Datenschutz und Informationssicherheit.
Die digitale Transformation rechtskonform meistern.

Von Steffen Pau[1]

Die Digitalisierung der sozialen Arbeit begegnet uns an vielen Stellen auf unterschiedliche Weise. Die Auswirkungen dieser Sachverhalte erscheinen oft vielfältig und die Bewertung kompliziert. Versucht man aber die Sachverhalte in einzelne Prozessschritte zu zerlegen, werden die Sachverhalte bewertbar.

Bei der Bewertung ist auf die Grundgedanken und Grundsätze des Datenschutzes zurückzugreifen. Ausgangspunkt der Überlegungen ist das Schutzgut des Datenschutzes.

Nach § 1 des Gesetzes über den Kirchlichen Datenschutz (KDG) ist das Ziel des Gesetzes „den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“. Ziel ist also die Sicherstellung der informationellen Selbstbestimmung der Einzelnen – hier der Nutzer der kirchlichen Einrichtungen, also der Patienten. Aber auch die Gruppe der Beschäftigten ist von der Digitalisierung betroffen. Auch deren Rechte sind bei der Bewertung der Digitalisierung mit zu betrachten. Praktisch bedeutet dieses Grundrecht, dass die einzelne Person die Möglichkeit haben muss, über die Verwendung der eigenen personenbezogenen Daten selbst bestimmen zu können.

Gesetzestechnisch arbeitet das neue Datenschutzrecht – ebenso wie schon das alte, bis Mai 2018 anwendbare Recht – mit einem Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Verarbeitung personenbezogener Daten verboten ist, wenn für die konkrete, vorzunehmende Verarbeitung keine konkrete Rechtsgrundlage vorhanden ist. Diese Rechtsgrundlage kann ein Vertrag sein (z.B. der Arbeitsvertrag), es kann eine gesetzliche Regelung sein (z.B. im Sozialrecht) oder – neben den anderen in § 6 KDG aufgezählten Möglichkeiten – eben auch eine Einwilligung der betroffenen Person sein, um deren Daten es geht.

Für die Digitalisierung der sozialen Arbeit bedeutet dies, dass für jede Verarbeitung der personenbezogenen Daten der Betroffenen, also z.B. der Patienten, Heimbewohner, oder eben auch der Beschäftigten, eine Rechtsgrundlage benötigt wird. Liegt eine solche Rechtsgrundlage vor, dann muss noch der Zweck der Verarbeitung festgelegt werden, wenn sich dieser nicht schon aus der Rechtsgrundlage ergibt.

Es kann auch mehrere Zwecke zu unterschiedlichen Rechtsgrundlagen geben. Wenn z.B. im Pflegeheim eine Person dauerhaft neu aufgenommen wird, dann werden verschiedene personenbezogene Daten erfasst. Dabei werden z.B. Kontodaten erfasst, damit die Miete für das Pflegeheim abgebucht werden kann. Zweck der Verarbeitung ist dabei die Zahlung der vereinbarten Gegenleistung für die Überlassung des Heimplatzes und Grundlage für die Verarbeitung der Heimvertrag. Gleichzeitig muss eventuell auch die Anmeldung des Wohnsitzes beim Einwohnermeldeamt von der Einrichtung vorgenommen werden. Zweck dieser Verarbeitung wäre dann die Durchführung der Anmeldung beim Einwohnermeldeamt, Grundlage der Verarbeitung das Bundesmeldegesetz. Wenn evtl. im Anmeldebogen zusätzlich auch nach der Konfession der Person gefragt wird um eine Betreuung durch den zuständigen Seelsorger zu ermöglichen, dann wäre der Zweck der Verarbeitung hier die Ermöglichung einer Begleitung durch einen Geistlichen und Grundlage der Verarbeitung die Einwilligung der Person.

---

[1] Steffen Pau ist Diözesandatenschutzbeauftragter der fünf nordrhein-westfälischen (Erz-)Diözesen und Verbandsdatenschutzbeauftragter des Verbandes der Diözesen Deutschlands.
Dieser Text ist eine überarbeitete Version des Vortrags vom 27.11.2018 im Rahmen des 12. Paderborner caritas.diskurs Ethik „Digitalisierung – Soziale Arbeit im Wandel“ in Schwerte.

An diesem Beispiel wird deutlich, dass die einzelnen Zwecke und die jeweiligen Grundlagen der Verarbeitung sauber aufgeschlüsselt werden müssen, da diese beiden Kriterien immer wieder wichtig werden für den Umgang mit den Daten.
Wenn die Daten, die einmal für einen Zweck erhoben wurden, nun auch noch für einen anderen Zweck verarbeitet werden sollen, dann ist zu prüfen, ob der neue Verarbeitungszweck von der ursprünglichen Rechtsgrundlage und dem ursprünglichen Zweck noch umfasst werden, ob eine Zweckänderung mit einem kompatiblen neuen Zweck vorliegt oder ob im Datenschutzgesetz oder in den Spezialgesetzen die Erlaubnis zu einer Zweckänderung oder eine neue Rechtsgrundlage für den neuen Zweck vorhanden ist. Nur dann dürfen die Daten zu dem neuen Zweck verarbeitet werden, auch wenn dabei auf vorhandene Daten zurückgegriffen wird und die Person nicht erneut nach den Daten gefragt wird.
Rechtsgrundlage und strenge Zweckbindung – diese beiden Prinzipien ziehen sich durch den gesamten Lebenszyklus eines Datums.
Auch bei der Frage, wann personenbezogene Daten zu löschen sind, kommt der festgelegte Zweck wieder zum Tragen. Auch wenn in Zeiten von Big Data das Löschen von Daten fast anachronistisch erscheint, so gewinnt das Thema bei der zunehmenden Profilbildung in sozialen Netzwerken, durch Suchmaschinen oder andere Diensteanbieter immer mehr an Aktualität und Bedeutung.
Das Datenschutzrecht geht beim Löschen von dem einfachen Grundsatz aus, dass personenbezogene Daten zu löschen sind, wenn sich der Zweck erledigt hat, zu dem sie erhoben und verarbeitet wurden.
Erfolgt die Angabe der Adresse im Rahmen eines Gewinnspiels nur und ausschließlich zur Teilnahme an diesem Gewinnspiel, dann muss der Veranstalter des Gewinnspiels die Adresse löschen, wenn das Gewinnspiel beendet ist und die Gewinner benachrichtigt sind. Eine weitere Speicherung oder gar eine Nutzung zu Werbezwecken würden eine Zweck-änderung darstellen, die wieder einer neuen gesetzlichen Grundlage bedürfte.

Datenschutz besteht aber nicht nur aus den rechtlichen Vorgaben, sondern auch aus dem technischen Schutz der Daten. Ohne diesen technischen Schutz wäre der Datenschutz nicht umsetzbar. Die technischen Vorkehrungen zum Schutz der Daten sind daher eine wichtige Grundlage.
§ 26 KDG gibt vor, dass der Verantwortliche technische und organisatorische Maßnahmen zu ergreifen hat. Diese Maßnahmen sind nicht für jede Verarbeitung gleich, sondern müssen sich an dem Risiko orientieren, dem die personenbezogenen Daten durch die konkrete Verarbeitung ausgesetzt sind. Mit diesen Maßnahmen ist dann ein angemessenes Schutzniveau zu erreichen. Im Rahmen der Dokumentationspflicht sind die Risiken und Maßnahmen auch festzuhalten.
§ 27 KDG setzt dann noch zwei Vorgaben der Europäischen Datenschutzgrundverordnung um, die dort mit den Schlagworten „Privacy by Design“ und Privacy by Default“ beschrieben werden. Mit dem Begriff „Privacy by Design“ wird ausgedrückt, dass bei der Planung, Umsetzung und der späteren Durchführung von Verarbeitungen personenbezogener Daten technische und organisatorische Maßnahmen geplant und umgesetzt werden sollen, die es ermöglichen, die Datenschutzgrundsätze des Gesetzes zu erfüllen, damit die konkrete Verarbeitung der Daten den Vorgaben des Gesetzes entspricht. Zu diesen Grundsätzen zählt ja unter anderem auch die Datensparsamkeit.
Der Grundsatz „Privacy by Default“ ergänzt das Prinzip „Privacy by Design“. Die Systeme zur Verarbeitung personenbezogener Daten sollen eben nicht nur eine datenschutzkonforme und datensparsame Verarbeitung der personenbezogenen Daten ermöglichen, sondern solche datenschutzfreundlichen Einstellungen sollen als Standard in den Systemen und Programmen voreingestellt sein.

Während man in der Vergangenheit in den Anwendungen und Apps teilweise die datenschutzfreundlichen Einstellungen suchen und aktivieren musste, soll dies zukünftig die Voreinstellung sein.
Diese eigentlich einfachen Spielregeln für den Umgang mit personenbezogenen Daten werfen in der Praxis aber immer wieder Probleme auf.
Da wären als Beispiel Ortungs- und Trackingsysteme. Mit Hilfe dieser technischen Hilfsmittel, also z.B. von intelligenten Armbändern („Wearables“), können Aufenthaltsorte von Menschen überwacht werden. Der Verantwortliche, der diese Hilfsmittel z.B. in einem Pflegeheim einsetzt, hat den Zweck der Datenverarbeitung zu dokumentieren und welche personenbezogenen Daten das Ortungssystem lokal am Armband und zentral auf einem Server aufzeichnen soll. Besteht der Zweck z.B. in der Lokalisierung dementer Menschen im Notfall, wirft schon die Einschränkung „im Notfall“ die Frage auf, welche Daten denn wie lange vorzuhalten sind. Werden die Daten des Tages aus dem Ortungssystem noch benötigt, wenn die betroffene Person abends wieder wohlbehalten in ihrem Zimmer ist? Zumindest für diesen Zweck erscheint dies fraglich.
Als mögliche Rechtsgrundlage käme auf jeden Fall eine Einwilligung der betroffenen Person in Betracht – bei betreuten Personen die des Betreuers. Ob noch andere Rechtsgrundlagen vorhanden sind, wäre im konkreten Einzelfall zu prüfen.
Ebenfalls zu dokumentieren sind die technisch-organisatorischen Schutzmaßnahmen (Wie sind evtl. Daten auf dem Armband geschützt? Wie ist die Übertragung der Daten auf den Server gesichert? Wie sind die Daten auf dem Server vor unberechtigtem Zugriff geschützt? Besteht ein Nutzer- und Berechtigungskonzept für den Zugriff auf die Daten? Wann werden die Daten gelöscht?). Und damit sind nur einige wenige Aspekte der Umsetzung der technischen und organisatorischen Schutzmaßnahmen genannt.
Auch bei diesem Beispiel ist an mögliche indirekt von der Datenverarbeitung Betroffene zu denken wie z.B. die eigenen Beschäftigten. Bei dem obigen Beispiel wäre eine Verhaltens- und Leistungsüberwachung von Beschäftigten zumindest denkbar.
Wenn z.B. eine Person im Pflegeheim, die ein solches Ortungsarmband mit ständiger Ortbarkeit trägt, von einem Beschäftigten zu einem Arztbesuch begleitet wird, dann ist auch dieser Beschäftigte für die Zeit der Begleitung der Person überwachbar. Der kurze Halt am Zigarettenautomaten auf dem Rückweg vom Arzt wäre für den Dienstgeber also genau nachvollziehbar. Dies könnte für die Mitarbeitervertretungen ein Anlass sein, über Regelungen für die Auswertungsmöglichkeiten der Ortungsdaten bezogen auf die Beschäftigten nachzudenken.
Auch der Einsatz von Pflegerobotern bietet sich als Anwendungsbeispiel an. Während die Kategorie der Pflegeroboter, die unter Anleitung eines Menschen bei mechanischen Tätigkeiten unterstützen, also z.B. den Patienten aus dem Bett heben, wahrscheinlich keine oder nur wenige Daten des Patienten erfassen, kann dies bei „Therapierobotern“ anders aus-sehen. Wenn diese Roboter Bild- und Tonaufnahmen von den Patienten machen, um Verhalten, Gestik, Mimik oder Sprache auszuwerten oder wenn Interaktion mit dem Roboter gemessen und bewertet wird, liegen hier aus datenschutzrechtlicher Sicht andere Kategorien vor.
Aber auch wenn dieser Anwendungsfall komplex erscheint, so wird er mit der Zerlegung des Anwendungsfalles in die einzelnen Datenverarbeitungen und der Frage nach Zweck der Verarbeitung und der Rechtsgrundlage sowie den damit verbundenen und notwendigen Schutzmaßnahmen auch datenschutzrechtlich handhabbar und bewertbar: Wie weit darf die Begleitung oder Beobachtung der Patienten hier gehen? Wie lange müssen solche Daten vorhanden sein für welche Zwecke, auch um ungewollten Profilbildungen vorzubeugen?
Auch in diesem Fall sollten die Rechte der Beschäftigten nicht außer Betracht bleiben, da die Bild- und Tonaufzeichnung auch die Beschäftigten betreffen kann.

Wenn Projekte zur Digitalisierung der sozialen Arbeit in den Einrichtungen eingeführt werden, dann sind die genannten Grundsätze (Rechtsgrundlage, Zweckbindung und technisch-organisatorische Schutzmaßnahmen) zu berücksichtigen. Die rechtzeitige und umfassende Beteiligung des betrieblichen Datenschutzbeauftragten erspart spätere Schwierigkeiten und Verzögerungen in der Umsetzung.
Für die Beschäftigten ergeben sich aber noch weitere indirekte Folgen der Digitalisierung. Die kirchlichen Einrichtungen müssen sich mit der Frage beschäftigen, wie sie – nicht nur unter Datenschutzgesichtspunkten – mit Situationen umgehen, wo z.B. die Pflegekraft in der mobilen Pflege in eine Wohnung hineinkommt, in der eine zu pflegende Person von einer Kamera in der Wohnung beobachtet wird und Alexa oder vergleichbare Dienste im Raum vorhanden sind? Wie können hier die Rechte der Beschäftigten gewahrt bleiben? Ist der Dienstgeber in der Pflicht, den Beschäftigten eine Erledigung der Arbeit ohne (fremde) digitale und dauerhafte Überwachung zu ermöglichen?

Der Datenschutz will die Digitalisierung der sozialen Arbeit weder verbieten noch verhindern. Der Datenschutz will aber die Rechte der betroffenen Personen bei der Verwendung ihrer personenbezogenen Daten wahren.
Und unabhängig von Kostendruck oder der Effizienz und Effektivität digitaler Systeme bleibt der Mensch Mittelpunkt des Handelns in der Kirche und ihren Einrichtungen. Nicht nur in der Pflege oder im Krankenhaus als Patient, sondern auch als Mensch mit dem Recht auf Selbstbestimmung über die Verwendung seiner Daten.
