schriftliche Befragung von Betroffenen

Alternativ zu den Betroffeneninterviews finden schriftliche Befragungen von Betroffenen mit einem Onlinefragebogen mittels SoSci Survey statt. Auch die im Rahmen dieser schriftlichen Befragung erhobenen Daten sind gegen unbefugten Zugriff gesichert. Eine durchgängige SSL-Verschlüsselung (HTTPS; SSL-Zertifikat mit Extended Validation, EV) schützt die Daten sowohl beim Ausfüllen des Fragebogens als auch beim Abruf der erhobenen Daten. Die SoSci Survey GmbH hat ihren Sitz in München (Deutschland), ebenso wie das Rechenzentrum, welches den Befragungsserver s2survey.net beherbergt. Die Daten werden somit ausschließlich auf Servern innerhalb von Deutschland verarbeitet. Der Server selbst steht im zertifizierten und gesicherten Rechenzentrum des Anbieters M-net Telekommunikations GmbH. Die Verwaltung des Servers erfolgt mittels SSH-Verschlüsselung, die zusätzlich gegen Hackerangriffe gesichert ist.

Zur Nutzung des Pro-Servers der SoSci Survey GmbH, welcher für die Erhebung von personenbezogenen Daten ausgelegt ist, wird eine Lizenz für die Dauer von 12 Monaten mit einer Kapazität von 250 Teilnehmenden erworben. Zusätzlich wird ein Vertrag zur Auftragsdatenverarbeitung (AVV) mit der SoSci Survey GmbH geschlossen.

Für die schriftliche Befragung ist ein Befragungszeitraum von drei Monaten vorgesehen. Nach Abschluss der Befragung werden die erhobenen Daten heruntergeladen und in verschlüsselter Form in dem zuvor bereits beschriebenen, verschlüsselten VeraCrypt-Container auf den Servern der PHB gespeichert. Hier verbleiben die Daten auch während der Datenauswertung. Im Anschluss an das Herunterladen der Daten von den SoSci Survey-Servern werden die Daten bei SoSci Survey gelöscht. Jegliche Sicherheitskopien auf dem Befragungsserver s2survey.net werden nach Löschung der erhobenen Daten durch die Studienleiterin nach Ablauf eines Monats gelöscht.

Für Personen, die nicht auf elektronischem Weg teilnehmen wollen, wird die Möglichkeit angeboten, eine ausgedruckte Version des Fragebogens sowie einen bereits an die PHB rückadressierten und frankierten blickdichten Briefumschlag anzufordern. Die betreffenden Personen werden dabei darauf hingewiesen, dass kein Absender auf dem Rücksendeumschlag vermerkt werden soll, um eine Anonymität zu gewährleisten. Sollte ein Umschlag dennoch mit einem Absender an der PHB eingehen, wird der Umschlag umgehend vernichtet. Die händisch ausgefüllten Fragebögen werden von den Projektmitarbeitenden in SoSci Survey übertragen und nach Kontrolle durch eine zweite Projektmitarbeitende umgehend in der PHB geschreddert und entsorgt.

7.4 Interviews mit Funktionsträgern

Die Verarbeitung der Interviews mit Funktionsträgern erfolgt analog zu der Verarbeitung der Betroffeneninterviews (s. 7.2).

7.5 Übergreifende Speicherung

Alle personenbezogenen Daten werden auf einem eigens für das Forschungsprojekt auf dem PHB-Server eingerichteten Ordner mittels Verschlüsselungssoftware VeraCrypt gespeichert. Zugangsberechtigt zu den VeraCrypt-Containern sind grundsätzlich nur die an der Teilstudie beteiligten Mitarbeitenden. Alle Mitarbeitende des Projektes verpflichten sich dabei darauf, stets nur sichere Passwörter zu verwenden, die den jeweils aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik entsprechen. Zudem werden die Geräte, mit denen der Zugang erfolgt, stets sicher verwahrt, d.h. in abschließbaren Räumlichkeiten oder, soweit eine Mitnahme eines Laptops auf Dienstreisen, z.B. zu Betroffeneninterviews, notwendig ist, im unmittelbaren und ununterbrochenen persönlichen Gewahrsam der jeweiligen Mitarbeitenden. Verlassen Projektmitarbeitende auch nur kurzzeitig ihren Arbeitsplatz, wird stets entweder die Bildschirmsperre aktiviert oder der Computer in den Ruhezustand gefahren bzw. ausgeschaltet und, sofern andere Mitarbeitende nicht mehr im Raum anwesend sind, der Arbeitsraum verschlossen.

Entsprechend sind von informationstechnischer Seite ausreichende Sicherungsmaßnahmen im Sinne der DSGVO und der kirchenrechtlichen Datenschutzbestimmungen gewahrt, sodass eine darüberhinausgehende, spezielle Sicherung der Arbeitsräume in der PHB nicht notwendig ist.

Gemäß Art. 5 Abs. 2 DSGVO muss die Einhaltung der Datenschutzgrundsätze jederzeit nachweisbar sein. Um dies zu gewährleisten, wird ein Verzeichnis von Verarbeitungstätigkeiten (VVT) geführt. Details der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit werden zum Schutz dieser Maßnahmen nicht veröffentlicht.

7.6 Datenaustausch mit der UG

Der mögliche Datenaustausch mit der UG erfolgt zu einem zuvor vereinbarten Zeitpunkt über die NextCloud der UG. Die NextCloud ist ein cloudbasiertes, von der UG auf eigenen Servern gehostetes Speichermedium. Nach Mitteilung des erfolgreichen Uploads durch die PHB übertragen die Projektmitarbeitenden der UG die Daten von der NextCloud auf einen universitäts- und projektinternen Netzwerkordner. Dieser Ordner ist nur nach individueller Freischaltung für Projektmitarbeitende der UG aus dem Netz der UG bzw. via VPN mit einer sicherheitszertifikatsbasierten Identifizierung zugänglich. Die Daten, welche auf der NextCloud gespeichert wurden, sind nach der Übertragung umgehend datenschutzkonform zu löschen. Das Schutzniveau der serverbasierten Datenspeicherung entspricht der Schutzklasse „CRITICAL“. Bei Datenaustausch der UG an die PHB werden die Daten aus der NextCloud in den verschlüsselten VeraCrypt-Container auf dem PHB-Server übertragen.

8 Anonymisierung und Aufbewahrungsfristen

§ 5 Abs. 6 der „Ordnung zur Regelung von Einsichts- und Auskunftsrechten“ und Abs. 5 der „Normen zur Aufarbeitung“ regeln zudem Vorgaben zur Anonymisierung und zu den Aufbewahrungsfristen personenbezogener Daten. § 5 Abs. 6 hat dabei folgenden Wortlaut: „Sobald der Forschungszweck es erlaubt, sind die personenbezogenen Daten vor Offenlegung gegenüber Dritten zu anonymisieren. Solange dies noch nicht möglich ist, sind die Merkmale gesondert aufzubewahren, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert. Sie sind spätestens zwei Jahre nach Erfüllung des Forschungszwecks zu vernichten oder an die (Erz-)Diözese zurückzugeben.“ Die Vorgaben nach Abs. 5 der „Normen zur Aufarbeitung“ haben einen vergleichbaren Inhalt.

Als Maßnahme der Anonymisierung kommt dabei auch eine Pseudonymisierung in Betracht. Eine Pseudonymisierung erhält die Bezüge der Daten zu Personen grundsätzlich aufrecht, entfernt aber alle Merkmale, anhand derer die Personen wirksam reidentifiziert werden können. Eine Pseudonymisierung kann insbesondere dadurch erreicht werden, dass anstelle der Namen von Personen Personennummern eingesetzt werden, mit denen diese Personen ab da in dem Forschungsprojekt benannt werden (also z.B. Beschuldigter 1, Beschuldigter 2, usw.). Zudem werden bei einer Pseudonymisierung alle anderen Daten, die für die Auswertung nicht notwendig sind und zugleich eine schnelle Reidentifizierung der Personen erlauben würden, z.B. konkrete Geburtsdaten oder Geburtsorte, entfernt. Auch Art. 32 Abs. 1 lit. a DSGVO benennt die Pseudonymisierung als wirksame Schutzmaßnahme. Eine solche Pseudonymisierung mit Personenkennziffern wird auch im vorliegenden Projekt vorgenommen, sobald und soweit der Forschungszweck dies erlaubt.

Die Aufbewahrung nicht pseudonymisierter bzw. anonymisierter Daten wird für die gesamte Dauer des Forschungsprojektes erforderlich sein. Dies ist zum einen darauf zurückzuführen, dass im Rahmen des Projektes eine Verknüpfung der Forschungsergebnisse zwischen den Betroffenenbefragungen und denen von Funktionsträgern nötig ist. Zusätzlich ist eine Verknüpfung der Befragungen, die von der PHB verantwortet werden, und der Aktenauswertungen, die von der UG verantwortet werden, zwingend notwendig. Dies ist mit pseudonymisierten bzw. anonymisierten Daten nicht möglich.

Um der Vorgabe der gesonderten Aufbewahrung der personenbezogenen Daten Rechnung zu tragen, wird eine Referenzliste erstellt, in der den Pseudonymen der jeweiligen Personen (Betroffene, Beschuldigte und zuständige Mitarbeitende der EB) die Klarnamen zugeordnet werden. Über diese Referenzliste können die notwendigen Verknüpfungen zwischen den Betroffenenbefragungen und für den Datenaustausch zwischen PHB und UG hergestellt werden. Bei der eigentlichen qualitativen und quantitativen Datenanalyse der Befragungen der Betroffenen und von Funktionsträgern werden im Übrigen nur pseudonymisierte Daten verwendet. Eine Ausnahme davon wird nur gemacht, soweit eine Veröffentlichung personenbezogener Daten im Rahmen des Projektes datenschutzrechtlich zulässig und für die Aufarbeitung notwendig ist, z.B. bezogen auf das Projektziel der Identifikation persönlicher Verantwortlichkeiten von Führungspersonen der Erzdiözese (s. unten, Abschnitt „Veröffentlichung personenbezogener Forschungsergebnisse“).

Die Referenzliste wird getrennt von den Kontakt- und Forschungsdaten in einem mit VeraCrypt verschlüsselten Container auf dem PHB-Server gespeichert. Nach Abschluss des Forschungsprojektes (s. unten) wird die Referenzliste mit den enthaltenen Klarnamen gelöscht. Sämtliche pseudonymisierte

Forschungsdaten werden in einem VeraCrypt-Container auf dem Server der PHB archiviert, um gemäß DFG-Richtlinien eine Speicherung der Forschungsdaten von mindestens 10 Jahren zu gewährleisten. Die Server der PHB stehen in den Räumen der PHB. Der Serverraum ist durch eine stets verschlossene Tür vor unbefugten Zutritten geschützt.

Eine Ausnahme von dieser Vernichtungsregelung gilt, wie in § 6 Abs. 3 S. 2 der Kooperationsvereinbarung festgehalten, aus technischen Gründen für Sicherheitskopien und Backups, die sich auf den IT-Systemen der UG und/oder der PHB befinden. Die hiernach von der Löschpflicht ausgenommenen Daten werden so gesperrt, dass ein Zugang zu diesen organisatorisch ausgeschlossen ist.

9 Veröffentlichung personenbezogener Forschungsergebnisse

Im Rahmen des Aufarbeitungsprojektes wird zum Teil auch die Veröffentlichung personenbezogener Daten notwendig sein, insbesondere im Kontext des mit der Erzdiözese Bamberg bzw. der UKSM vereinbarten Projektziels der Identifikation der individuellen Verantwortlichkeiten von Personen der Führungsebene. Für eine solche Veröffentlichung personenbezogener Daten treffen § 5 Abs. 7 und 8 der „Ordnung zur Regelung von Einsichts- und Auskunftsrechten“ und Abs. 6 und 7 der „Normen zur Aufarbeitung“ besondere Regelungen. Danach ist eine solche nicht anonymisierte Veröffentlichung nur zulässig, soweit Personen (und nach Abs. 6 der „Normen zur Aufarbeitung“ auch Ereignisse) der Zeitgeschichte betroffen sind und zudem diese Art der Veröffentlichung für die Aufarbeitung bzw. für den Forschungszweck unerlässlich ist. Soweit eine solche identifizierende Veröffentlichung erfolgt, sind zudem die Persönlichkeitsrechte der genannten Personen zu wahren.

Zu den Personen der Zeitgeschichte im vorstehenden Sinne zählen einerseits die jeweiligen Führungspersonen in der Erzdiözese Bamberg, deren individuelle Verantwortlichkeiten im Umgang mit Missbrauchsfällen im Kontext des Forschungsprojekts rekonstruiert werden. Andererseits können auch Beschuldigte des sexuellen Missbrauchs dann zu Personen der Zeitgeschichte werden, wenn sie aufgrund des Umfangs oder Ausmaßes ihrer Taten exzeptionell hervorstechen, und insbesondere, wenn dies bereits der Öffentlichkeit im Grundsatz bekannt ist, z.B. weil bereits eine identifizierende Berichterstattung über die entsprechenden Personen stattgefunden hat. In beiden Fällen, d. h. bei dem Führungspersonal der Erzdiözese Bamberg und bei den in diesem Sinne identifizierten „Haupttätern“ des sexuellen Missbrauchs in der Erzdiözese Bamberg, besteht auch ein überragendes Interesse der Allgemeinheit an einer nicht anonymisierten Darstellung der Forschungsergebnisse, da ohne diese eine erfolgreiche Aufarbeitung nicht gelingen kann.

Für das Führungspersonal der EB ist noch ergänzend hinzuzufügen, dass eine vollständige Anonymisierung schon faktisch unmöglich ist, weil aus der Einordnung bestimmter Missbrauchsfälle in einen konkreten zeitlichen Zusammenhang unter Darstellung der Entscheidungsprozesse zu diesem Missbrauchsfall im Bereich der Erzdiözese Bamberg stets deutlich werden würde, wer die jeweils beteiligten Führungspersonen waren, denn deren Namen und Amtszeiten sind bereits jetzt öffentlich bekannt.

Die Persönlichkeitsrechte von Personen der Zeitgeschichte werden jedoch auch bei identifizierender Veröffentlichung dadurch im Sinne des § 5 Abs. 8 der „Ordnung zur Regelung von Einsichts- und Auskunftsrechten“ und Abs. 7 der „Normen zur Aufarbeitung“ gewahrt, dass sich die Veröffentlichung

allein auf diejenigen Fakten beschränkt, deren Darstellung für die Aufarbeitung des sexuellen Missbrauchs und eines diesbezüglichen Fehlverhaltens der betreffenden Personen unerlässlich ist. Personenbezogene Daten, die in keinem relevanten Zusammenhang zu dem aufzuarbeitenden Missbrauchsgeschehen stehen, werden daher nicht veröffentlicht.

Formal abgesichert wird die Begrenzung der Veröffentlichung personenbezogener Forschungsergebnisse auf den vorstehend abgesteckten Rahmen dadurch, dass im Kooperationsvertrag in mit der EB bzw. der UKSM, Anhörungs- bzw. Zustimmungserfordernisse der anderen beteiligten Partnerinnen vor Veröffentlichung solcher Ergebnisse vorgesehen sind. Dadurch kann etwaigen Bedenken gegenüber einer datenschutzrechtlichen Zulässigkeit der Veröffentlichung rechtzeitig vor Veröffentlichung Rechnung getragen und die Veröffentlichung, soweit notwendig, angepasst werden.

10 Datenschutzfolgeabschätzung

Im Folgenden wird die Datenschutzfolgeabschätzung nach Art. 35 DSGVO im Rahmen des Forschungsprojekts überblicksartig dargelegt. Eine detaillierte Version der geplanten Verarbeitungsschritte liegt in Form eines Verfahrensverzeichnisses zusammen mit einer detaillierten Darstellung der Datenschutzfolgeabschätzung vor und kann bei berechtigtem Interesse eingesehen werden.

Umfassen soll eine solche Folgeabschätzung nach Art. 35 Abs. 7 DSGVO zumindest diese Aspekte: „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck; eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.“

10.1 Systematische Beschreibung der geplanten Verarbeitungsvorgänge, Zwecke der Verarbeitung und Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

Die in Art. 35 Abs. 7 Nr. 1 und Nr. 2 verlangte „systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen [… und …] Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck“ ist schon vollumfänglich und detailliert unter den vorstehenden Nummern 1 bis 9 des Datenschutzkonzeptes erfolgt.

10.2 Bewertung der Risiken

Da die Verarbeitung der personenbezogenen Daten aus den Befragungen von Betroffenen und Funktionsträgern ein hohes Risiko für die Rechte und Freiheiten der betreffenden Personen zur Folge haben kann, wird vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten vorgenommen. Dabei können entsprechende Risiken nur durch ein unerwünschtes Öffentlich-Werden von Daten eintreten, nicht hingegen bei regulärer

Datenverarbeitung im Einklang mit den oben unter 1. bis 9. dargelegten Voraussetzungen. Insofern werden im Folgenden die Risiken erläutert, welche bei einem unerwünschten Öffentlich-Werden von personenbezogenen Daten eintreten könnten.

Grundsätzlich kann ein unerwünschtes Öffentlich-Werden von im Rahmen des Forschungsprojektes ASMEB erhobenen personenbezogenen Daten gravierende Folgen für die betreffenden Personen haben, da es sich potentiell um höchstpersönliche Informationen, insbesondere auch über die Betroffenheit durch (sexualisierte) Gewalt und Missbrauch bzw. über (mögliches oder erwiesenes) eigenes sexualbezogenes Fehlverhalten handelt. Entsprechend werden für die unterschiedlichen betreffenden Personengruppen nachfolgend mögliche Folgen dargelegt.

10.2.1 Betroffene

Für die Personengruppe der Betroffenen von sexualisierter Gewalt und Missbrauch ist bei unerwünschtem Öffentlich-Werden ihrer personenbezogenen Daten im schlimmsten Fall mit folgenden Beeinträchtigungen zu rechnen:

- Die Betroffenen machen ein weiteres Mal eine Erfahrung der Ohnmacht, da ihnen die Gelegenheit genommen wurde, souverän und selbstbestimmt über ihre Belange zu bestimmen.
- Ein Öffentlich-Werden personenbezogener Daten birgt grundsätzlich die Gefahr von Beschämungen der und Angriffen auf die betroffenen Personen, besonders vor dem Hintergrund der schnellen Verbreitung und Bewertung von Informationen im Bereich der sozialen Medien.
- Auch ist eine Gefährdung der sozialen Beziehungen oder des Arbeitsplatzes etc. der betroffenen Person vorstellbar.
- Psychische sowie körperliche Belastungen und Erkrankungen sind als Folge denkbar.

10.2.2 Funktionsträger, Beschuldigte und sonstige Bedienstete der EB

Darüber hinaus sind auch für die Personengruppen der Funktionsträger, Beschuldigten und sonstigen Bediensteten der EB die Folgen zu betrachten, wenn personenbezogene Daten unerwünscht öffentlich werden.

Es ist insofern zunächst festzuhalten, dass in der Personengruppe der Funktionsträger, Beschuldigten und sonstigen Bediensteten der EB eine kleine Untergruppe von Personen enthalten ist, die als Personen der Zeitgeschichte einzustufen sind. Es handelt sich insofern einerseits um verantwortliches Führungspersonal der EB und die Gruppe der sogenannten Haupttäter. In diesen Fällen ist eine kontrollierte Veröffentlichung von personenbezogenen Daten zum Zwecke der Aufarbeitung und der Darstellung von Verantwortlichkeit vorgesehen. Die dafür nötige Abwägung der betroffenen Interessen und Darstellung der zusätzlichen Schutzmaßnahmen wurde bereits oben unter 9. vorgenommen.

Selbst in der Gruppe der Personen der Zeitgeschichte dürfen jedenfalls nicht alle personenbezogenen Daten öffentlich werden, sondern nur solche mit klarem Bezug zu Fehlverhalten im Kontext von sexuellem Missbrauch in der EB (auch dazu näher unter 9). Alle anderen Beschuldigten und sonstigen Bediensteten der EB haben ein schutzwürdiges Interesse an der Geheimhaltung ihrer personenbezogenen Daten.

Auch in dieser Personengruppe ist mit negativen Folgen zu rechnen, sollten unerwünscht personenbezogene Daten öffentlich werden. Konkret ist dann für diese Personengruppe mit folgenden Beeinträchtigungen zu rechnen:

- Ein Öffentlich-Werden personenbezogener Daten birgt grundsätzlich die Gefahr von verbalen oder gar physischen Angriffen auf beschuldigte Personen oder für das Geschehenlassen sexuellen Missbrauchs verantwortlich gemachte sonstige Bedienstete, besonders vor dem Hintergrund der schnellen Verbreitung und Bewertung von Informationen im Bereich der sozialen Medien.
- Bei nichtbeschuldigten Funktionsträgern und Bediensteten kann das unerwünschte Öffentlich-Werden ihres Namens im Kontext dieser Studie zudem zu falschen Verdächtigungen führen, die vergleichbare Auswirkungen haben können wie vorstehend skizziert, und zudem eine ungerechtfertigte öffentliche Beschämung zur Folge haben können.
- Auch ist eine Gefährdung der sozialen Beziehungen oder des Arbeitsplatzes etc. in beiden Personengruppen vorstellbar.
- Psychische sowie körperliche Belastungen und Erkrankungen sind als Folge denkbar.

10.2.3 Dritte

Schließlich können von einem unerwünschten Öffentlich-Werden personenbezogener Daten auch Dritte betroffen sein, deren Namen in den Interviews benannt werden. Die daraus resultierenden Beeinträchtigungen dürften davon abhängen, ob die Personen dem aufzuarbeitenden Missbrauchsgeschehen nahestehen, z.B. als Angehörige der Betroffenen oder Beschuldigten, oder ohne konkreten Bezug zum Missbrauchsgeschehen in den Akten genannt werden.

Gravierende Beeinträchtigungen durch ein unerwünschtes Öffentlich-Werden sind insbesondere bei Personen zu erwarten, die dem Missbrauchsgeschehen eher nahestehen. Im ungünstigsten Fall können diese Beeinträchtigungen an diejenigen heranreichen, die vorstehend für die Betroffenen, Beschuldigten und sonstigen Bediensteten genannt wurden.

10.3 Abhilfemaßnahmen

Es werden umfangreiche Maßnahmen getroffen, um den erforderlichen Datenschutz zu gewährleisten und so ein unerwünschtes Öffentlich-Werden personenbezogener Daten zu verhindern. Von besonderer Bedeutung sind insofern die unter 7. und 8. in diesem Datenschutzkonzept beschriebenen Maßnahmen. Die aufgeführten datenschutzrechtlichen Maßnahmen werden zudem fortlaufend geprüft, überwacht und dokumentiert. Zu diesem Zweck wird eine gesonderte (digitale) Akte angelegt, in die sämtliche datenschutzrechtlichen Abwägungen und Entscheidungen aufgenommen werden. Dadurch sind die Risiken eines unerwünschten Öffentlich-Werdens personenbezogener Daten als insgesamt gering einzuschätzen.