SANOVIS

CONSULTING WITH CARE.

DATENSCHUTZ-FOLGENABSCHÄTZUNG

SIILO

Dokumentenhistorie

Version	Datum	Beschreibung	Name
0.1	[redacted]	Erstellung der Datenschutz-Folgenabschätzung im Entwurf	[redacted]
0.2	[redacted]	[redacted]	[redacted]

[redacted]

INHALT

Abbildungs- und Tabellenverzeichnis

Gender-Hinweis: Aus Gründen der Lesbarkeit wird in diesem Dokument darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Männer, Frauen und Diverse in gleicher Weise und sind als geschlechtsneutral zu bewerten.

[redacted]

1. Sachverhalt

Durch die Verwendung wird den Ärzte- und Pflegeteams sowie anderen Fachkräften die Möglichkeit eröffnet, ortsunabhängig Dateien sicher auszutauschen. Hierdurch werden insbesondere die Potenziale zur kollaborativen Arbeit erhöht. Gerade in der Corona-Krise zeigt sich, dass eine schnelle Kommunikation in den Krankenhäusern unerlässlich ist. Auch im [redacted] sind die Forderungen nach einer kurzweiligen, ortsunabhängigen Kommunikation im Zuge der Corona-Pandemie größer geworden. Um zusätzlich einem informellen Austausch über Dienste, die nicht den Anforderungen an den Datenschutz und die Datensicherheit genügen, vorzugreifen, plant die [redacted] die Einführung des Messenger-Dienstes der Firma Siilo Holding B.V. (1017 DR Amsterdam).

Die zuvor aufgeführten Anforderungen, werden durch die Messenger-App der Firma Siilo dargestellt. Bei dieser App handelt es sich um eine sichere Plattform zum Austausch von Kurznachrichten, Bildern, Videos und/oder Dateien in direktem Bezug zu medizinischen Inhalten (Patientendaten). Über die Siilo-App können Patienten-befunde (z. B. EKGs, Röntgenbilder) schnell unter den an der Behandlung eines Patienten Beteiligten des Gesundheitswesens ausgetauscht werden.

Für die Kommunikation mittels Siilo (z. B. Befundübermittlung, allgemeiner Aus-tausch) ist eine Internetverbindung notwendig (Mobilfunknetz oder klinikinternes WLAN). Die App lässt sich in den App-Stores auf Smartphones mit iOS- oder Android-Betriebssystem herunterladen. Die App kann sowohl auf Mitarbeiter-eigenen, als auch auf klinik-eigenen Smartphones installiert werden – wobei sich ausschließlich medizinisches Personal z. B. Ärzte, Apotheker, Pflegemitarbeiter für Siilo registrieren können. Die notwendigen Nachweise werden von einem Service-Desk durch geschulte Siilo-Mitarbeiter individuell verifiziert. Der Verifizierungsstatus eines Nutzers ist für andere Siilo-Nutzer sofort erkennbar. Durch die Siilo-App kann die Übermittlung medizinischer Daten, mobil und möglicherweise schneller als bisher (Fax, Telefon) erfolgen, sodass die Behandlung des Patienten beschleunigt werden kann. Zudem kann der Messenger auch als Web-App genutzt werden. Dadurch können auch Daten vom PC verschickt und empfangen werden.

Die Siilo-App setzt dabei verschiedene Sicherheitseigenschaften ein, die einen Zugriff von Dritten ausschließt.

[redacted]

2. Schwellwertanalyse

Zunächst ist zu ermitteln, ob die Durchführung einer Datenschutz-Folgenabschätzung (kurz „DSFA“) notwendig ist. Dieses Verfahren kann auch „Schwellwertanalyse“ genannt werden (eng. „threshold analysis“).

Eine DSFA ist gemäß § 35 KDG in folgenden drei Fällen durchzuführen:

1. Die Form der Verarbeitung, insbesondere die Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung hat voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (§ 35 Abs. 1 KDG).

2. Die Verarbeitung fällt unter eines der Regelbeispiele aus § 35 Abs. 4 KDG. Hierzu zählen:
    a) Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
    b) Die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß § 4 Abs. 2 KDG oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 KDG.
    c) Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
3. Die Verarbeitung befindet sich auf einer Liste nach § 35 Abs. 5 KDG.

Nach den Ausführungen des Sachverhalts ist im vorliegenden Fall vor allem der nachfolgende Tatbestand betroffen:

- Umfangreiche Verarbeitung besonderer Kategorien von personenbezogener Daten der Patienten (vgl. § 4 Ziffer 2 KDG), sodass sich Rechtsfolgen oder andere erhebliche Beeinträchtigungen für diese ergeben können. Diese Daten sind der Datenschutzklasse III gem. § 13 KDG-DVO zuzuordnen und bedürfen einen besonderen Schutz.

Hierbei handelt es sich um einen Grund zur Durchführung einer Datenschutz-Folgenabschätzung, der auch in der Positivliste der Datenschutzkonferenz (Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“; Datenschutzgruppe nach Artikel 29, 04.10.2017) aufgeführt ist.

Tabelle 1. Ergebnisse der Prüfung der Zehnerregel zur Durchführung einer Schwellwertanalyse

Punkt aus „Zehnerregel“	Vorhanden?
Scoring	-
Automatisierte Einzelentscheidung mit Rechtswirkung	-
Systematisches Beobachten	X
Sensitive Daten	X
Umfangreiche Datenverarbeitung	X
Verkettung von Daten	(x)
Besonders schutzwürdige Betroffene	X
Neue Technologien/Verarbeitungen	X
Verarbeitung außerhalb des Europäischen Wirtschaftsraums (EWR)	-
Hürde für die Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen zu können	X

- trifft nicht zu (x) trifft eingeschränkt zu X trifft zu

Da sechs Kriterien erfüllt und ein weiterer mit Einschränkungen erfüllt wird, ist nach WP 248 im Sinne einer „Daumenregel“ eine Datenschutz-Folgenabschätzung durchzuführen.

Darüber hinaus erscheint die Durchführung der Datenschutz-Folgenabschätzung auch auf freiwilliger Basis als sinnvoll um Sanktionsrisiken der Datenschutzaufsicht zu reduzieren, da die Rechtsgrundlagen und technischen Rahmenbedingungen in Einzelfällen zweifelhaft erscheinen und die Verhältnismäßigkeit zumindest Diskussionen erlaubt.

Darüber hinaus fasste die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland am 26.07.2018 einen Beschluss. Dieser befasste sich mit der Beurteilung von Messenger-Diensten und fordert, dass vor der Verwendung von Messenger-Diensten Kriterien wie u. a. Serverstandort und der sicherere Datentransport zu prüfen sind. Dieser Forderung möchte [redacted] mit der vorliegenden DSFA nachkommen.

Ergebnis:

Es ist eine Datenschutz-Folgenabschätzung gem. § 35 KDG für die Nutzung des Messenger-Dienstes Siilo in [redacted] durchzuführen.

[redacted]

3. Vorbereitung

3.1. DSFA-Team

Im Rahmen der Vorbereitung der DSFA sind die zuständigen Personen zu ermitteln, die die DSFA durchführen sollen. Das DSFA-Team besteht im konkreten Fall aus einem interdisziplinären Team, das Kompetenzen u. a. in den Bereichen Datenschutz, Risikoermittlung, Prozessmanagement und in den Fachprozessen mitbringt:

Tabelle 2. Mitglieder des Teams zur Durchführung der Datenschutz-Folgenabschätzung zum Messenger-Dienst Siilo in [redacted]

Name	Funktion
[redacted]	Pflegedienstleiter
[redacted]	Stabsstelle Kooperationsmanagement/Recht
[redacted]	Geschäftsführer [redacted]
[redacted]	Leitung Qualitäts- und Risikomanagement
[redacted]	IT-Leiter
[redacted]	Betrieblicher Datenschutzbeauftragter [redacted]
Sassan Sangsari	Medical Director, Siilo Germany

3.2. Beurteilungsumfang (Scope)

Die Siilo-App besitzt verschiedene Sicherheitseigenschaften, die sie von den gängigen „Social Media“ oder „Consumer“ Messenger-Apps (WhatsApp, Facebook Messenger etc.) unterscheidet.

Der Zugang zur Siilo-App erfolgt zwingend über PIN-Code, per Fingerabdruckscanner oder Face-ID. Die Datenübertragung geschieht per sicherer End-zu-End-Verschlüsselung, wobei die Daten ausschließlich auf den genutzten Endgeräten gespeichert und nach 30 Tagen automatisch gelöscht werden.

Zur Übermittlung der Nachrichten werden Server in Deutschland genutzt. Die Server werden nur für die Übermittlung genutzt, d. h. gesendete Nachrichten werden nach Abrufen durch das Empfänger-Smartphone vollständig vom Server gelöscht und nur auf den mobilen Endgeräten gespeichert. Fotos/Videos, die mit der Siilo-App aufgenommen werden, werden – im Gegensatz zu o. g. „Consumer“ Messenger – getrennt vom vorinstallierten Kameraverzeichnis des Smartphones in einem speziellen „Container“ gespeichert. In dem Siilo-Container werden auch Nachrichteninhalte und Daten von Siilo-Kontakten gespeichert. Dieser Container wird von der App auf dem Smartphone des Nutzers automatisch bei Installation der App eingerichtet.

[redacted]

Der Zugang zu diesem Container ist nur über die Siilo-App und damit nur nach Eingabe des PIN-Codes möglich. Dies verhindert, dass bei einem Verlust des Smartphones unautorisiert auf die Fotos/Daten, die in der Siilo-App gespeichert sind, zugegriffen werden kann.

Die mit der Kamerafunktion der Siilo-App gemachten Fotos werden nicht mit Clouddiensten synchronisiert. Dies verhindert die u. U. automatisierte und unabsichtliche Übertragung sensibler medizinischer Daten auf andere mit dem Clouddienst verbundener Endgeräte wie Tablets etc.

Die Siilo-App bietet darüber hinaus Werkzeuge, mit denen Patienteninformationen auf Bildern leicht unkenntlich gemacht („Blur-Tool“) oder wichtige Aspekte durch Pfeile hervorgehoben werden können. Für die medizinische Nutzung ist die Möglichkeit zur Erstellung von individuellen Patientenfällen möglich, über die sich getrennt von anderen Fällen ausgetauscht werden kann, sodass das Risiko von Verwechslungen minimiert wird.

Die Siilo-App erhebt bei Nutzung der App durch den Nutzer Informationen. Die Rechtsgrundlage dieser Erhebung beruht auf einer Einwilligung nach § 6 Abs. 1 lit. b) KDG. Die Erhebung von Daten bezieht sich auf Daten während der Registrierung und auf Metadaten von Nachrichten. Letzteres dient dazu, die Nutzungsweise der App durch den Nutzer besser zu verstehen. Bei technischen Problemen kann zudem besser an der Lösung des Problems gearbeitet werden, wenn bestimmte Daten wie z. B. Versionsnummer der Siilo-App, Betriebssystem und Gerätestatus bekannt sind.

Ziel dieser DSFA ist es daher, zu beurteilen, ob und wie Siilo von der [redacted] in Bezug auf die Verarbeitung von Daten über die Nutzung der App KDG-konform eingesetzt werden kann.

In dieser DSFA werden daher insbesondere die Maßnahmen bewertet, die von Siilo ergriffen werden, um sicherzustellen, dass die Verarbeitung personenbezogener Daten in Zusammenhang mit der Nutzung in Übereinstimmung mit den Anforderungen des KDG erfolgen kann und welche Datenschutzoptionen der [redacted] zur Verfügung stehen, um die verbleibenden Risiken für die Patienten zu reduzieren und ob dies schließlich den Einsatz in der Organisation für die im Sachverhalt beschriebenen Zwecke ermöglicht.

3.3. Rechtsgrundlagen

Nachfolgend werden die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert.

Die [redacted] schließt mit Siilo einen Lizenzvertrag über die Nutzung der Apps und Dienste ab. Die Rechtsgrundlage für die Datenverarbeitung beruht auf § 6 Abs. 1 lit. f) i. V. m. § 6 Abs. 1 lit g) KDG. Das Interesse besteht in der effizienten Gestaltung der Arbeitswelt und der besseren Versorgung der Patienten. Eine differenzierte Abwägung der Interessen erfolgt nachfolgend.

[redacted]

Den Beschäftigten [redacted] werden die Anwendungen von Siilo im Rahmen des geschlossenen Dienstvertrags als Arbeitsmittel zur Verfügung gestellt. Soll die App auf privaten Endgeräten genutzt werden, erfolgt dies durch den Mitarbeiter freiwillig auf Grundlage einer Einwilligung § 6 Abs. 1 lit. b) KDG. Wird Siilo auf dienstlichen Geräten zur Verfügung gestellt ergibt sich die Nutzung durch die Beschäftigten aus einer arbeitsvertraglichen Nebenpflicht (§ 6 Abs. 1 lit. a) KDG i. V. m. mit § 53 KDG) des Dienstnehmers.

3.4. Abwägung der Notwendigkeit und Verhältnismäßigkeit

Die in den vorigen Schritten beschriebene Verarbeitungsverfahren ist nun ausgehend von den mit ihnen verfolgten Zwecken daraufhin zu bewerten, ob der durch das Verfahren bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zum angestrebten Zwecken steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Betroffenenrechte weniger stark eingreifen. Ggf. ist von der verantwortlichen Stelle eine Anpassung der Verarbeitungsverfahren vorzunehmen, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

Bewertung der Notwendigkeit

Die [redacted] sieht sich mit einer Vielzahl schwerwiegender Herausforderungen konfrontiert. So ist auf der einen Seite der sich verschärfende Fachkräftemangel zu nennen, der es erforderlich macht, vorhandene personelle, technische und zeitliche Ressourcen so effizient wie möglich auszuschöpfen. Auf der anderen Seite steigen, nicht auch zuletzt wegen der Corona-Pandemie, die Anforderungen der Beschäftigten dort, wo dies im Rahmen der Art und Weise der auszuführenden Tätigkeit möglich ist, an eine zeitlich sowie räumlich flexiblere Arbeitsmöglichkeit. Somit liegt die Nutzung von Siilo nicht nur im Interesse der [redacted], sondern trifft auch in einer Vielzahl von Fällen die Anforderungen der Patienten, für eine schnellere und qualifiziertere Versorgung durch einen effizienteren Austausch der Personen, die am Behandlungsprozess beteiligt sind. Somit ist es unstrittig, dass die Notwendigkeit an einem neuen Instrument zur Kommunikation in [redacted] besteht.

Bewertung der Verhältnismäßigkeit

Die Nutzung von Siilo, welches ein Werkzeug zur ortsunabhängigen kollaborativen Arbeit ist, ist zudem ein wesentlicher Bestandteil um die [redacted] im Marktumfeld zukunftssicher aufzustellen. Aktuell gibt es keine vergleichbare Alternative im europäischen Markt, die einen vergleichbaren hohen Schutz der personenbezogenen Daten darstellt.

Für die Nachrichten in Transit verwendet Siilo eine sichere Ende-zu-Ende Verschlüsselung, umgesetzt über die sogenannte NaCl crypto library (https://nacl.cr.yp.to/). Das bedeutet, dass jede Nachricht zwischen Absender und Empfänger über ein öffentliches/nicht-öffentliches Schlüsselpaar verschlüsselt ist. Nur Absender und Empfänger können die von ihnen ausgetauschten Nachrichten entschlüsseln und lesen. Die Authentizität der Nachrichten kann empirisch

[redacted]

nachgewiesen werden. Dritte, darin eingeschlossen das Unternehmen Siilo und dessen Angestellte, sind keinesfalls in der Lage, die Inhalte der ausgetauschten Nachrichten zu lesen, da die Schlüssel der Ende-zu-Ende Verschlüsselung nur zwischen den Endgeräten von Absender und Empfänger ausgetauscht werden.

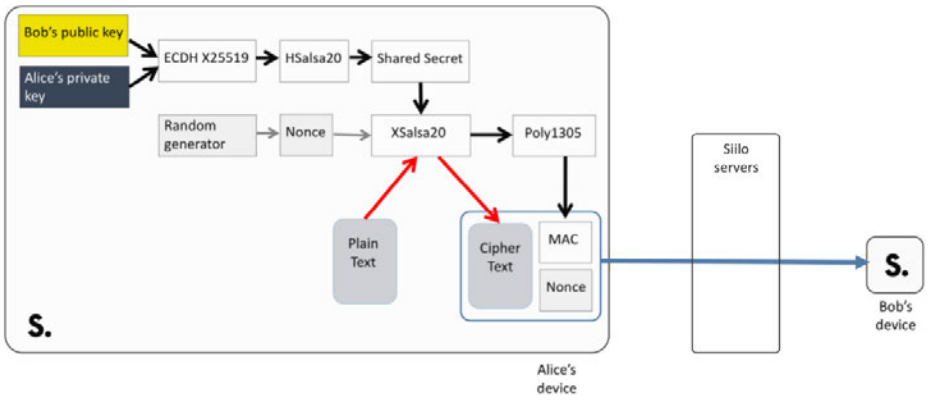

Abbildung 1.Schema des Ende-zu-Ende Verschlüsselungsprotokolls zwischen zwei Siilo-Nutzern (Alice und Bob)

Interessenabwägung

Den berechtigten Interessen [redacted] an der Nutzung der Siilo-App stehen die Interessen und Grundrechte/-freiheiten der Betroffenen gegenüber. Folgende Kriterien sind für die Abwägung zu betrachten und werden nachfolgend dargestellt:

Tabelle 3. Checkliste zur Abwägung der Interessen Betroffener und [redacted]

Kriterium	Gewichtung	Beschreibung	Ergebnis
Kreis der beteiligten Akteure	Je kleiner, desto besser	Es sollen nur jene Mitarbeiter an der Nutzung der App beteiligt werden, wo die Nutzung aufgrund der Arbeitsorganisation angezeigt ist.	Grundsatz der Erforderlichkeit wird erfüllt
Kreis der Betroffenen	Je kleiner, desto besser	Betroffene sind die Patienten der [redacted] und die Nutzer der Siilo-App. Auch hier wird die Erforderlichkeit zum Austausch der Behandlungsbeteiligten nicht jeden Patienten betreffen und nicht jeder Mitarbeiter wird dort als Nutzer von Anfang an hinterlegt.	Grundsatz der Erforderlichkeit wird erfüllt
Datenkategorien	Je weniger sensibel, desto besser	Vom System werden verschiedene Daten erhoben, die aber gänzlich relevant für die Nutzung (Legitimation) des Systems sind. Daten mit einer geringeren Relevanz wurden mit dem Hinweis „optional“ versehen.	Grundsätze der Erforderlichkeit und Datenminimierung werden erfüllt

[redacted]

Kriterium	Gewichtung	Beschreibung	Ergebnis
Datenmenge	Je geringer, desto besser	Die Menge der Daten ist in Abhängigkeit vom jeweiligen Behandlungszweck und wird vom [redacted] stets berücksichtigt.	Grundsatz der Datenminimierung wird erfüllt
Dauer der Aufbewahrung der Daten	Je kürzer, desto besser	Die Nutzerdaten werden sofort nach dem Ende der Lizenzvereinbarung gelöscht. Übermittelte Daten werden nach 30 Tagen auf dem Endgerät gelöscht.	Grundsatz der Speicherbegrenzung wird erfüllt
Verkettung mit weiteren Daten (Profilbildung)	Je stärker von bereits erhobenen Daten getrennt, desto besser	Um Zugang zu den Metadaten zu erhalten, müssen die Siilo-Entwickler ein extra dafür generiertes Passwort erstellen. Jeder Zugriff auf diese Metadaten durch Mitarbeiter von Siilo werden durch einen speziellen „Einbuchungsprozess“ dokumentiert.	Grundsatz der Zweckbindung wird erfüllt
Weitergabe	Je kleiner der Empfängerkreis, desto besser	Die Daten werden ausschließlich an den Auftragsverarbeiter Siilo weitergegeben.	Grundsatz der Vertraulichkeit wird erfüllt
Vernünftige Erwartung der Betroffenen	Kann ein Betroffener die Verarbeitung in dieser Form erwarten?	Die [redacted] den Beschäftigen eine detaillierte Darstellung zur Datenverarbeitung zur Verfügung.	Grundsatz der Transparenz wird erfüllt
Eingriffsmöglichkeit durch Betroffene	Je mehr, desto besser	Eine Eingriffsmöglichkeit des Patienten besteht nicht, ist aber auch nicht erforderlich. Die Mitarbeitenden können ihrer Einwilligung zur Nutzung der Daten widersprechen.	Eingriffsmöglichkeiten der Betroffenen, dort wo erforderlich, vorhanden

[redacted]

Ergebnis:

Das Interesse der betroffenen Beschäftigten am Schutz ihrer personenbezogenen Daten bei der Nutzung von Siilo überwiegt nicht und die Grundrechte und Grundfreiheiten werden in ausreichendem Umfang gewahrt. Damit ist eine Verarbeitung wie oben beschrieben auf der Grundlage des berechtigten Interesses möglich.

4. Durchführung

4.1. Risikoanalyse und -beurteilung

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die Risiken werden hinsichtlich der Schwere des Schadens und der Eintrittswahrscheinlichkeit beschrieben. Die Risikobeurteilung orientiert sich hierbei an den Vorgaben der ISO 31000.

Die Risikobeurteilung besteht dabei aus der Risikoidentifikation, der Risikoanalyse und der Risikobewertung. Zur Risikoidentifikation gehören die Risikobeschreibung samt -quelle. Die Risikoanalyse umfasst den möglichen Schaden für die Betroffenen, die Eintrittswahrscheinlichkeit und die Schwere des Schadens. Aus den letzten Punkten ergibt sich das Ergebnis der Risikobewertung. Die Risiken werden anschließend gem. dem Maßnahmenbereich aus § 26 Abs. 1 KDG aggregiert dargestellt. Die Risikobewertung anhand der Eintrittswahrscheinlichkeit und der Schwere des Schadens erfolgt in Anlehnung an den BSI-Standard 200-3 (Tab. 4):

Tabelle 4. Objektivierung zu Dimensionen zur Eintrittswahrscheinlichkeit und Schadenshöhe

Eintritts-wahrscheinlichkeit	**Beschreibung**
Unwahrscheinlich	Das Risikoereignis tritt alle 10 Jahre oder seltener ein.
Sehr selten	Das Risikoereignis tritt einmal innerhalb von 10 Jahren ein.
Selten	Das Risikoereignis tritt einmal jährlich ein.
Möglich	Das Risikoereignis tritt einmal monatlich ein.
Häufig	Das Risikoereignis tritt wöchentlich oder häufiger ein.
Schadenshöhe	**Schadensauswirkungen**
Unbedeutend	Die Auswirkungen sind für den Betroffenen nicht schädlich, aber geringer Aufwand zur Wiederherstellung des Ist-Zustands ist erforderlich.
Gering	Geringe Nachteile für den Betroffenen (wirtschaftlich, gesellschaftlich).
Spürbar	Das Risikoereignis kann zu spürbaren finanziellen Folgen oder zu gesellschaftlichen Sanktionen (Diskriminierung) führen.
Kritisch	Kritische Folgen des Risikoereignisses (Identitätsdiebstal, gesellschaftliche Meidung).
Katastrophal	Das Risikoereignis ist für den Betroffenen existenzgefährdend.

4.1.1. Pseudonymisierung

Im Rahmen der Nutzung des Messenger Dienstes von Siilo werden Daten durch die Siilo-App erhoben und verarbeitet. Dies sind Nutzer- und Nachrichtendaten wie u. a. der Namen, die Mobiltelefonnummern aber auch Textnachrichten. Aufgrund der Verschlüsselungstechniken, die zum Einsatz kommen, handelt es sich bei allen Daten um vollständig anonymisierte bzw. verschlüsselte Daten.

Ein Risiko der Depseudonymisierung kann somit faktisch nicht stattfinden und somit ist eine Eintrittswahrscheinlichkeit insgesamt als „Unwahrscheinlich" zu bewerten. Der zu erwartende Schaden für die Anwender ist jedoch als kritisch einzustufen, da Rückschlüsse auf die Nutzer und individuelle Schwächen bei der Anwendung möglich wären.

Aggregierte Risikobewertung im Maßnahmenbereich Pseudonymisierung:

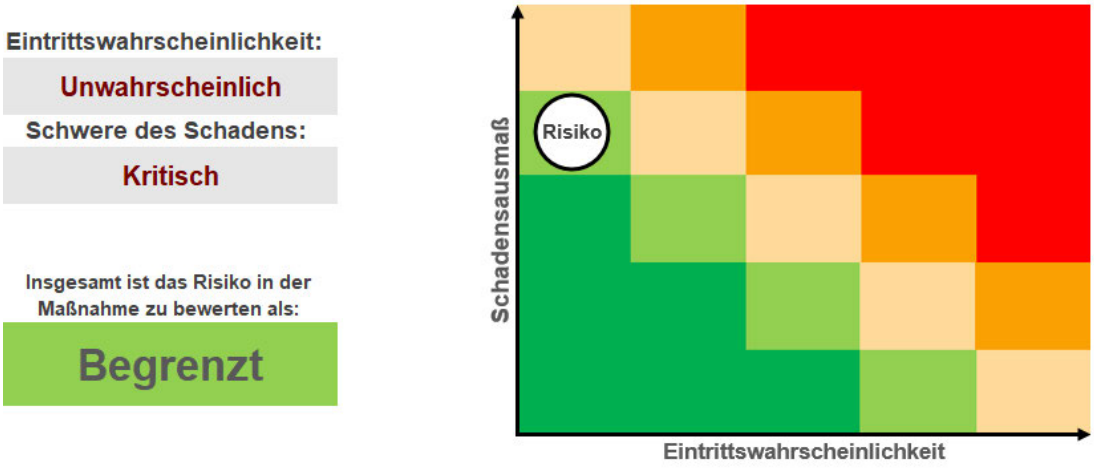

Abbildung 1. Risikomatrix zum Maßnahmenbereich Pseudonymisierung

4.1.2. Verschlüsselung

Patientendaten (einschließlich aller darin enthaltenen personenbezogenen Daten), die über öffentliche Netzwerke zwischen Anwender und Siilo übertragen werden, werden standardmäßig verschlüsselt.

Siilo teilt die Nachrichtendaten in zwei Status ein.

1. Nachrichten/Daten in Transit („data in transit"), d. h. dann, wenn die Informationen von einem Gerät zum anderen versendet werden.
2. Nachrichten/Daten im Ruhezustand („data at rest"), d. h. dann, wenn die Informationen auf dem Endgerät angekommen und nicht weiter in Bewegung sind.

Data in transit

Siilo verwendet Zertifikate zur Vermeidung sogenannter „Man-in-the-Middle-Angriffe", ein Vorgang, bei dem Angreifer auf den Datenverkehr zwischen den Smartphones zugreift und versucht, die Kommunikationslinien anzugreifen, um die Nachrichten zu

lesen. Die Standard TLS v1.2-Kommunikation erfordert ein gültiges SSL-Zertifikat, ausgestellt von einer vertrauenswürdigen Zertifizierungsstelle. Dieses Zertifikat wird vom Endgerät erkannt. Die Verankerung von Zertifikaten geht weiter und setzt voraus, dass diese Zertifikate von einer Vertrauenskette von einem festgelegten Aussteller ausgehen. Dies schließt eine ganze Reihe an angreifbaren Stellen aus, welche aus den grundlegenden Verteilungsproblemen im Zusammenhang mit der Struktur der Authentifizierung durch Zertifikate des Internets entstehen.

Im Rahmen der Verschlüsselung von Nachrichten in Transit werden des Weiteren „Authentifikatoren mit öffentlichen Schlüsseln" genutzt. Diese Eigenschaft erlaubt es der Applikation, mathematisch nachzuweisen, dass die Nachricht von einer der beiden Parteien ausgegangen ist (Absender/Empfänger). Dies reicht jedoch bezüglich sogenannter „Social-Engineering"-Angriffe nicht aus. In diesem Szenario nutzen Angreifer ähnliche Namen oder Profile, um sensible Informationen von einem möglichen Ziel zu „phishen". Ein wirksamer Mechanismus gegen solche Angriffe ist das Konzept der „Out-of-Band"-Verifikation. Siilo unterstützt dies darüber, dass Nutzern ermöglicht wird, auf ihr Profil zuzugreifen und ihre einzigartige ID, genannt „Key Fingerprint" einzusehen. Zwei Nutzer können diese IDs austauschen – idealerweisen persönlich – und stellen so sicher, dass sie in der Tat diejenigen sind, die sie zu sein behaupten.

Data at rest

Befinden sich die Daten in der Siilo-App, werden diese nicht an Apps von Drittanbietern weitergeleitet. Mit Siilo aufgenommene bzw. übermittelte Bilder landen nicht in der einfach zugänglichen Standard-Bildergalerie (Kameraverzeichnis) des Smartphones, sondern in einem speziellen Verzeichnis („Container"), das durch die Siilo-App auf dem Smartphone angelegt wird. Dadurch ist der Zugang zu den Bildern nur über die Siilo-App und somit nur nach Eingabe des Zugangspassworts (PIN-Code) möglich. Ein automatisches Backup der in der Siilo-App gespeicherten Informationen auf Servern von Drittanbietern (etwa iCloud, Google Drive oder Dropbox) wird verhindert. Per Siilo übermittelte Nachrichten/Bilder/Videos/Dateien werden nach 30 Tagen automatisch gelöscht.

Zwar besteht theoretisch noch ein Restrisiko, dass die Verschlüsselung durch Unbefugte gebrochen wird; dies ist aber aufgrund von Erfahrungswerten der Vergangenheit als unwahrscheinlich einzustufen.

Siilo verfügt über ein Informationssicherheitsmanagementsystem (ISMS) und ist gemäß ISO 27001 und NEN 7510 (Niederländische Norm für Informationssicherheit im Gesundheitswesen) zertifiziert. Zudem verfügt Siilo über verschiedene technische und organisatorische Vorgehensweisen und Kontrollen, wie etwa periodische und standardisierte Risikoabschätzungen, interne Audits, Informationssicherheitsbestimmungen, eine „need-to-know"-Richtlinie (Richtlinie für minimale Benutzerrechte), regelmäßige Fortbildung des Personals, Management von (Sicherheits-)Zwischenfällen und einen festen Ablauf für die Mitteilung einer Verletzung der Datensicherheit.

Jede von Siilo umgesetzte Lösung durchläuft einen Prozess der Risikoabschätzung und einen Prozess der Datenschutz-Folgenabschätzung (DSFA). Dieser folgt einem streng geregelten Ablauf in Übereinstimmung mit den ISO 27001- und NEN 7510-

Vorgaben. Die Prozesse werden innerhalb von Siilo durch einen unabhängigen Sicherheitsbeauftragten sowie Datenschutzbeauftragten überwacht, der bei der niederländischen Datenschutzbehörde registriert ist.

Die von Siilo vertraglich eingesetzten Maßnahmen sind als hinreichend zu sehen, sodass auch hier das theoretische Restrisiko als unwahrscheinlich einzustufen ist.

Aggregierte Risikobewertung im Maßnahmenbereich Verschlüsselung:

Eintrittswahrscheinlichkeit:

Sehr selten

Schwere des Schadens:

Kritisch

Insgesamt ist das Risiko in der Maßnahme zu bewerten als:

Wesentlich

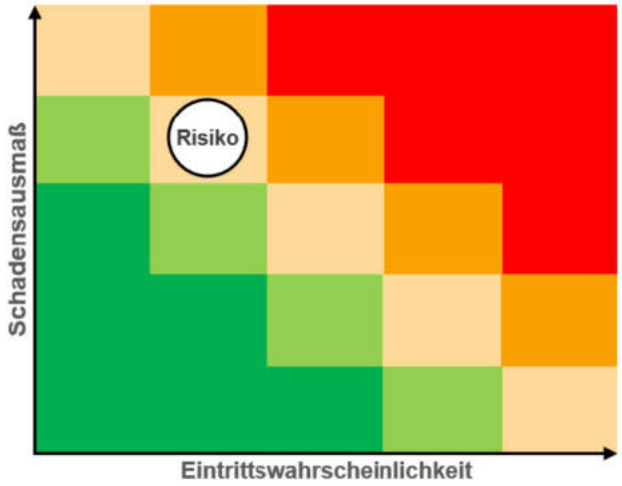

Abbildung 2. Risikomatrix zum Maßnahmenbereich Verschlüsselung

4.1.3. Gewährleistung der Integrität und der Vertraulichkeit

Siilo hat eine Reihe wirksamer Maßnahmen ergriffen, um die Integrität und die Vertraulichkeit der in den Anwendungen von der App verarbeiteten Daten zu gewährleisten:

Nachrichtendaten - Daten im Ruhezustand auf dem Nutzergerät

Für im Ruhezustand auf dem Endgerät (iPhone, iPad, Android) befindliche Daten sind folgende Absicherungen eingerichtet:

- Alle „Schlüsselmaterialien“, auch bekannt als die von der Kryptografie verwendeten Codes, sind entsprechend in der iOS-KeyChain oder der Android KeyStore gespeichert.
- Alle „Schlüsselmaterialien“ sind über einen „Masterschlüssel“ verschlüsselt.
- Die gesamte Datenbank ist über SQLiteCipher verschlüsselt. Alle Nachrichten, Metadaten von Nachrichten und Kontaktinformationen von Siilo-Nutzern sind auf diese Weise gespeichert.
- Alle eingegangenen Medien werden an deren Speicherort (sog. „Silo“-Konzept) gespeichert, mit einem lokalen symmetrischen Schlüssel verschlüsselt, welcher für alle lokalen Medien verwendet wird. Auf diesen Schlüssel wird über die o. g. Datenbank zugegriffen.

- Ein Pin Code-Mechanismus (Fingerabdruck, Face-ID) auf Ebene der Applikation verhindert den Zugriff durch Unbefugte, die direkten Zugang zu dem Endgerät des Siilo-Nutzers haben. Dies deckt die meisten Formen persönlichen Social-Engineerings ab, wie etwa die Bitte um ein Ausleihen des Telefons für einen kurzen Anruf etc.
- Alle in der Siilo-App ausgetauschten Informationen werden nach 30 Tagen automatisch gelöscht. Nutzer können eigenständig entscheiden, individuelle Nachrichten sofort zu löschen, wenn ihnen 30 Tage als zu lang erscheinen. Auf Countdown-Timer oder Angaben von Lebensspannen für Nachrichten wurde bewusst verzichtet, da dies beim Nutzer ein Gefühl der Dringlichkeit auslösen kann, sodass Screenshots oder andere ungewollte Verhaltensweisen auf Empfängerseite getätigt werden könnten.
- Ist einem Nutzer bekannt, dass sein/ihr Gerät verloren gegangen/gestohlen worden oder auf andere Weise beeinträchtigt ist, kann die Siilo-App und die darin enthaltenen Daten per Fernzugriff vom Gerät gelöscht werden.

Nachrichtendaten - Im Ruhezustand befindliche Daten auf Siilos Servern

Für im Ruhezustand befindliche Daten auf den von Siilo genutzten Servern sind die folgenden Absicherungen eingerichtet:

- Alle von Siilo genutzten Server befinden sich innerhalb der Europäischen Union und erfüllen höchste Sicherheitsanforderungen.
- Firewall-Regeln verhindern den Netzwerkzugriff auf die Datenbanken (MySQL und ElasticSearch). Von extern ist lediglich ein beschränkter Netzwerkzugriff auf ein untergeordnetes Netzwerk möglich. Nur eine eingeschränkte Auswahl von Siilo-Angestellten kann auf diese zugreifen.
- Die MySQL-Datenbank, die Nachrichtendaten, Metadaten von Nachrichten, Siilo.Connect Konfigurationsdaten und Daten von Nutzerprofilen enthält, ist passwortgeschützt und verschlüsselt unter Verwendung der Industrienorm AES-256.
- Die von Siilo genutzten Server verschlüsselten bestimmte Felder, z. B. E-Mail und Telefonnummer. Andere Profilfelder, welche in der App Siilo-Mitgliedern als „öffentlich“ angezeigt werden, werden als Klartext gespeichert.
- Alle Medien (welche über die Siilo-App versandt und daher als sensibel angesehen werden) werden mit dem einmaligen, symmetrischen Verschlüsselungsschlüssel verschlüsselt gespeichert. Dieser auf den Endgeräten von Absender und Empfänger generierte Schlüssel wird auf keinem von Siilo genutzten Server gespeichert, es sei denn, als Teil der verschlüsselten, unter MySQL gespeicherten Nachrichtendaten. Die für die Entschlüsselung dieser Daten erforderlichen Schlüssel sind nur auf den Endgeräten von Absender und Empfänger vorhanden.

Nur ein bewusstes, d. h. absichtliches Fehlverhalten eines Nutzers kann für Abweichungen von den eingesetzten Einstellungen und Maßnahmen führen und somit die Vertraulichkeit der Daten gefährden. Hiergegen muss eine entsprechende Dienstanweisung durch den Verantwortlichen [redacted] an die Mitarbeiter als Nutzer von Siilo erfolgen.

[redacted]

Insgesamt ist die Eintrittswahrscheinlichkeit für das Risiko, dass die Integrität und Vertraulichkeit der Daten gefährdet wird, als sehr selten einzustufen. Die Schadensschwere für den Betroffenen, kann in Abhängigkeit von den jeweils verarbeiteten Daten als kritisch bewertet werden. So könnte dies zu einem offenlegen von Krankendaten führen, was Erhebliche bis hin zu existenzgefährdeten Auswirkungen zur Folge haben kann.

Aggregierte Risikobewertung im Maßnahmenbereich Integrität und Vertraulichkeit:

Eintrittswahrscheinlichkeit:

Sehr selten

Schwere des Schadens:

Kritisch

Insgesamt ist das Risiko in der Maßnahme zu bewerten als:

Wesentlich

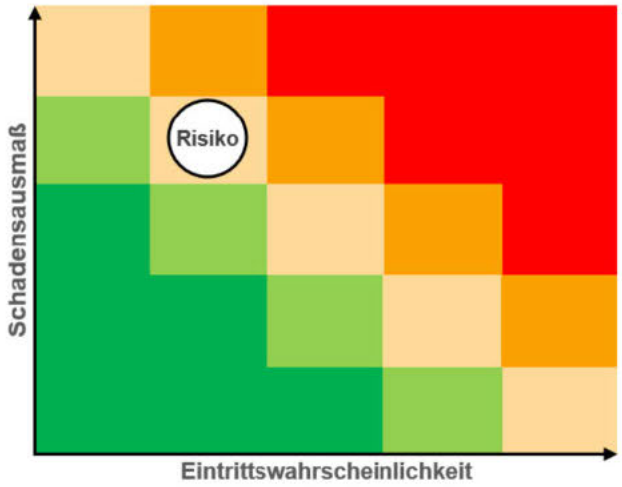

Abbildung 3. Risikomatrix zum Maßnahmenbereich Integrität und Vertraulichkeit

4.1.4. Gewährleistung der Verfügbarkeit und Belastbarkeit

Siilo hat eine Reihe wirksamer Maßnahmen ergriffen, um die Verfügbarkeit und die Belastbarkeit der Systeme von der Siilo-App in Zusammenhang mit den verarbeiteten Daten zu gewährleisten:

So bietet es den Nutzern die Möglichkeit, ein Backup ihrer Kontaktdaten und Chatinhalte zu erstellen. Die Funktion wurde so implementiert, dass nur der Nutzer den Schlüssel für diese Sicherung und Wiederherstellung besitzt. Siilo kann auf diesen Schlüssel nicht zugreifen („zero knowledge policy").

Für die Patientendokumentation relevante Chatinhalte können aus der Siilo-App exportiert und in die IT-Struktur eines Krankenhauses übermittelt werden. Ein Nutzer kann relevante Inhalte manuell auswählen und dann als pdf-Datei exportieren. Die Export-Funktion kann auch automatisiert erfolgen durch Integration von Siilo in das jeweilige Krankenhaus-Informationssystem.

Siilo garantiert den Nutzern, dass alle Nachrichten vollständig an den/die Empfänger übertragen werden. Der Übertragungsstatus der Nachricht wird graphisch mittels (doppelter) Häkchen, je nach Empfangsstatus in unterschiedlicher Farbe, dargestellt. Wird eine Nachricht (z. B. aufgrund fehlender Mobilfunkverbindung) nicht übertragen, wird dies für den Nutzer klar sichtbar durch eine rote Markierung der nicht-übermittelten Nachricht hervorgehoben. Bei wiederhergestellter Datenverbindung können Sie

die Nachricht durch einfachen Klick erneut senden. Die Siilo-App verteilt Mitteilungen grundsätzlich nicht auf mehrere Nachrichten, sondern verschickt eine Mitteilung als eine Nachricht an den Empfänger.

Insgesamt sind die Anwendungen von Siilo als sehr belastbar anzusehen, die so ein Höchstmaß der Verfügbarkeit garantieren. Aber auch im Falle eines temporären Ausfalls der Siilo-App würde dies nicht zu kritischen Folgen für [redacted] und die Betroffenen führen, da die wesentlichen Leistungsprozesse weiterhin abgebildet werden können. So kann die Kommunikation weiterhin u. a. per Telefon oder Fax erfolgen.

Aggregierte Risikobewertung im Maßnahmenbereich Verfügbarkeit und Belastbarkeit:

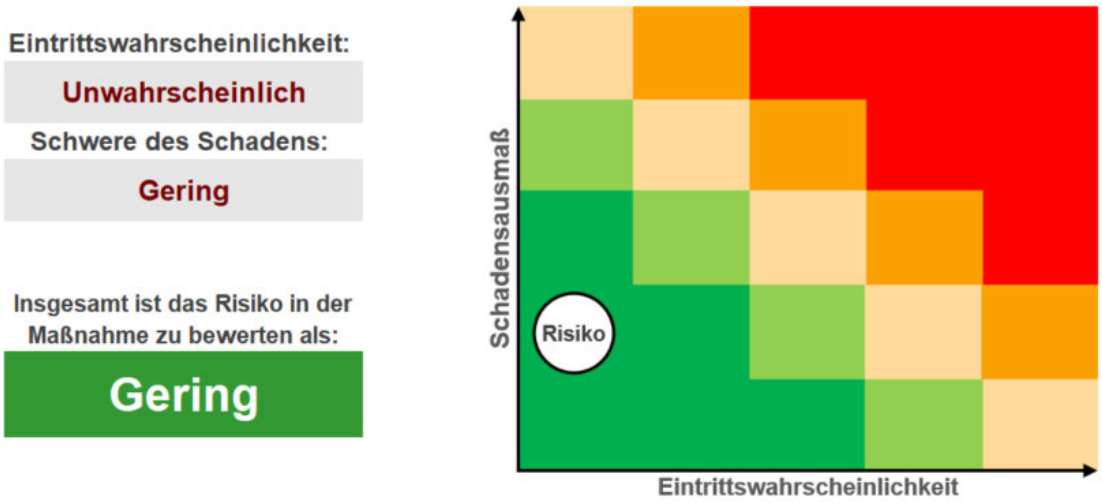

Abbildung 4. Risikomatrix zum Maßnahmenbereich Verfügbarkeit und Belastbarkeit

4.1.5. Wiederherstellung nach einem technischen Zwischenfall

Siilo hat eine Reihe wirksamer Maßnahmen ergriffen, um die Wiederherstellung, der in den Anwendungen von der App verarbeiteten Daten, nach einem technischen Zwischenfall zu gewährleisten.

Speicherung personenbezogener Daten auf von Siilo genutzten Servern

Nachrichtendaten werden auf Servern in Frankfurt a. M. gespeichert. Für Backup-Zwecke werden jeden Tag automatische „snap-shots“ erstellt, welche aber für höchstens sieben Tage gespeichert werden. Diese Schnappschüsse sind im Ruhezustand verschlüsselt. Die von Siilo genutzte Serverinfrastruktur wird von Amazon Inc. gehostet. Siilo hat Amazon Web Services (AWS) ganz bewusst ausgewählt, da diese die höchsten Sicherheits- und Verschlüsselungsstandards erfüllen und sicherstellen (DSGVO), dass Ihre SOC-Level I-II-III, ISO 9001, ISO 27001, ISO 27017 und ISO 27018 eingehalten werden.

Nutzerdaten

Die Daten der Siilo-Nutzer werden auf Servern in Dublin (Irland) gespeichert. Es werden tägliche Backups erstellt. Diese Backups werden für höchstens 30 Tage in einem im Voraus konfigurierten Daten-„Bucket“ gespeichert, welcher im Ruhezustand verschlüsselt ist.

Es sind bereits ausreichende Maßnahmen zur Wiederherstellung der Verfügbarkeit und nach einem technischen Zwischenfall implementiert worden; aber selbst im Fall eines temporären Ausfalls der Anwendungen würde dies nicht zu kritischen Folgen für die Betroffenen in [redacted] führen, da die wesentlichen Leistungsprozesse über andere Kommunikationswege bzw. das Krankenhausinformationssystem abgebildet werden können.

Aggregierte Risikobewertung im Maßnahmenbereich Wiederherstellung nach einem technischen Zwischenfall:

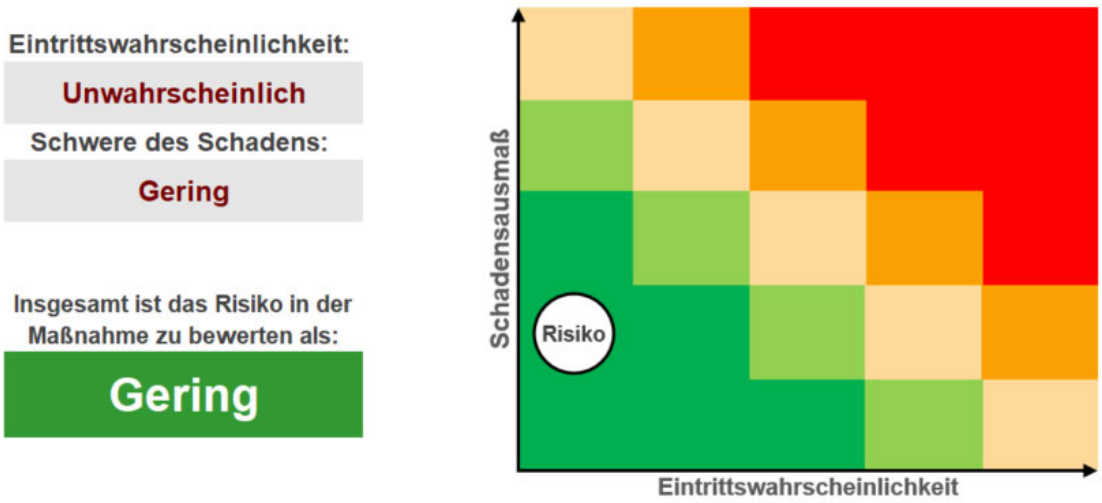

Abbildung 5. Risikomatrix zum Maßnahmenbereich Wiederherstellung nach einem technischen Zwischenfall

4.1.6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Siilo und [redacted] haben im Zusammenhang mit der Verarbeitung personenbezogener Daten in den Anwendungen von der App bereits Maßnahmen etabliert, um die regelmäßige Überprüfung, Bewertung und Evaluierung zu gewährleisten.

Siilo:

- Siilo führt eine Vielzahl von Maßnahmen durch, um die Sicherheit der Verarbeitung zu gewährleisten; hierzu werden die Metadaten der Nutzer analysiert und erforderlichenfalls notwendige Abhilfemaßnahmen durchgeführt sowie den Nutzern zur Verfügung gestellt.
- Der Datenschutzbeauftragte der Firma Siilo wird als internes Kontrollorgan in die Weiterentwicklungen der Siilo-App eingebunden.

[redacted]

- Es erfolgten Prüfungen durch externe Stellen wie ZTG und DEKRA. Eine aktuelle Zertifizierung auf der Grundlage der ISO/IEC 27001:2013 mit Bezugnahme auf die Entwicklung, Implementierung und Nutzung sicherer Kommunikations- und Speicherdienste für vertrauliche Informationen liegt bis zum 1. August 2022 vor.

[redacted]

- Bei [redacted] wird der betriebliche Datenschutzbeauftragte regelhaft bei der Einführung neuer oder Anpassung bestehender Datenverarbeitungssysteme beteiligt, gleiches trifft in Zukunft auch für eventuelle Anpassungen der Anwendungen von der Siilo-App bzw. eine Zweckänderung im Rahmen der Datenverarbeitung zu.
- Der betriebliche Datenschutzbeauftragte behält Änderungen an den rechtlichen und technischen Rahmenbedingungen engmaschig in der Beobachtung und kann erforderlichenfalls kurzfristig auf notwendige Anpassungen in den Systemen hinwirken.

Damit sind in der Summe ausreichende Maßnahmen umgesetzt worden, um die regelmäßige Überprüfung, Bewertung und Evaluierung sowie erforderlichenfalls die Anpassung der App und der technischen und organisatorischen Maßnahmen gewährleisten zu können. Trotzdem besteht das Risiko, dass eine Überprüfung der Anwendung nicht regelmäßig durchgeführt wird, weshalb die Eintrittswahrscheinlichkeit als selten einzustufen ist.

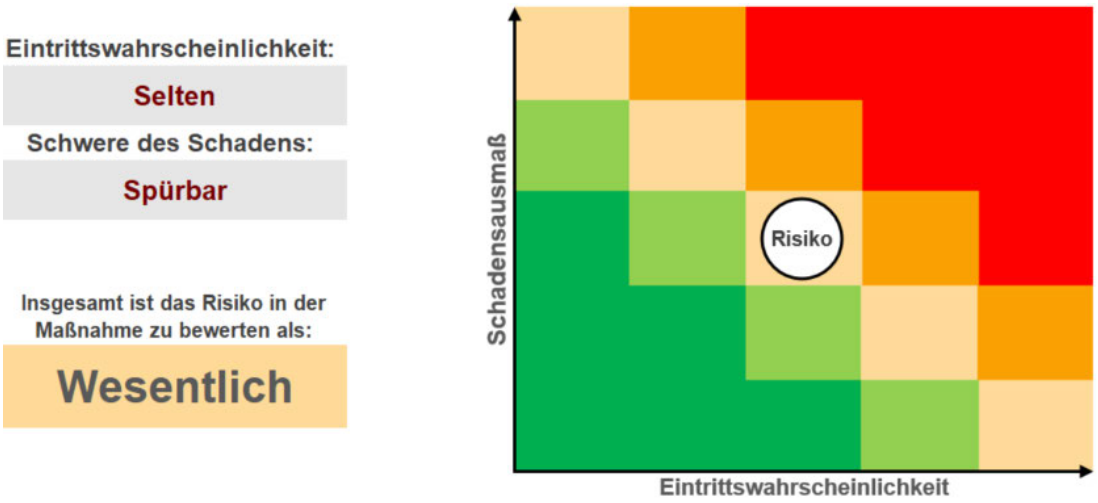

Abbildung 6. Risikomatrix zum Maßnahmenbereich der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung, Planung von Abhilfemaßnahmen

Im Anschluss an die Risikoidentifizierung und -bewertung sind verschiedene Abhilfemaßnahmen zu bestimmen, die hohe Risikobewertungen insoweit reduzieren sollen, dass eine erneute Analyse der Risiken eine akzeptable Risikoeinschätzung ergibt. Nachfolgend werden ausgewählte Abhilfemaßnahmen vorgestellt.

[redacted]

4.2. Risikobewertung

4.2.1. Maßnahmen zur Sicherstellung der Pseudonymisierung, Verschlüsselung und Vertraulichkeit

Es wurde festgestellt, dass Siilo Metadaten von Nachrichten sammelt. Diese Metadaten werden ausschließlich gesammelt, um Nachrichten zu verschicken sowie für allgemeine statistische Zwecke. Ein Rückschluss auf das Verhalten einzelner Nutzer ist aber nicht möglich, da diese Daten anonymisiert erhoben werden, was dazu führt, dass kein direkter Rückschluss auf eine natürliche Person erfolgen kann.

Weitere Maßnahmen zur Risikoeindämmung im Maßnahmenbereich Pseudonymisierung, Verschlüsselung und Vertraulichkeit sind nicht erforderlich.

4.2.2. Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit

Bei [redacted] soll die Siilo-App überwiegend für die kollaborative Arbeit eingesetzt werden, die Verarbeitung von besonderen Datenkategorien nach § 11 Abs. 1 KDG, z. B. Gesundheitsdaten der Patienten, stehen dabei im Mittelpunkt der Nutzung.

Maßnahmen zur Risikoeindämmung:

Wir empfehlen, die Erstellung einer Richtlinie zur Nutzung von Siilo im [redacted] und die Mitarbeiter entsprechend der Nutzung zu unterweisen, damit ein Fehlverhalten des Nutzers vorgebeugt werden kann.

Gemäß dem White-Paper „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ der Datenschutzkonferenz vom 07.11.2019 müssen die genutzten Endgeräte einem Dienst für das Mobile Device Management (MDM) unterworfen werden. Dies ist für die Siilo-App nicht notwendig, da die Datenverarbeitung durch die App selbst in einem Container erfolgt und bei Verlust des Endgerätes eine Fernlöschung möglich ist. Damit wird sichergestellt, dass die im Siilo Container geschützten Daten nicht in falsche Hände gelangen können.

4.2.3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der betriebliche Datenschutzbeauftragte in [redacted] wird regelhaft bei wesentlichen Anpassungen am System beteiligt. Gleiches trifft für eventuelle Anpassungen der Office-Anwendungen bzw. eine Zweckänderung im Rahmen der Datenverarbeitung zu. Allerdings ist hierzu noch kein verbindlicher Prozess definiert.

Maßnahmen zur Risikoeindämmung:

Damit diese Beteiligung auch formal sichergestellt wird, ist zu empfehlen regelmäßige Jours fixes zwischen dem IT-Verantwortlichen [redacted] und [redacted] zu vereinbaren, um die datenschutzrechtlichen Anforderungen in jedem Fall berücksichtigt zu wissen.

[redacted]

[redacted] kann im Rahmen dieser Jours fixes wiederum auf technische und rechtliche Entwicklungen aufmerksam machen und selbst notwendige Anpassungen an den technischen und organisatorischen Maßnahmen anstoßen.

4.2.4. Maßnahmen zur Gewährleistung der Transparenz und Umsetzung der Betroffenenrechte

Wie im Rahmen der durchgeführten Interessenabwägung festzustellen war, ist die Umsetzung der Rechte der Betroffenen sowie die Eingriffsmöglichkeiten der Betroffenen selbst im Rahmen der Nutzung von der Siilo-App sehr schwierig. Vor diesem Hintergrund legt [redacted] größten Wert darauf, ihren Informationspflichten gemäß § 15 KDG nachzukommen und somit gegenüber den Betroffenen eine notwendige Transparenz zu schaffen.

Maßnahmen zur Risikoeindämmung:

[redacted] muss den Mitarbeitenden, welche die Siilo-App nutzen möchten, die notwendigen Informationen nach §§ 15,16 KDG bezüglich der Datenverarbeitung zur Verfügung stellen. Die erarbeiteten Hinweise zur Datenverarbeitung sind dieser Ausarbeitung als Anlage 2 beigefügt.

Ferner ist die Mitarbeitervertretung gemäß § 29 Abs. 1 Nr. 14 MAVO anzuhören und bei der Einführung mitberatend zu beteiligen.

[redacted]

5. Umsetzung und Bericht

5.1. Umsetzung und Testung der Abhilfemaßnahmen

Nachdem das Ergebnis der Risikobewertung feststeht und geeignete Abhilfemaßnahmen zur Bewältigung der Risiken in den Maßnahmenbereichen erarbeitet wurden, müssen sich die Maßnahmen unter realen Bedingungen beweisen. In den meisten Fällen bringen die geplanten Maßnahmen tatsächlich die gewünschte Wirkung und je nach eingesetzter Maßnahme wird entweder die Eintrittswahrscheinlichkeit, die Schwere des Schades oder auch beide gleichzeitig in den grünen Bereich der Risikomatrix gerückt. Manche Maßnahmen haben jedoch nicht die geplante Wirkung und erfordern Anpassungen durch effizientere Lösungsansätze oder erwirken ein Umdenken bei der Risikobewertung. Manche Maßnahmen können auch die Risiken in anderen Bereichen erhöhen.

Im Falle von der Siilo-App besteht nun die Besonderheit, dass die Maßnahme durch die Mitarbeitenden zu beachten ist und daher ist eine Wirksamkeit erst zu bewerten, wenn sich das System im Einsatz befindet. Daher ist die Wirksamkeit dieser Maßnahmen im Rahmen der regelmäßig durchzuführenden Jours fixes zwischen dem IT-Verantwortlichen [redacted] und dem betrieblichen Datenschutzbeauftragten eine unabdingbare Notwendigkeit.

5.2. Bericht

[redacted] als Verantwortlicher kommt der Dokumentations- und Rechenschaftspflicht gem. § 7 Abs. 2 KDG durch die Erstellung des nachfolgenden, zusammenfassenden DSFA-Berichtes und die Bestätigung der Wirksamkeit der umgesetzten Maßnahmen nach.

[redacted] versteht die Datenschutz-Folgenabschätzung nicht als einmalige Aktion, sondern vielmehr als kontinuierlichen Prozess, der während der Durchführung des Verarbeitungsverfahrens ganz oder teilweise mehrfach durchgeführt wird. Als verantwortliche Stelle hat sie daher ein System implementiert, dass durch die Planung, Umsetzung, Evaluierung und Anpassung gemäß dem PDCA-Zyklus die stetige Optimierung des eingesetzten Verfahrens hinsichtlich der rechtlichen Datenschutzvorgaben sicherstellt.

Um die Frage zu klären, ob für die Verarbeitung durch die Siilo-App die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist, wurde initial eine Schwellwertanalyse durchgeführt. Diese ergab anhand der Zehner-Regel der DSK, dass die Erforderlichkeit zur Durchführung gegeben ist.

Bei der Erstellung der Datenschutz-Folgenabschätzung wurde ein dreiteiliges Verfahren gewählt.

Im ersten Schritt ist ein Prüfteam zusammengestellt worden, dass die Balance zwischen Unabhängigkeit und Verantwortlichkeit sicherstellt. Neben Personen, die selbst in den Prozess eingebunden sind bzw. diesen gut kennen, sind auch Personen aus neutralen Stellen benannt worden.

[redacted]

Die im Verfahren betrachteten Prüfgegenstände sind vor allem hinsichtlich des Zwecks und des Kontextes der Datenverarbeitung bewertet worden. Hierbei wurden die Daten selbst inklusive ihrer Formate beim Speichern und Transferieren, die verwendeten IT-Systeme und deren Schnittstellen sowie die Prozesse und Funktionsrollen überprüft.

Des Weiteren wurde neben der Einzelbetrachtung eine ganzheitliche Sichtweise bei der Überprüfung eingenommen, die neben der technischen Gestaltung auch die organisatorische Gestaltung und die Einbettung des Verfahrens in die Organisation berücksichtigt hat. Bei Unsicherheiten hinsichtlich der Prognose des Verfahrens sind darüber hinaus als typisch erachtete Szenarien für verschiedene Einsatzkontexte bedacht worden.

[redacted] möchte die Siilo-App einführen, um die Kommunikation der am Behandlungsprozess beteiligten noch effizierter darzustellen. Dies soll insgesamt zu einem besseren Behandlungsprozess beitragen und somit die Versorgung des Patienten verbessern.

Im nächsten Schritt sind von der Arbeitsgruppe durch das Verfahren betroffene Akteure identifiziert worden. Dies sind neben an der Entwicklung und Verwendung des Verfahrens beteiligte Personen vor allem solche, die mittelbar oder unmittelbar durch den Einsatz berührt werden. Demnach sind primär die Mitarbeitenden und die Patienten [redacted] betroffen. Unter Umständen werden sekundär auch Daten von Externen Personen im Rahmen eines Konsils verarbeitet.

Das Prüfteam kam bei der Bewertung der Verhältnismäßigkeit der betrachteten Verfahren zu folgendem Ergebnis: Insbesondere die Potenziale zur kollaborativen Arbeit und die Verbesserung der Versorgung der Patienten innerhalb der Corona-Krise zeigen, dass eine schnelle Kommunikation in den Krankenhäusern unerlässlich ist. Ein vergleichbares Produkt mit dem hohen Sicherheitsstand ist aktuell am Markt nicht zu finden.

Um die Gewährleistung der Rechte der Betroffenen sicherzustellen und den eigenen Pflichten nachkommen zu können, folgte die Identifizierung der maßgeblichen Rechtsgrundlagen. Außerdem erfolgte eine differenzierte Abwägung der Interessen von Betroffenen und [redacted].

Die Datenschutz-Folgenabschätzung wurde unter Berücksichtigung der sechs Gewährleistungs- bzw. Schutzziele erstellt. Hierdurch konnten die operativen Risiken in kompakter und methodisch zugänglicher Form explizit gemacht werden, um darauf fußend die Anforderungen für die Maßnahmen zum Datenschutz und der IT-Sicherheit zu benennen.

Bei der Identifizierung der Risiken, in der Regel in Form von etwaigen Angreifern, Angriffsmotiven oder –zielen, wurde konsequent die Perspektive möglicher Betroffener eingenommen. Als mögliche Angreifer sind vor allem Organisationen und Unternehmen bedacht worden, die Daten erfassen, verarbeiten und weitergeben bzw. die im Rahmen des Dienstleistungsvertrages Zugriff auf Daten erhalten bzw. sich Zugriff verschaffen könnten.

[redacted]

Da die Maßnahmen zur Risikoreduktion im weiteren Verlauf innerhalb der einzelnen Maßnahmenbereiche erfolgen, wurden die identifizierten Risiken aggregiert und je Maßnahmenbereich bezüglich ihrer Eintrittswahrscheinlichkeit und der Schwere des eintretenden Schadens bewertet. Das Ergebnis in Form einer Einstufung wurde in Risikomatrizen dargestellt und diente so der Priorisierung der umzusetzenden Maßnahmen. Die Bewertung der Risiken stellte sich demnach wie folgt dar:

- **Sehr hohes Risiko:**
  Sehr hohe Risiken wurden im Rahmen der durchgeführten Datenschutz-Folgenabschätzung nicht identifiziert.
- **Hohes Risiko:**
  Hohe Risiken wurden im Rahmen der durchgeführten Datenschutz-Folgenabschätzung nicht identifiziert.
- **Wesentliches Risiko:**
  Wesentliche Risiken wurden in den Maßnahmenbereichen „Verschlüsselung", „Integrität und Vertraulichkeit" und „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung" identifiziert. Diese resultieren aus der Möglichkeit der Mitarbeitenden durch ein bewusstes, d. h. absichtliches, Fehlverhalten eine Abweichung von den standardmäßigen Werkseinstellungen vorzunehmen. Dies bezieht sich u. a. auf die Möglichkeit eines Screenshots und der Speicherung des Bildes auf dem Endgerät.
- **Begrenztes Risiko:**
  Ein begrenztes Risiko wurde in dem Maßnahmenbereich „Pseudonymsierung" identifiziert, da ausschließlich anonymisierte Daten verarbeitet werden.
- **Geringes Risiko:**
  Geringe Risiken wurden in den Maßnahmenbereichen „Wiederherstellung nach einem technischen Zwischenfall" und „Maßnahmen zur Gewährleistung der Verfügbarkeit" ermittelt.

Da es sich bei der vorliegenden Datenschutz-Folgenabschätzung um keinen strikt linearen oder abgeschlossenen Prozess handelt, wird diese abhängig von der Schwere der ermittelten Risiken für die Betroffenen in regelmäßigen Abständen für die gesamte Dauer des Verarbeitungsvorgangs überprüft und ggf. neu durchgeführt.

Diese Herangehensweise ist auch eine Forderung der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO). Dort ist im § 7 Abs. 1 Satz 1 KDG-DVO festgehalten:

„*Zur Gewährleistung der Sicherheit der Verarbeitung sind die getroffenen technischen und organisatorischen Maßnahmen durch den Verantwortlichen regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren, auf ihre Wirksamkeit zu überprüfen.*"

Um ein Höchstmaß an Transparenz sicherzustellen, verpflichtet sich die verantwortliche Stelle, den hier vorliegenden Bericht auf Anfrage, im Falle des Vorhandenseins von Betriebs- oder Geschäftsgeheimnissen in gekürzter Form, zugänglich zu machen.

Die nächste Überprüfung der durchgeführten Datenschutz-Folgenabschätzung soll am **31. März 2022** durchgeführt werden**.**

[redacted]

[redacted]

Wirtschaftsprüfungsgesellschaft

[redacted]

[redacted]

[redacted]

Anlage 1: Maßnahmenplan

Nachfolgend werden die umzusetzenden Maßnahmen sowie deren Zuständigkeiten und Zieltermine dargestellt.

	Maßnahme	Zuständigkeit	Frist
1.	Bereitstellung der Hinweise zur Datenverarbeitung gem. §§ 15, 16 KDG gegenüber den Beschäftigten.	DSK	Vor Einführung
2.	Information der MAV gem. § 34 MAVO hinsichtlich der geplanten Einführung der Siilo-App.	GF	Vor Einführung
3.	Erarbeitung einer Richtlinie für Beschäftigte zur Nutzung der Siilo-App. Zusätzliche Unterweisung der Mitarbeitenden, dass Daten nicht anderweitig gespeichert werden dürfen.	DSK	Q2 2021
4.	Vereinbarung halbjährlicher Jours fixes zwischen bDSB und IT-Leitung zur Beurteilung möglicher Entwicklungen und der Wirksamkeit umgesetzter Abhilfemaßnahmen.	IT, bDSB	Q2 2021

Abkürzungen:

bDSB betrieblicher Datenschutzbeauftragter
GF Geschäftsführung
IT Geschäftsbereich IT
DSK Datenschutzkoordinator

Anlage 2: Information zur Datenverarbeitung bei der Nutzung von Siilo

Sehr geehrte Mitarbeitende,

[redacted] möchte mit der Einführung der Siilo-App die nächsten wichtigen Schritte in der Digitalisierung gehen. Erklärtes Ziel ist es die neuen Formen der Arbeit effizienter zu gestalten und [redacted] als Ganzes zukunftssicher aufzustellen. Nachfolgend möchten wir Sie gem. § 15 des Gesetzes über den Kirchlichen Datenschutz (KDG) über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der Siilo-App informieren.

Verantwortlicher und Datenschutzbeauftragter

Verantwortlicher für Datenverarbeitung ist die

[redacted]

Bei Fragen zur Datenverarbeitung wenden Sie sich an unseren betrieblichen Datenschutzbeauftragten, den Sie unter folgenden Kontaktdaten erreichen können:

[redacted]

Zweck der Verarbeitung

Der Einsatz der Siilo-App hat den Zweck die Arbeit in [redacted] durch die örtliche und zeitliche Entzerrung der Tätigkeiten effizienter und effektiver zu gestalten. Der jeweilige konkrete Verarbeitungszweck ergibt sich aus den jeweiligen individuellen Tätigkeitsschwerpunkten.

Welche Daten werden verarbeitet?

Bei der Nutzung der Siilo-App werden verschiedene Datenarten verarbeitet. Der Umfang der Daten hängt davon ab, ob Sie mögliche optionale Daten auch hinterlegen.

Folgende personenbezogene Daten (Kunden- und vom System generierte Daten) können Gegenstand der Verarbeitung sein:

- **Pflichtangaben zum Benutzer:** z. B. Vorname, Nachname, E-Mail-Adresse, Mobiltelefonnummer
- **Optionale Angaben zum Benutzer:** z. B. Titel, Fachgebiet, Organisation

- **Support-/Feedbackdaten:** Informationen im Zusammenhang mit Problembehandlungstickets oder an Siilo gesendetem Feedback.
- **Diagnose- und Dienstdaten (Telemetriedaten):** Diagnosedaten im Zusammenhang mit der Dienstnutzung. Diese personenbezogenen Daten ermöglichen es Siilo, Nachrichten zu verschicken und für statistische Auswertungen. Diese Statistiken werden dem Krankenhaus zur Verfügung gestellt, um die Nutzung von Siilo innerhalb der Organisation evaluieren zu können.

Rechtsgrundlagen der Datenverarbeitung

Die Daten der Beschäftigten [redacted] werden im Rahmen der Nutzung der Siilo-App auf Grundlage einer Einwilligung gemäß § 6 Abs. 1 lit b) i. V. m. § 8 KDG verarbeitet. Sollten im Zusammenhang mit der Nutzung der Siilo-App Daten nicht für Datenverarbeitung erforderlich, gleichwohl aber elementarer Bestandteil bei der Nutzung von Siilo sein, so ist § 6 Abs. 1 lit. f) i. V. m. § 6 Abs. 1 lit. g) KDG die Rechtsgrundlage für die Datenverarbeitung. Hierzu haben wir eine ausführliche Abwägung der Interessen [redacted] und den Betroffenen durchgeführt, die auf Anfrage gerne eingesehen werden kann.

Empfänger/Weitergabe von Daten

Personenbezogene Daten, die im Zusammenhang mit der Nutzung der Siilo-App verarbeitet werden, werden nicht an Dritte weitergegeben.

Zur Bereitstellung und Nutzung der Dienste von Siilo ist die Übermittlung personenbezogener Daten an den Auftragsverarbeiter erforderlich. Mit diesem Dienstleister hat [redacted] Vereinbarung zur Datenverarbeitung geschlossen (sog. „Auftragsverarbeitung“ nach § 29 KDG); konkret nutzen wir den nachstehenden Auftragsverarbeiter:

Siilo Holding B.V. Keizersgracht 585, 1072 DR Amsterdam, Niederlande

Nähere Informationen zu der Datenverarbeitung durch Siilo und den datenschutzrechtlichen Angaben finden Sie unter https://www.siilo.com/assets/downloads/Siilo_Kommentar_zum_Whitepaper_der_Datenschutzkonferenz_DSK_18.pdf

Dauer der Speicherung der personenbezogenen Daten

Die Daten, die im Zuge des Registrierungsprozesses und der Nutzung der Siilo-App verarbeitet werden, unterliegen definierten Löschfristen.

Nutzerdaten: Siilo speichert die Nutzerdaten (Daten, die durch die Beschäftigten der [redacted] mit Hilfe der Siilo-App verarbeitet werden) für die Dauer der Nutzung des Dienstes durch den Kunden und bis zu dem Zeitpunkt, an dem alle Kundendaten gelöscht werden. Die Löschung erfolgt nach dem Ende der Lizenzvereinbarung.

Chatinhalte: Inhalte aus Chats (Text, Fotos, Dokumente) können individuell vom Nutzer gelöscht werden. Andernfalls löschen sich diese Daten automatisch nach 30 Tagen.

[redacted]

Ihre Rechte als Betroffene*r

Sie haben das Recht auf Auskunft (§ 17 KDG) über die Sie betreffenden personenbezogenen Daten. Sie können sich für eine Auskunft jederzeit an uns wenden.

Ferner haben Sie ein Recht auf Berichtigung (§ 18 KDG), Löschung (§ 19 KDG) oder auf Einschränkung (§ 20 KDG) der Verarbeitung, soweit Ihnen dies gesetzlich zusteht.

Ein Recht auf **Datenübertragbarkeit** (§ 22 KDG) besteht ebenfalls im Rahmen der datenschutzrechtlichen Vorgaben.

Schließlich haben Sie ein Widerspruchsrecht (§ 23 KDG) gegen die Verarbeitung im Rahmen der gesetzlichen Vorgaben. Die Wahrnehmung des Widerspruchsrecht kann jedoch unmittelbare Auswirkungen auf die Art und Weise, in der Sie Ihre Tätigkeit durchführen, und kann auch die Beendigung des Dienstverhältnisses bedeuten.

Beschwerderecht bei einer Aufsichtsbehörde

Sie haben das Recht, sich über die Verarbeitung personenbezogener Daten durch uns bei einer Aufsichtsbehörde (§ 48 KDG) für den Datenschutz zu beschweren. Die Beschwerde bei der Aufsichtsbehörde kann formlos erfolgen:

Diözesandatenschutzbeauftragte