Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 26.07.2018 in Frankfurt)

Liste von Verarbeitungsvorgängen nach §35 Abs. 5 KDG

Die Konferenz der Diözesandatenschutzbeauftragten beschließt und veröffentlicht die nachfolgende Liste von Verarbeitungsvorgängen nach § 35 Abs. 5 KDG.

Liste von Verarbeitungsvorgängen nach § 35 Abs. 5 KDG

A Gesetzliche Grundlage

Das Gesetz über den kirchlichen Datenschutz (KDG) regelt im § 35 „Datenschutz-Folgenabschätzung und vorherige Konsultation“ die Rahmenbedingungen zur sog. Datenschutz-Folgenabschätzung (kurz: DSFA). Der § 35 KDG nennt dabei die Grundsätze, bei welchen Fällen eine DSFA durchzuführen ist und was diese enthält. Er beschreibt ferner das besondere Verfahren der Konsultation des Verantwortlichen bei der Aufsichtsbehörde bei Fortbestehen hoher Risiken auch nach Anwendung der auf Grundlage der DSFA festgelegten verhältnismäßigen technischen und organisatorischen Maßnahmen.

Mit diesem Dokument kommen die Diözesandatenschutzbeauftragten dem Auftrag aus § 35 Abs. 5 KDG nach und legen eine Positivliste von Verarbeitungsvorgängen vor, bei denen aus Sicht der Diözesandatenschutzbeauftragten immer eine DSFA durchzuführen ist. Diese Liste orientiert sich an den bislang bekannten Vorgaben der staatlichen Aufsichtsbehörden.

Führt ein Verantwortlicher Verarbeitungsvorgänge aus, die in § 35 Abs. 4 KDG oder der vorliegenden Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Datenschutzaufsicht wegen Verstoßes gegen § 35 Abs. 1 KDG von ihren Abhilfebefugnissen gemäß § 47 KDG einschließlich der Verhängung von Geldbußen gemäß § 51 KDG Gebrauch machen. Gegen einen derartigen Beschluss der Datenschutzaufsicht steht der Rechtsweg gemäß § 49 KDG offen.

Die in dem Dokument dargestellte Liste wird nachfolgend als „Muss-Liste“ oder „Positiv-Liste“ bezeichnet.

B Ziel dieses Dokuments

Ziel des Dokuments ist es, eine an den Listen der staatlichen Aufsichtsbehörden orientierte Liste zu entwickeln, die an die Situation der kirchlichen Einrichtungen im Geltungsbereich des KDG angepasst ist.

Auf Grund der Schnelllebigkeit im digitalen Umfeld kann dieses Dokument nur als „lebendiges“ Papier angesehen werden, das ständigen Änderungskontrollen hinsichtlich der Aufnahme neuer Verarbeitungen in die Liste der Verarbeitungsvorgänge unterliegt. Änderungen an Einträgen der Muss-Liste werden dokumentiert, so dass die Muss-Liste eine entsprechende Versionshistorie erhalten wird.

Wichtiger Hinweis: Wird die Verarbeitungstätigkeit eines Verantwortlichen in der vorliegenden Liste nicht aufgeführt, so ist hieraus nicht der Schluss zu ziehen, dass keine DSFA durchzuführen wäre. Stattdessen ist es Aufgabe des Verantwortlichen, als ersten Schritt einer DSFA einzuschätzen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen aufweist und damit die Voraussetzungen des § 35 Abs. 1 Satz 1 KDG erfüllt.

C Liste nach Art. 35 Abs. 5 KDG

Die „Artikel 29-Gruppe“, der Vorläufer des Europäischen Datenschutzausschusses als Zusammenschluss aller nationalen Datenschutz-Aufsichtsbehörden in der EU, hat in seinem Working Paper (WP) 248 vom 4. April 2017 maßgebliche Kriterien zur Einordnung von Verarbeitungsvorgängen wie folgt formuliert:

1. Bewerten oder Einstufen (Scoring)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche oder höchst persönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

Erfüllt ein Verarbeitungsvorgang zwei oder mehr dieser Kriterien, so ist vielfach ein hohes Risiko gegeben und aus Sicht der Artikel 29-Gruppe eine DSFA durch den Verantwortlichen durchzuführen. In wenigen Einzelfällen mag es jedoch auch vorkommen, dass nur eines der genannten Kriterien erfüllt wird und dennoch auf Grund eines hohen Risikos des Verarbeitungsvorgangs eine DSFA notwendig wird.

Das Ergebnis dieses ersten Schrittes und die zugrundeliegenden Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.

Die folgende Liste von Verarbeitungsvorgängen einschließlich der genannten Beispiele ist nicht als abschließende Liste von Anwendungsfällen zu sehen, in denen einige der o.a. Kriterien als erfüllt erkannt werden, sondern soll beispielhaft verdeutlichen, in welchen Formen die Ausprägungen der Kriterien angetroffen werden können. Dementsprechend ergibt sich für Verantwortliche, die prüfen, ob für einen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung durchzuführen ist, die folgende Prüfreihenfolge:

1. Prüfung, ob der Verarbeitungsvorgang einen Fall nach § 35 Abs. 4 KDG darstellt oder in der folgenden Liste genannt ist.
2. Wenn nein, dann Prüfung anhand der o.a. Kriterien, ob dennoch ein hohes Risiko nach § 35 Abs. 1 KDG vorliegt.

Nur wenn beide Prüfungen negativ ausfallen, muss eine Datenschutz-Folgenabschätzung nicht durchgeführt werden.

Nach § 6 Abs. 1 KDG ist eine Verarbeitung nur dann rechtmäßig, wenn einer der dort genannten Erlaubnistatbestände vorliegt. Mit der vorliegenden Liste wird keine Aussage darüber getroffen, ob für einen Verarbeitungsvorgang eine Rechtsgrundlage vorliegt oder nicht. Ein Eintrag auf der Liste bedeutet daher weder, dass eine Verarbeitung verboten ist, noch dass ein Verarbeitungsvorgang allein auf der Grundlage einer Datenschutz-Folgenabschätzung durchgeführt werden kann.

Zum Aufbau der Liste:

In der ersten Spalte erfolgt zur einfachen Bezugnahme eine Nummerierung. In der zweiten Spalte findet sich die maßgebliche Beschreibung des Verarbeitungsvorgangs. Fällt ein Verarbeitungsvorgang unter diese Beschreibung, dann ist für ihn eine Datenschutz-Folgenabschätzung durchzuführen. Lässt sich ein Verarbeitungsvorgang nicht unter die zweite Spalte subsumieren, ist nach dem oben dargestellten Schema weiter zu prüfen. Die dritte und die vierte Spalte enthalten zur Veranschaulichung typische Einsatzfelder und Beispiele für Verarbeitungsvorgänge – vorzugsweise aus dem kirchlichen Bereich - die unter die zweite Spalte zu subsumieren wären.

In der fünften Spalte wird auf diejenigen der o.a. neun Kriterien referenziert, die bei dem jeweiligen Verarbeitungsvorgang typischerweise erfüllt werden und die deshalb dazu führen, den Vorgang in die Liste aufzunehmen.

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
1.	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß §§ 11 und 12 KDG handelt	Krankenhäuser, Praxisverbünde, Apotheken-dienste Sozialleistungs-träger	Ein Praxisverbund führt eine gemeinsame Patientenkartei. Eine Betreuungs-einrichtung übermittelt Bewohnerdaten an einen Apothekendienst zur Medikamentenversorgung	4, 5
2.	Umfangreiche Verarbeitung von Daten über den Aufenthalt von Personen	Ambulante Dienste	Ein Dienstleister erfasst die Standorte, Fahrstrecken und Verweilzeiten der Mitarbeiter um daraus eine Routenoptimierung zu errechnen.	3,5,8

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
		Fahrzeugdaten-verarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungs-sensoren in Dienstfahr-zeugen	Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.	5,8
		Demenz-überwachung	Eine Betreuungseinrichtung erfasst laufend den Aufenthalt von Bewohnern mit Weglauftendenz	3,7
3.	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und • der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können	Verknüpfung von Beratungs-angeboten	Eine Beratungsstelle gleicht die erhobenen Daten aus verschiedenen Beratungsangeboten (z.B. Suchthilfe und Schuldnerberatung) ohne das Wissen der Betroffenen miteinander ab, um zusätzliche Beratungsansätze zu finden.	2,4,6,8
		Fundraising	Caritative Organisationen nutzen nicht selbst erhobene Daten um die Betroffenen um eine Spende zu bitten	5,6

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
4.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG durch Auftrags-verarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Art. 48 DSGVO zu exportieren oder offenzulegen	Einsatz von Dienstleistern mit Sitz außerhalb der EU durch pädagogische Einrichtungen	Datenverarbeitung von personenbezogenen Schülerdaten gemäß Art. 11 KDG in einer öffentlichen Cloud (z. B. in einem digitalen Klassenbuch – Dokumentation von Fehlzeiten, Entschul-digungen oder anderen Dokumentationen).	4,6,8
		Medizinische Leistungs-erbringer	Abwicklung einer Tele-Sprechstunde mit Daten- oder Dokumentenübertragung	
5.	Mobile und für die Betroffenen intransparente opto-elektronische Erfassung öffentlicher Bereiche	Einsatz mobiler Videotechnik	Ein ambulanter Dienst rüstet seine Mitarbeiter mit Videokameras aus, um diese bei der Dokumen-tation ihrer Tätigkeiten zu unterstützen.	3,7,8
		Fahrzeugdaten-verarbeitung – Umgebungs-sensoren	Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Park-plätze oder verbessert Algorithmen zum automatisierten Fahren.	3,5,8
6.	Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	Betrieb von Bewertungsportal en	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Pfleger, Selbstständige oder Lehrer.	1,6,9

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
7.	Verarbeitung von umfangreichen Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen	Zentrale Aufzeichnung des Internetverlaufs und der Aktivitäten am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen.	3,4,5,8
		Geolokalisierung von Beschäftigten	Eine Einrichtung lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Rettungsdienst, Ersthelfer), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung) oder zur Überwachung kritischer Zeitabläufe (Transport von Blutkonserven, Spenderorganen) oder zur Koordination/Optimierung von Arbeitseinsätzen im Außendienst.	

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
8.	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	Big-Data-Analyse von Kunden- und sonstigen personenbez. Daten, die mit Angaben aus Drittquellen angereichert wurden	Quartiersanalyse: In einem größeren Wohngebiet werden die Daten von Wohnungs-gesellschaften, Meldebehörden, Einzelhändlern, sozialen Diensten etc. zusammengeführt, um kommunalen Handlungs-bedarf zu ermitteln	1,5,6
9.	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Die Telefonseelsorge ermittelt mit Hilfe einer Stimmfrequenzanalyse die Stimmungslage des Anrufers.	1,3,4,8
10.	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	Erfassung des Kauf- oder Freizeit-verhaltens unterschiedlicher Personenkreise zur Profilbildung und Kunden-bindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Verbund sozialer Einrichtungen gibt eine „Ehrenamtskarte“ aus, mit der Vergünstigungen in öffentlichen Freizeit-einrichtungen und bei bestimmten Einkaufs-möglichkeiten verbunden sind.	3,5

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
11.	Anonymisierung von besonderen personenbezogenen Daten nach § 11 KDG, falls diese (ggf. vermeintlich) anonymen Daten an Dritte weitergegeben oder zu nicht nur internen statistischen Zwecken verarbeitet werden sollen. Risiko: Beim Dritten können Daten aus anderen Quellen vorliegen, durch deren Verknüpfung die Anonymisierung aufgehoben werden könnte.	Weitergabe von anonymisierten Daten an einen Dachverband	Eine Beratungsstelle gibt anonymisierte Daten über Klienten zwecks statistischer Auswertung an einen Dachverband. Dort liegen auch Daten anderer Stellen vor, die durch eine Verknüpfung Rückschlüsse auf die vermeintlich anonymisierten Daten erlauben.	4,6
12.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG - auch wenn sie nicht als „umfangreich“ im Sinne des § 35 Abs. 4 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder bietet eine App an, um Patienten detailliert und systematisch zu behandeln.	4,8
		Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Eine Einrichtung organisiert und bewirbt ein Fitnessprogramm, bei dem die sportlichen Aktivitäten der Mitarbeiter über ein Fitnessarmband erfasst, zentral ausgewertet und gegen ein Ziel gemessen werden.	1,2,3,4
13.	Verarbeitung von Daten gemäß §§ 11 und 12 KDG - auch wenn sie nicht als „umfangreich“ im Sinne des § 35 Abs. 4 lit. b) anzusehen ist - sofern die Daten dazu verwendet werden, die Leistungsfähigkeit von Beschäftigten zu bestimmen	Erfassung von Leistungsdaten in medizinischen oder pflegerischen Berufen	Ein ambulanter Dienst setzt eine minutengenaue elektronische Leistungserfassung an.	1,3,8
14.	Verarbeitung von Daten der Personenstands- und Melderegister sowie anderer Stellen, die Daten aus diesen Registern in großem Umfang oder Meldedaten mit Sperrvermerken gemäß § 51 Abs. 1 und 5 Bundesmeldegesetz verarbeiten	Pfarramtlicher Bereich	Ein Pfarramt nutzt Meldedaten zur Durchführung einer Werbeaktion für kirchliche Vereine	4,5

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele	Erfüllte Kriterien
15.	Umfangreiche Verarbeitung von Daten über Kinder	Schulsozialarbeit	Ein Caritas-Verband wird mit der Über-Mittag- und Hausaufgabenbetreuung von Schülern eines Schulzentrums beauftragt. Dazu werden umfang-reiche Schülerdaten übergeben.	4,5,7
		Kinderheime	Der Betreiber eines Kindererholungsheims plant ein neues IT-System zur Verwaltung und Abrechnung der Aufenthalte	5,7

Frankfurt, 26.07.2018

Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22