

- b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
 - c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und der dort getroffenen geeigneten Garantien;
 - d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 26 dieses Gesetzes.
- (3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
- (4) Der Verantwortliche und der Auftragsverarbeiter stellen dem betrieblichen Datenschutzbeauftragten und auf Anfrage der Datenschutzaufsicht das in den Absätzen 1 und 2 genannte Verzeichnis zur Verfügung.
- (5) Die in den Absätzen 1 und 2 genannten Pflichten gelten für Unternehmen oder Einrichtungen, die 250 oder mehr Beschäftigte haben. Sie gilt darüber hinaus für Unternehmen oder Einrichtungen mit weniger als 250 Beschäftigten, wenn durch die Verarbeitung die Rechte und Freiheiten der betroffenen Personen gefährdet werden, die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung besondere Datenkategorien gemäß § 11 bzw. personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des § 12 beinhaltet.

§ 32

Zusammenarbeit mit der Datenschutzaufsicht

Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage der Datenschutzaufsicht mit dieser bei der Erfüllung ihrer Aufgaben zusammen.

§ 33

Meldung an die Datenschutzaufsicht

- (1) Der Verantwortliche meldet der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Erfolgt die Meldung nicht binnen 72 Stunden, nachdem die Verletzung des Schutzes personenbezogener Daten bekannt wurde, so ist ihr eine Begründung für die Verzögerung beizufügen.
- (2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese unverzüglich dem Verantwortlichen.
- (3) Die Meldung gemäß Absatz 1 enthält insbesondere folgende Informationen:
- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b) den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer

sonstigen Anlaufstelle für weitere Informationen;

- c) eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (4) Wenn und soweit die Informationen nach Absatz 3 nicht zeitgleich bereitgestellt werden können, stellt der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.
- (5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Datenschutzaufsicht die Überprüfung der Einhaltung der Bestimmungen der Absätze 1 bis 4 ermöglichen.

§ 34

Benachrichtigung der betroffenen Person

- (1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.
- (2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in § 33 Absatz 3 lit. b), c) und d) genannten Informationen und Maßnahmen.
- (3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:
- a) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen getroffen und auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
 - b) der Verantwortliche hat durch nachträglich getroffene Maßnahmen sichergestellt, dass die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 nicht mehr gefährdet sind;
 - c) die Benachrichtigung erfordert einen unverhältnismäßigen Aufwand. In diesem Fall hat ersatzweise eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.
- (4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Datenschutzaufsicht unter Berücksichtigung

der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

§ 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.

Abschnitt 3

Betrieblicher Datenschutzbeauftragter

§ 36

Benennung von betrieblichen Datenschutzbeauftragten

- (1) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. a) benennen schriftlich einen betrieblichen Datenschutzbeauftragten.
- (2) Kirchliche Stellen im Sinne des § 3 Absatz 1 lit. b) und c) benennen schriftlich einen betrieblichen Datenschutzbeauftragten, wenn
 - a) sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen,
 - b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer