KDG-Praxishilfe 11

Datenschutz-Folgenabschätzung

nach dem neuen Gesetz über den kirchlichen Datenschutz

Stand 11/2017

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Inhalt

Praxishilfe 11
Datenschutz-Folgenabschätzung nach dem kirchlichen Datenschutzgesetz (KDG)

Herausgegeben von
der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

So erreichen Sie uns:
Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Autor dieser Praxishilfe:
Der Diözesandatenschutzbeauftragte für die norddeutschen (Erz-)Bistümer

Diese Praxishilfe der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands dient als erste Orientierung, wie nach Auffassung der Diözesandatenschutzbeauftragten das neue Gesetz über den kirchlichen Datenschutz (KDG) im praktischen Vollzug angewendet werden sollte. Sie kann noch keine verbindliche Auslegung bieten, sondern stellt die gegenwärtige Interpretation der neuen Vorschriften durch die Diözesandatenschutzbeauftragten dar.

Revision 1.0 / 07.12.2017

Datenschutz-Folgenabschätzung nach dem Kirchlichen Datenschutzgesetz (KDG)

Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung wird an die Stelle der bisher in § 3 Abs. 5 und 6 KDO geregelten „Vorabkontrolle“ treten. Sie ist nur für bestimmte, risikobehaftete Verfahren durchzuführen. § 35 Abs. 1 KDG legt grundsätzlich die Fälle fest, bei denen sie durchgeführt werden **muss**. Im Einzelnen wird hierbei angegeben:

- Es muss ein **hohes Risiko für die Rechte und Freiheiten der Personen** gegeben sein. Dabei sind die Art, der Umfang, der Umstand und der Zweck der Verarbeitung maßgeblich.
- Insbesondere bei der Verwendung neuer Technologien dürfte in der Regel eine erstmalige Absicherung hinsichtlich der zu erwartenden Risiken erforderlich sein.

Wann ist von einem Risiko für die Rechte und Freiheiten der Betroffenen auszugehen? Der Erwägungsgrund 75 zur Datenschutzgrundverordnung (DS-GVO) gibt an, dass dies anzunehmen ist, wenn die Datenverarbeitung zu einem physischen, materiellen oder immateriellen Schaden führen könnte und bezeichnet hierfür wichtige Risiken. So ist die Datenschutz-Folgenabschätzung immer dann vorzunehmen, wenn der Datenverarbeitungsvorgang zu Lasten der betroffenen Personen

- eine Diskriminierung verursachen könnte;
- eine Gefahr eines Identitätsdiebstahls oder -betruges darstellt;
- zu einem finanziellen Verlust oder
- einer Rufschädigung führen kann;
- die Vertraulichkeit personenbezogener Daten, die einem besonderen Berufsgeheimnis unterliegen, gefährden würde;
- eine unbefugte Aufhebung einer Pseudonymisierung ermöglicht;
- ihn daran hindert, die Verwendung seiner Daten zu kontrollieren;
- Persönlichkeitsprofile unter Verwendung besonderer Kategorien personenbezogener Daten erstellt;
- Daten schutzbedürftiger Personen, insbesondere Kinder verarbeitet;
- eine große Menge von Daten einer Vielzahl von betroffenen Personen beinhaltet.

Da dieser Erwägungsgrund entscheidende Bedeutung für die Notwendigkeit und Verpflichtung zu einer Datenschutz-Folgenabschätzung hat, wird er hier noch einmal in seinem vollständigen Wortlaut wiedergegeben:

> *(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.*

Auf Grund dieser Erwägungen benennt § 35 Abs. 4 KDG eine Reihe von Verfahren, bei denen **in jedem Fall** eine Datenschutz-Folgenabschätzung vorzunehmen ist:

- Automatisierte Verarbeitungen, bei denen die systematische und umfassende **Bewertung persönlicher Aspekte** natürlicher Personen zur Grundlage von Entscheidungen gemacht werden, die für die Betroffenen Rechtswirkung entfalten oder sie in vergleichbarer Form beeinträchtigen. Profiling wird hier ausdrücklich als Anwendungsfall genannt.
- Eine umfangreiche Verarbeitung **besonderer Kategorien** personenbezogener Daten.
- Die systematische umfangreiche **Überwachung** öffentlicher Bereiche. Hierzu zählt im Besonderen auch die Videoüberwachung.

Zudem sollen die Diözesandatenschutzbeauftragten nach § 35 Abs. 5 KDG eine Liste von Verarbeitungsvorgängen erstellen und veröffentlichen, bei denen in jedem Fall eine Datenschutz-Folgenabschätzung durchzuführen ist (sog. „**Positivliste**“). Für Verfahren bei denen keine Folgeabschätzung erforderlich ist, kann ebenso eine zu veröffentlichende Liste erstellt werden (sog. „**Negativliste**“). Die kirchlichen Aufsichtsinstanzen werden solche Listen gemeinsam erstellen. Dabei werden sie sich mit den Bundes- und Landesbeauftragten für Datenschutz abstimmen und zudem die Empfehlungen des EU-Datenschutz-Ausschusses (Art. 29 Gruppe) mit einbeziehen. Jede Einrichtung hat sich über die Festlegungen der Diözesandatenschutzbeauftragten zu informieren und ist **verpflichtet** eine Folgenabschätzung vorzunehmen, wenn das Verfahren auf der Postivliste vermerkt ist.

Ausgestaltung der Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung (DSFA) besteht aus zwei wesentlichen Teilen, der Risikoanalyse und aus geeigneten Maßnahmen zur Verminderung oder gar Ausschaltung der Risiken.

Die **Risikoanalyse** soll zunächst die Gefahren, die den zu verarbeitenden personenbezogenen Daten drohen, **nach objektiven Kriterien ermitteln**. Dabei ist es wichtig, dass dabei folgende Punkte berücksichtigt werden:

Welche Schäden sind nach objektiven Maßstäben zu erwarten?

- Aufgrund der Art der Datenverarbeitung
- Durch den Umfang der Datenverarbeitung
- Durch den Zweck der Datenverarbeitung

Welche Umstände sind in der Lage einen Schaden hervorzurufen?

- Das Versagen des gesamten Systems oder seiner einzelnen Teile
- Der unzulässige Eingriff von vorhandenen oder ehemaligen Mitarbeitern
- Ein unzulässiger Eingriff von außen (z.B. Hacker)
- Menschliche Fahrlässigkeit durch falsche Bedienung des Systems
- Menschliche Fahrlässigkeit durch unzulässige Auskunftserteilung an Dritte

Zu betrachten ist hierbei allein das „Datenschutzrisiko“ und nicht der möglicherweise entstehende Finanzschaden, der die Einrichtung treffen könnte. Im Mittelpunkt steht der Mensch in seinen Rechten und Grundfreiheiten! Daher sind aus seiner Sicht die Risiken zu ermitteln.

Erforderlich ist nach § 35 Abs. 7 KDG daher mindestens eine systematische Beschreibung der geplanten Verarbeitungsvorgänge. Weiterhin sind die Zwecke der Datenverarbeitung vollständig anzugeben und eine Bewertung der eingesetzten Technik zur Erreichung der Ziele durchzuführen. Selbstverständlich hat dabei hat auch eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen stattzufinden.

Sind die realistischerweise bestehenden Risiken ermittelt, so sind alle Maßnahmen vorzusehen, die geeignet sind, die Gefahren zu mindern oder gar auszuschließen (Risikoreduktion). Der § 35 Abs. 7 bestimmt unter lit. d), dass eine Folgenabschätzung auch die geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren zum Schutz personenbezogener Daten umfassen muss. Es muss darüber hinaus der Nachweis erbracht werden, dass die Bestimmungen dieses Gesetzes eingehalten werden. Hierzu gehört ganz wesentlich auch die Beachtung der §§ 26, 27 KDG.

Ergibt die Datenschutz-Folgenabschätzung, dass ein hohes Datenschutzrisiko gegeben ist und der Verantwortliche keine Maßnahmen zu ihrer Eindämmung trifft oder treffen kann, so besteht eine Mitteilungspflicht nach § 35 Abs. 11 an die zuständige Datenschutzaufsicht. Der Diözesandatenschutzbeauftragte ist dann in jedem Fall vor Beginn der Verarbeitung zu konsultieren.

Verfahren

Die Durchführung einer Datenschutz-Folgenabschätzung ist nach § 35 Abs. 1 KDG Aufgabe des Verantwortlichen. Im Gegensatz zum bisher geltenden Recht des § 3 Abs. 6 KDO liegt die Verantwortung für die Durchführung des Verfahrens nicht mehr beim betrieblichen Datenschutzbeauftragten. Ist ein solcher bestellt worden, so muss er aber für der Folgenabschätzung als Berater nach § 35 Abs. 2 KDG hinzugezogen werden. Eine solche Beratung sollte vor allem in folgenden Fragen in Anspruch genommen werden:

- Ist die Durchführung einer Datenschutz-Folgenabschätzung erforderlich?
- Entwicklung einer Strategie für die Durchführung
- Sollten fachbezogene externe Dienstleister hinzugezogen werden?
- Wurden ausreichende Sicherheitsvorkehrungen getroffen, um die Risiken aus Sicht der Betroffenen zu minimieren?

- Wurde die Folgenabschätzung korrekt durchgeführt und stehen die hierbei getroffenen Feststellungen im Einklang mit den Vorgaben des KDG und ihrer Durchführungsverordnung?

Diese Neuregelung ist angesichts der Bedeutung der Folgenabschätzung konsequent. Die Durchführung dieses Verfahrens führt zur Bewertung aller technischen Prozesse der Datenverarbeitung, einschließlich der eingesetzten IT-Systeme, der Softwareprogramme, der geplanten Datenflüsse und vielem anderen mehr. Es geht letztendlich um die Feststellung der Systemgrenzen. Diese Aufgabe kann hinsichtlich ihrer Komplexität nicht allein von einem betrieblichen Datenschutzbeauftragten durchgeführt werden. Hier müssen zugleich alle datenschutzrechtlich beteiligten Personen, wie IT-Techniker, Systemadministratoren, Organisationsleiter aus der Verwaltung und jeder, der sonst für dieses Verfahren Verantwortung trägt, beteiligt werden. Schließlich geht es um die grundsätzliche organisatorische Ausrichtung der Datenverarbeitungsstelle und das Vertrauen der Mitarbeiter und der betroffenen Personen in eine rechtlich zulässige Ausgestaltung der Verarbeitung personenbezogener Daten.

Zur Unterstützung hierbei, gibt § 35 Abs. 3 KDG dem Verantwortlichen die Möglichkeit, die Datenschutzaufsicht zu beteiligen. Dies kann aber erst dann geschehen, wenn der betriebliche Datenschutzbeauftragte angehört worden ist. Dadurch soll sichergestellt werden, dass von einer Beteiligung der Aufsicht nur in gravierenden Fällen Gebrauch gemacht wird.

Die Diözsandatenschutzbeauftragten werden gemeinsam mit den übrigen Aufsichtsbehörden ein gemeinsames Muster für die Durchführung solcher Verfahren entwickeln.

Merkposten zur Datenschutz-Folgenabschätzung (DSFA)

- Eine DSFA ist durchzuführen, wenn das Verfahren in einer Positivliste der Diözesandatenschutzbeauftragten aufgeführt wird.
- Eine DSFA ist nicht durchzuführen, wenn die geplante Art der Verarbeitung durch Veröffentlichung in einer Negativliste der Diözesandatenschutzbeauftragten erscheint.
- Wird eine Datenverarbeitung angestrebt, die nicht in einer Postitiv- oder Negativliste aufgeführt ist, so ist eine eigenständige Prüfung ihrer Notwendigkeit nach § 35 Abs.1 KDG durchzuführen. Hierbei sollten auch die Ausführungen im Erwägungsgrund 75 zur Datenschutzgrundverordnung berücksichtigt werden.
- Stellt sich heraus, dass eine DSFA notwendig ist, sollte sie im Sinne der von den Aufsichtsbehörden festgelegten Verfahren und unter Verwendung, der zur Verfügung gestellten Muster, durchgeführt werden. Die Verfahrensbeschreibung darf dabei inhaltlich nicht unterschritten werden. Es muss in jedem Fall eine genaue Risikoanalyse stattfinden und Maßnahmen zur Bewältigung der Risiken vorgesehen sein.
- Bei risikobehafteten Datenverarbeitungen ist deren Rechtmäßigkeit und die Übereinstimmung mit den Grundsätzen des KDG nur durch eine DSFA nachzuweisen.
- Die Nichtdurchführung einer notwendigen DSFA ist bußgeldbewehrt.

§ 35
Datenschutz-Folgenabschätzung und vorherige Konsultation

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des betrieblichen Datenschutzbeauftragten ein, sofern ein solcher benannt wurde.

(3) Ist der Verantwortliche nach Anhörung des betrieblichen Datenschutzbeauftragten der Ansicht, dass ohne Hinzuziehung der Datenschutzaufsicht eine Datenschutz-Folgenabschätzung nicht möglich ist, kann er der Datenschutzaufsicht den Sachverhalt zur Stellungnahme vorlegen.

(4) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) 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) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß § 12 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(5) Die Datenschutzaufsicht soll eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine Datenschutz-Folgenabschätzung gemäß Absatz 1 durchzuführen ist. Sie kann ferner eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist.

(6) Die Listen der Datenschutzaufsicht sollen sich an den Listen der Aufsichtsbehörden des Bundes und der Länder orientieren. Gegebenenfalls ist der Austausch mit staatlichen Aufsichtsbehörden zu suchen.

(7) Die Datenschutz-Folgenabschätzung umfasst insbesondere:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) 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 dieses Gesetz eingehalten wird.

(8) Der Verantwortliche holt gegebenenfalls die Stellungnahme der betroffenen Person zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder kirchlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(9) Falls die Verarbeitung auf einer Rechtsgrundlage im kirchlichen Recht, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 5 nicht.

(10) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

(11) Der Verantwortliche konsultiert vor der Verarbeitung die Datenschutzaufsicht, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hat, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

§ 4
Begriffsbestimmungen

Im Sinne dieses Gesetzes bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. „besondere Kategorien personenbezogener Daten“ personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie personenbezogener Daten.

3. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
4. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
5. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
6. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
7. „Anonymisierung“ die Verarbeitung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können;
8. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
9. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
10. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
11. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht;

12. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
13. “Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;
14. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
15. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
16. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
17. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;
18. „Drittland“ ein Land außerhalb der Europäischen Union oder des europäischen Wirtschaftsraums;
19. „Unternehmen“ eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;
20. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
21. „Datenschutzaufsicht“ die von einem oder mehreren Diözesanbischöfen gemäß §§ 42 ff. errichtete unabhängige, mit der Datenschutzaufsicht beauftragte kirchliche Behörde;
22. „Diözesandatenschutzbeauftragter“ den Leiter der Datenschutzaufsicht;
23. „Betrieblicher Datenschutzbeauftragter“ den vom Verantwortlichen oder vom Auftragsverarbeiter benannten Datenschutzbeauftragten;

24. „Beschäftigte“ insbesondere
    a) Kleriker und Kandidaten für das Weiheamt,
    b) Ordensangehörige, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind,
    c) in einem Beschäftigungsverhältnis oder in einem kirchlichen Beamtenverhältnis stehende Personen,
    d) zu ihrer Berufsbildung tätige Personen mit Ausnahme der Postulanten und Novizen,
    e) Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitanden),
    f) in anerkannten Werkstätten für Menschen mit Behinderungen tätige Personen,
    g) nach dem Bundesfreiwilligendienstgesetz oder dem Jugendfreiwilligendienstegesetz oder in vergleichbaren Diensten tätige Personen sowie Praktikanten,
    h) Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
    i) sich für ein Beschäftigungsverhältnis Bewerbende sowie Personen, deren Beschäftigungsverhältnis beendet ist.

Weitere Praxishilfen:

01 Wichtige Schritte bis zum In-Kraft-Treten des KDG

02 Der Betriebliche Datenschutzbeauftragte nach dem KDG

03 Verantwortlichkeiten nach dem KDG

04 Auftragsverarbeitung nach dem KDG

05 Verzeichnis der Verarbeitungstätigkeiten nach dem KDG

06 Betroffenenrechte nach dem KDG

07 Transparenz- und Dokumentationspflichten nach dem KDG

08 Datenübermittlung in Drittländer

09 Befugnisse und Sanktionsmöglichkeiten der Aufsicht nach dem KDG

10 Umgang mit Datenpannen nach dem KDG

12 Neue Anforderungen an die IT-Sicherheit nach dem KDG

13 Datenschutzorganisation und -managementsysteme nach dem KDG

14 Der Rechtsweg nach der KDSGO

15 Technischer Datenschutz nach dem KDG

16 Begriffe im neuen KDG

17 Rechtmäßigkeit der Verarbeitung/Einwilligung

18 Nutzung der Daten für Werbezwecke

Diese Schriftenreihe wird gemeinsam herausgegeben von:

Diözesandatenschutz-
beauftragter für die nord-
deutschen Diözesen

Diözesandatenschutz-
beauftragter für die ost-
deutschen Diözesen

Diözesandatenschutzbeauftragter für die
nordrhein-westfälischen Diözesen

Diözesandatenschutzbeauftragter
für die bayerischen Diözesen

Gemeinsame Datenschutzstelle der (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stutt-
gart, Speyer und Trier