

# Datenschutzordnung (DSO)

*des Bundes Freier evangelischer Gemeinden in Deutschland KdÖR*

Diese Datenschutzordnung wurde von der Bundesleitung am 27. April 2018 beschlossen und ist am 24. Mai 2018 in Kraft getreten.

Sie ersetzt die Datenschutzordnung des Bundes in der Fassung vom 08. August 2008.

## Inhalt

Inhaltsverzeichnis .....	1
Präambel .....	3
ERSTER ABSCHNITT: ALLGEMEINE BESTIMMUNGEN.....	3
§ 1. Gegenstand, Ziele und Anwendungsbereich.....	3
§ 2. Verantwortlichkeit für die Durchführung des Datenschutzes .....	4
§ 3. Begriffsbestimmungen.....	4
§ 4. Seelsorgegeheimnis und Amtsverschwiegenheit .....	5
§ 5. Rechtmäßigkeit der Verarbeitung .....	6
§ 6. Bedingungen für die Einwilligung.....	7
§ 7. Datenübermittlung an Stellen des Bundes, sowie Dritte .....	8
§ 8. Verarbeitung besonderer Daten .....	8
ZWEITER ABSCHNITT: RECHTE DER BETROFFENEN PERSON .....	10
§ 9. Transparente Information, Kommunikation .....	10
§ 10. Informationspflichten bei Datenerhebung.....	10
§ 11. Auskunftsrecht der betroffenen Person .....	11
§ 12. Recht auf Berichtigung .....	12
§ 13. Recht auf Löschung .....	12
§ 14. Recht auf Einschränkung der Verarbeitung .....	13
§ 15. Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung.....	13
§ 16. Widerspruchsrecht.....	13
DRITTER ABSCHNITT: PFLICHTEN DER VERANTWORTLICHEN UND AUFTRAGSVERARBEITER ....	14
§ 17. Datengeheimnis und Verschwiegenheit.....	14
§ 18. Technische und organisatorische Maßnahmen.....	14
§ 19. Verarbeitung von personenbezogenen Daten im Auftrag.....	15

§ 20. Verzeichnis von Verarbeitungstätigkeiten .....	16
§ 21. Meldung von Verletzungen des Schutzes personenbezogener Daten .....	17
§ 22. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person .....	17
§ 23. Datenschutz-Folgenabschätzung .....	18
VIERTER ABSCHNITT: AUFSICHTSGREMIEN UND BEAUFTRAGTE FÜR DEN DATENSCHUTZ .....	19
§ 24. Bestellung und Stellung des Bundesbeauftragten für Datenschutz .....	19
§ 25. Aufgaben und Befugnisse des Bundesbeauftragten für den Datenschutz .....	20
§ 26. Betriebsbeauftragte für den Datenschutz .....	20
§ 27. Aufsichtsgremium .....	21
§ 28. Geldbußen .....	22
§ 29. Recht auf Beschwerde .....	23
§ 30. Schlichtungsstelle für Datenschutz .....	23
§ 31. Schadensersatz durch Verantwortliche .....	23
FÜNFTER ABSCHNITT: VORSCHRIFTEN FÜR BESONDERE VERARBEITUNGSSITUATIONEN .....	24
§ 32. Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen .....	24
§ 33. Verarbeitung personenbezogener Daten für forschende und statistische Zwecke .....	25
§ 34. Verarbeitung personenbezogener Daten für journalistische Zwecke .....	25
§ 35. Veranstaltungen von Gemeinden des Bundes .....	26
§ 36. Videoüberwachung öffentlich zugänglicher Räume .....	26
SECHSTER ABSCHNITT: DATENSCHUTZ IN RECHTLICH SELBSTSTÄNDIGEN EINRICHTUNGEN UND GEMEINDEN .....	27
§ 37. Geltung der Datenschutzordnung für selbstständige Einrichtungen .....	27
§ 38. Geltung der Datenschutzordnung für selbstständige Gemeinden .....	27
SIEBENTER ABSCHNITT: SCHLUSSBESTIMMUNGEN .....	27
§ 39. Ergänzende Bestimmungen .....	27
§ 40. Übergangsregelungen .....	28
§ 41. Gleichstellung .....	28
§ 42. Inkrafttreten, Außerkrafttreten .....	28

# Datenschutzordnung (DSO)

*des Bundes Freier evangelischer Gemeinden in Deutschland KdÖR*

## Präambel

Diese Ordnung wird erlassen in Ausübung des gemäß Artikel 140 Grundgesetz garantierten Rechts des Bundes Freier evangelischer Gemeinden (im Folgenden auch: Bund genannt), seine Angelegenheiten selbstständig innerhalb der Schranken der für alle geltenden Gesetze zu ordnen und zu verwalten.

Dieses Recht ist europarechtlich geachtet und festgeschrieben in Artikel 91 der Verordnung EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). In Wahrnehmung dieses Rechts regelt diese Ordnung die Datenverarbeitung im Bund.

## ERSTER ABSCHNITT: ALLGEMEINE BESTIMMUNGEN

### § 1. Gegenstand, Ziele und Anwendungsbereich

- (1) Diese Datenschutzordnung gilt für die im Bund Freier evangelischer Gemeinden zusammengeschlossenen Ortsgemeinden und den Bundesbereichen sowie für die Arbeitszweige und Einrichtungen des Bundes und deren Verwaltung (im Folgenden: Bund).
- (2) Diese Ordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Sie dient dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Diese Ordnung gilt für die ganz- oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Akten und Aktensammlungen gelten nur als Dateisystem, wenn sie nach bestimmten Kriterien geordnet sind.
- (4) Für rechtlich selbstständige Einrichtungen des Bundes (Bundeswerke) gilt diese Datenschutzordnung nach Maßgabe des dritten Abschnittes.
- (5) Diese Ordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht zum Bund gehörigen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung den Zwecken des Bundes dient.
- (6) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

## § 2. Verantwortlichkeit für die Durchführung des Datenschutzes

- (1) Die Geschäftsführende Bundesleitung des Bundes stellt die Einhaltung des Datenschutzes im Sinne dieser Ordnung innerhalb der Stellen des Bundes sicher, die nicht Bundeswerke oder Mitgliedsgemeinden sind.
- (2) Die Bundeswerke stellen in eigener Zuständigkeit den Datenschutz im Sinne dieser Verordnung sicher.
- (3) Die Ortsgemeinden bestellen für die Einhaltung des Datenschutzes einen Beauftragten für Datenschutz. Dieser stellt die Einhaltung des Datenschutzes im Sinne dieser Ordnung innerhalb der Ortsgemeinde, deren Arbeitszweige und Einrichtungen sicher.

## § 3. Begriffsbestimmungen

Im Sinne dieser Verordnung 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 Daten“ sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetisch oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
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. „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;
5. „Drittland“ ein Land, das nicht Mitglied der Europäischen Union ist;
6. „Stelle des Bundes“ eine Gemeinde, die Mitglied im Bund Freier evangelischer Gemeinden ist, ein Arbeitszweig, eine Einrichtung, ein Bundesbereich, ein Bundesgremium oder ein Organ dieses Bundes ist;
7. „Verantwortlicher“ eine Stelle des Bundes, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
8. „Auftragsverarbeiter“ eine natürliche oder juristische Person oder - falls der Verantwortliche zu einer anderen juristischen Person gehört - eine Stelle des Bundes, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet;

9. „Dritter“ eine natürliche oder juristische Person, Behörde, selbstständige Gemeinde oder Einrichtung außer der betroffenen Person, der verantwortlichen Stelle, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung der verantwortlichen Stelle oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten; öffentliche Stellen nach der Begriffsbestimmung des BDSG § 2.
10. „Anonymisierung“ ist die Verarbeitung personenbezogener Daten derart, dass die personenbezogenen Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden können oder nur mit einem großen Aufwand an Zeit, Kosten und Arbeitskraft einer identifizierten oder identifizierbaren Person zugeordnet werden können;
11. „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 können;
12. „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;
13. „Aufsichtsgremium“ bzw. „Datenschutzrat“ eine unabhängige Stelle des Bundes, die über die Einhaltung der Datenschutzordnung wacht;
14. „Bundesbeauftragter für Datenschutz“ der von der Geschäftsführenden Bundesleitung des Bundes bestellte Beauftragte für den Datenschutz (im Folgenden auch kurz: Datenschutzbeauftragter);
15. „Betriebsbeauftragter für Datenschutz“ der von einer Stelle des Bundes berufene Datenschutzbeauftragte innerhalb des Verantwortungsbereiches des Verantwortlichen;
16. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
17. „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;
18. „Datenschutzrat“ das Aufsichtsgremium des Bundes für den Datenschutz;
19. „Schlichtungsstelle“ die Anrufungsstelle bei Unstimmigkeiten zum Datenschutz zwischen Datenschutzrat und Stelle des Bundes.

#### § 4. Seelsorgegeheimnis und Amtsverschwiegenheit

Pastoren und Gemeindeferenten unterliegen dieser Ordnung. Abweichend von Satz 1 dürfen sie zum Zweck ihres Seelsorgeauftrags eigene Aufzeichnungen führen, die auch besondere Daten enthalten. Das gilt auch für Personen, denen ein besonderer Seelsorgeauftrag erteilt worden ist. Diese Aufzeichnungen dürfen Dritten nicht zugänglich gemacht werden. Dazu sind geeignete technische oder organisatorische Maßnahmen zu treffen.

## § 5. Rechtmäßigkeit der Verarbeitung

(1) Grundsätzlich gilt: Personenbezogene Daten müssen

- a) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Prinzip der Zweckbindung“),
- b) auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Prinzip der Datenminimierung“) und
- c) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, oder für im Interesse des Bundes liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke erforderlich ist („Prinzip der Speicherzeitbegrenzung“).

(2) Die Verarbeitung ist nur zulässig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- a) Eine Rechtsvorschrift des Bundes oder eine vorrangige staatliche Rechtsvorschrift die Verarbeitung der personenbezogenen Daten erlaubt oder sie anordnet;
- b) die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- c) die Verarbeitung ist zur Erfüllung der Aufgaben des Verantwortlichen erforderlich, einschließlich der Ausübung kirchlicher Aufsicht;
- d) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche bzw. die Stelle des Bundes unterliegt;
- e) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- f) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im Interesse des Bundes liegt;
- g) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht;
- h) die Verarbeitung ist zur Durchführung von historischer oder wissenschaftlicher Forschung im Interesse des Bundes erforderlich, das historische oder wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens überwiegt das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich und der Zweck der Forschung kann auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden;
- j) sie dient Archivzwecken im Interesse einer Stelle des Bundes.

(3) Der Zweck der Datenverarbeitung und der Kreis der betroffenen Personen müssen festgelegt oder erkennbar sein.

(4) Die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden (Zweckänderung), ist nur zulässig, wenn die Möglichkeit der Pseudonymisierung geprüft wurde und mindestens einer der nachstehenden Bedingungen erfüllt ist:

- a) Eine Rechtsvorschrift sieht dies vor und Interessen des Bundes stehen nicht entgegen;

- b) die betroffene Person hat eingewilligt;
- c) es ist offensichtlich, dass die Verarbeitung im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass diese in Kenntnis des anderen Zweckes ihre Einwilligung verweigern würde;
- d) Angaben der betroffenen Person überprüft werden müssen, weil Anhaltspunkte für deren Unrichtigkeit bestehen;
- e) die Daten können aus allgemein zugänglichen Quellen entnommen werden oder der Verantwortliche darf sie veröffentlichen, es sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung offensichtlich überwiegt;
- f) es besteht Grund zu der Annahme, dass andernfalls die Wahrnehmung des kirchlichen Auftrages gefährdet würde;
- g) es ist zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich;
- h) die Verarbeitung ist zur Durchführung wissenschaftlicher Forschung im Interesse des Bundes erforderlich, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens überwiegt das Interesse der betroffenen Person an dem Ausschluss der Zweckänderung erheblich und der Zweck der Forschung kann auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden;
- i) sie ist für statistische Zwecke zur Erfüllung des kirchlichen Auftrages erforderlich.

(5) Eine Verarbeitung für andere Zwecke ist zulässig, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen des Bundes, der Rechnungsprüfung, der Revision oder der Durchführung von Organisationsuntersuchungen für die Verantwortlichen dient. Das gilt auch für die Verarbeitung zu Ausbildungszwecken durch die Verantwortlichen, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

## § 6. Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Ordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung von Satz 1 und Satz 2 in Kenntnis gesetzt.

(4) Sollen Daten von Kindern verarbeitet werden, so kann, wenn das Kind das sechzehnte Lebensjahr noch nicht vollendet hat, eine wirksame Einwilligung nur durch den Träger der elterlichen Sorge für das Kind erfolgen. Andernfalls darf die Einwilligung eigenständig durch das Kind erfolgen. Das Kind soll die Eltern über eine solche Einwilligung in Kenntnis setzen. Diese Regelung gilt insbesondere für die Datenverarbeitung im Rahmen von elektronischen Angeboten von Stellen des Bundes.



## § 7. Datenübermittlung an Stellen des Bundes, sowie Dritte

- (1) Die Übermittlung von personenbezogenen Daten an Stellen des Bundes ist zulässig, wenn
  - a) sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden Stelle liegenden Aufgaben erforderlich ist und
  - b) die Zulässigkeitsvoraussetzungen des § 5 vorliegen.
- (2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt der Verantwortliche. Erfolgt die Übermittlung auf Ersuchen der empfangenden Stelle des Bundes, trägt auch diese Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der datenempfangenden Stelle des Bundes liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.
- (3) Die datenempfangende Stelle des Bundes darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 5 Abs. 4 zulässig.
- (4) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen oder einer anderen Person so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen der betroffenen oder einer anderen Person an deren Geheimhaltung offensichtlich überwiegen; eine Verwendung dieser Daten ist unzulässig.
- (5) Absatz 4 gilt entsprechend, wenn personenbezogene Daten innerhalb einer Stelle des Bundes weitergegeben werden.
- (6) Personenbezogene Daten dürfen an Dritte nichtöffentliche Stellen übermittelt werden, wenn diese zur Erfüllung der Aufgaben des Verantwortlichen erforderlich ist, sofern sichergestellt ist, dass bei der empfangenden Stelle ausreichende Datenschutzmaßnahmen getroffen werden, und nicht berechnete Interessen der betroffenen Person entgegenstehen.
- (7) Personenbezogene Daten dürfen an staatliche und öffentliche Stellen übermittelt werden, wenn dies eine Rechtsvorschrift zulässt oder dies zur Erfüllung der Aufgabe der Stelle des Bundes erforderlich ist und nicht berechnete Interessen der betroffenen Person entgegenstehen.

## § 8. Verarbeitung besonderer Daten

- (1) Die Verarbeitung besonderer Daten gemäß § 3 Nummer 2 ist untersagt.
- (2) Absatz 1 gilt nicht in folgenden Fällen:
  - a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach dem Recht des Bundes kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden;
  - b) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben;
  - c) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat;



- d) die Verarbeitung erfolgt durch den Verantwortlichen im Rahmen seiner rechtmäßigen und für die Aufgabenerfüllung notwendigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die besonderen Daten nicht ohne Einwilligung der betroffenen Personen an Dritte, die keine Stelle des Bundes sind, übermittelt werden;
  - e) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Schlichtungsstelle im Rahmen ihrer justiziellen Tätigkeit erforderlich;
  - f) die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses erforderlich und der Verantwortliche hat angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen;
  - g) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin oder für die Beurteilung der Arbeitsfähigkeit des Beschäftigten und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich;
  - h) die Verarbeitung ist für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke, die im Interesse des Bundes sind, erforderlich und der Verantwortliche hat angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen.
- (3) Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen ist unter den Voraussetzungen von § 6 zulässig, wenn dies das kirchliche Recht des Bundes oder staatliches Recht zulässt.

## ZWEITER ABSCHNITT: RECHTE DER BETROFFENEN PERSON

### § 9. Transparente Information, Kommunikation

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen, die nach dieser Ordnung hinsichtlich der Verarbeitung zu geben sind, in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln.

(2) Der Verantwortliche stellt der betroffenen Person Informationen über die ergriffenen Maßnahmen gemäß den §§ 11 bis 16 innerhalb von zwei Monaten nach Eingang eines entsprechenden Antrags zur Verfügung. Diese Frist kann um zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl der Anträge erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person nach Ablauf von 2 Monaten nach Eingang über eine Fristverlängerung zusammen mit den Gründen für die Verzögerung.

(3) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens nach Ablauf von 2 Monaten nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, beim Datenschutzrat Beschwerde einzulegen.

(4) Informationen werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder - insbesondere im Fall von häufiger Wiederholung - exzessiven Anträgen einer betroffenen Person kann der Verantwortliche sich weigern, aufgrund des Antrags tätig zu werden, oder ein angemessenes Entgelt verlangen.

(5) Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die einen Antrag gemäß den §§ 11 bis 16 stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

### § 10. Informationspflichten bei Datenerhebung

(1) Der Bundesbeauftragte für Datenschutz stellt folgende Informationen zur Datenerhebung öffentlich zur Verfügung:

1. Das Bestehen eines Rechts auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit sowie eines Widerspruchsrechts gegen die Verarbeitung;
2. das Bestehen des Rechts eine gegebenenfalls erteilte Einwilligung zu widerrufen;
3. das Bestehen eines Beschwerderechts beim Datenschutzrat.

(2) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person auf Verlangen Folgendes mit:

1. Den Namen und die Kontaktdaten der verantwortlichen Stelle;
2. die Kontaktdaten des zuständigen Betriebsbeauftragten für Datenschutz oder die Kontaktdaten des Datenschutzbeauftragten;
3. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen;
4. die Rechtsgrundlage für die Verarbeitung;
5. gegebenenfalls die Empfänger der personenbezogenen Daten und

6. wenn die Verarbeitung auf Artikel 5 Absatz 2 Buchstabe g beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden.

(3) Absatz 2 findet keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt oder die Informationspflicht einen unverhältnismäßigen Aufwand erfordern würde.

(4) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person über die in Absatz 2 aufgeführten Informationen hinaus die zu ihr gespeicherten Daten mit, auch soweit sie sich auf Herkunft oder empfangende Stellen beziehen. Absatz 3 gilt entsprechend. Der Verantwortliche ist weiterhin von dieser Verpflichtung befreit, wenn die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss oder wenn durch die Auskunft das Seelsorgegeheimnis oder die Amtsverschwiegenheit gemäß § 4 berührt wird.

(5) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt sie der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und gegebenenfalls die Empfänger der personenbezogenen Daten zur Verfügung. Diese Informationspflicht gilt nicht im Fall von § 5 Abs. 4.

## § 11. Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so ist der betroffenen Person auf Antrag Auskunft zu erteilen über die zu ihr gespeicherten personenbezogenen Daten. Die Auskunft muss folgende Informationen enthalten:

1. Die Verarbeitungszwecke;
2. die Kategorien personenbezogener Daten;
3. die Empfänger, gegenüber denen die personenbezogenen Daten offengelegt worden sind;
4. falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
5. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
6. das Bestehen eines Beschwerderechts beim Datenschutzrat;
7. Information über die Herkunft der Daten.

(2) Auskunft darf nicht erteilt werden, soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss, oder wenn durch die Auskunft das Seelsorgegeheimnis oder die Amtsverschwiegenheit gemäß § 4 berührt wird.

(3) Die Auskunft im Umfang einer Kopie ist unentgeltlich. Weitere Kopien müssen nicht erstellt werden. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

## § 12. Recht auf Berichtigung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

(2) Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

(3) Das Recht auf Berichtigung besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im Interesse des Bundes verarbeitet wurden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

## § 13. Recht auf Löschung

(1) Die betroffene Person hat das Recht, von der verantwortlichen Stelle zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern mindestens einer der folgenden Gründe zutrifft:

- a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig;
- b) die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;
- c) die betroffene Person legt gemäß § 16 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor;
- d) die personenbezogenen Daten wurden unrechtmäßig verarbeitet;
- e) die Löschung der personenbezogenen Daten ist zur Erfüllung einer Verpflichtung nach dem Kirchenrecht des Bundes erforderlich, dem der Verantwortliche unterliegt.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, um die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten anzustreben.

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist

1. zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
2. zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach staatlichem oder kirchlichen Recht des Bundes, dem der Verantwortliche unterliegt, erfordert,
3. zur Wahrnehmung einer Aufgabe aufgrund eines wichtigen Interesses des Bundes,
4. für im Interesse des Bundes liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(4) Ist eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, tritt an die Stelle des Rechts auf Löschung das Recht auf Einschränkung der Verarbeitung gemäß § 14.

## § 14. Recht auf Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- a) Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten und die Prüfung der Richtigkeit durch den Verantwortlichen ist noch nicht abgeschlossen. Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen;
- b) die betroffene Person hat Widerspruch gegen die Verarbeitung gemäß § 16 eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(2) Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten - von ihrer Speicherung abgesehen - nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aufgrund eines wichtigen Interesses des Bundes verarbeitet werden.

(3) Eine betroffene Person, die eine Einschränkung der Verarbeitung gemäß Absatz 1 erwirkt hat, wird von der verantwortlichen Stelle unterrichtet, bevor die Einschränkung aufgehoben wird.

## § 15. Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

(1) Der Verantwortliche teilt der betroffenen Person jede Berichtigung oder Löschung ihrer personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach § 12, § 13 oder § 14 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

(2) Der Verantwortliche unterrichtet die betroffene Person über alle Empfänger, denen personenbezogenen Daten offengelegt wurden, wenn die betroffene Person dies verlangt.

## § 16. Widerspruchsrecht

(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten gemäß § 5 Absatz 2 Buchstaben f) und g) Widerspruch einzulegen.

(2) Der Widerspruch verpflichtet den Verantwortlichen dazu, die Verarbeitung zu unterlassen, soweit nicht an der Verarbeitung ein zwingendes Interesse des Bundes besteht, das Interesse einer dritten Person überwiegt oder Recht des Bundes zur Verarbeitung verpflichtet.

(3) Die betroffene Person muss bei Datenverarbeitung gemäß § 5 Absatz 2 Buchstaben f) und g) spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das in Absatz 1 genannte Recht hingewiesen werden; dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

(4) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß § 5

Absatz 4 Buchstabe h oder i erfolgt, Widerspruch einzulegen, es sei denn, die Interessen des Bundes an der Verarbeitung überwiegen erheblich die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung.

## DRITTER ABSCHNITT: PFLICHTEN DER VERANTWORTLICHEN UND AUFTRAGSVERARBEITER

### § 17. Datengeheimnis und Verschwiegenheit

Den mit dem Umgang von personenbezogenen Daten betrauten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das gilt insbesondere für das Offenlegen solcher Daten. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer Ordnungen des Bundes zur Verschwiegenheit in diesem Sinne verpflichtet wurden. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

### § 18. Technische und organisatorische Maßnahmen

(1) Der Verantwortliche und gegebenenfalls der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen und zu dokumentieren, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

(2) Diese Maßnahmen erfordern die Betrachtung folgender Aspekte:

1. Die Pseudonymisierung, die Anonymisierung und die Verschlüsselung personenbezogener Daten;
2. die Fähigkeit, die Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit) der datenverarbeitenden Systeme und Dienste auf Dauer sicherzustellen;
3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
4. ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(3) Bei der Beurteilung des angemessenen Sicherheitsniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung personenbezogener Daten verbunden sind, insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang.

(4) Der Verantwortliche und gegebenenfalls der Auftragsverarbeiter treffen technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere geeignet sein, dass personenbezogene Daten nicht ohne

Eingreifen der verantwortlichen Stelle durch Voreinstellungen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(5) Bei der Auswahl der Maßnahmen darf berücksichtigt werden, dass ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Sicherheitsniveau steht.

(6) Die Einhaltung eines nach dem EU-Recht anerkannten Verfahrens zur Feststellung der Sicherheit der personenbezogenen Daten kann als Indiz für die Erfüllung der Pflichten gemäß den Absätzen 1 bis 4 gewertet werden.

(7) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur gemäß den Weisungen des Verantwortlichen verarbeiten.

## § 19. Verarbeitung von personenbezogenen Daten im Auftrag

(1) Erfolgt eine Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen, so ist der Verantwortliche für die Einhaltung der Vorschriften dieser Ordnung und anderer anzuwendender Vorschriften über den Datenschutz verantwortlich. Die im ZWEITEN ABSCHNITT genannten Rechte sind ihm gegenüber geltend zu machen. Zuständig für die Aufsicht ist der Datenschutzrat.

(2) Hat eine natürliche oder juristische Person Ihren Sitz oder eine Betriebsstätte, die für die Verarbeitung im Auftrag benötigt werden, in einem Drittland, so ist die Erteilung eines Auftrags zur Verarbeitung von personenbezogenen Daten durch den Verantwortlichen nur zulässig, wenn die EU-Kommission für dieses Land beschlossen hat, dass es ein angemessenes Datenschutzniveau bietet.

(3) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Schutz der Rechte der betroffenen Person gewährleistet und

- a) konform zu den Anforderungen dieser Ordnung erfolgt, wenn der Auftragsverarbeiter eine Stelle des Bundes ist oder anderenfalls
- b) konform zu den Anforderungen dieser Ordnung oder der Verordnung EU 2016/679 erfolgt.

(4) Bei der Beauftragung eines Auftragsverarbeiters, der keine Stelle des Bundes, kein Bundeswerk und - im Falle einer natürlichen Person - kein Mitglied einer Gemeinde des Bundes ist, ist die Entscheidung für diesen Auftragsverarbeiter schriftlich zu begründen und verfügbar zu halten.

(5) Der Auftragsverarbeiter wird dazu verpflichtet, keine weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch zu nehmen. Bedingung für eine Genehmigung durch den Verantwortlichen ist insbesondere die Verpflichtung des Auftragsverarbeiters zu gewährleisten, dass der weitere Auftragsverarbeiter gleichwertige Bedingungen gemäß § 18 und § 19 akzeptiert.

(6) Der Auftrag ist schriftlich zu erteilen. Dieser Auftrag beinhaltet insbesondere, dass der Auftragsverarbeiter

- c) die personenbezogenen Daten nur auf Weisung des Verantwortlichen verarbeitet,
- d) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen auf das Datengeheimnis gemäß § 17 verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- e) alle gemäß § 18 für Auftragsverarbeiter erforderlichen Maßnahmen ergreift,



- f) die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters gemäß Absatz 5 einhalten,
- g) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in ZWEITEN ABSCHNITT genannten Rechte der betroffenen Person nachzukommen,
- h) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl der verantwortlichen Stelle entweder löscht oder zurückgibt,
- i) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt und
- j) den Verantwortlichen unverzüglich informiert, falls er der Auffassung ist, dass eine Weisung der verantwortlichen Stelle gegen diese Ordnung oder gegen andere anzuwendende Datenschutzbestimmungen verstößt
- k) der Verpflichtung gemäß § 21 Absatz 2 nachzukommen hat.

(7) Der Verantwortliche hat sich vor Beginn der Datenverarbeitung und in geplanten Abständen von der Einhaltung der Vertragsbedingungen gemäß Absatz 6 zu überzeugen. Das Ergebnis ist zu dokumentieren. Es sind auch Fachwissen und Ressourcen zu beurteilen. Die Einhaltung eines nach dem EU-Recht anerkannten Verfahrens zur Feststellung der Sicherheit der personenbezogenen Daten durch den Auftragsverarbeiter ist als Begründung für erleichterte Kontrollen vor Auftragserteilung oder während des Vertragsverhältnisses zulässig.

(8) Handelt es sich um einen Druckauftrag, so muss der Verantwortliche nicht gemäß Absatz 7 handeln.

(9) Rechtsvorschriften des Bundes können bestimmen, dass vor der Auftragserteilung die Genehmigung einer Stelle des Bundes einzuholen ist oder Mustervereinbarungen zu verwenden sind.

## § 20. Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, führen. Dieses Verzeichnis enthält folgende Angaben:

1. Den Namen und die Kontaktdaten der verantwortlichen Stelle sowie gegebenenfalls des Auftragsverarbeiters und des dezentral Beauftragten;
2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten sowie
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder offengelegt werden sollen, einschließlich Empfängern in Drittländern.

(2) Auftragsverarbeiter, die nicht dieser Ordnung unterliegen, sind zur Einhaltung der EU-Verordnung 2016/679 verpflichtet. Ist der Auftragsverarbeiter Stelle des Bundes oder ein Mitglied einer Gemeinde des Bundes, führt er ein Verzeichnis von allen im Auftrag einer verantwortlichen Stelle durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:

1. die Angaben gemäß Absatz 1 sowie
  2. eine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 18.
- (3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen. Ein gängiges elektronisches Format ist zulässig.
- (4) Verantwortlicher und Auftragsverarbeiter stellen dem Datenschutzrat die Verzeichnisse auf Anfrage zur Verfügung.
- (5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Verantwortliche, die weniger als 50 Mitarbeiter beschäftigen oder Auftragsverarbeiter, die weniger als 250 Mitarbeiter beschäftigen. In diesen Fällen sind Verzeichnisse gemäß den Absätzen 1 und 2 nur hinsichtlich der Verfahren, die die Verarbeitung besonderer Daten einschließen, zu erstellen.
- (6) Rechtsvorschriften des Bundes können vorsehen, dass für bestimmte Verfahren ein zentral geführtes Verzeichnis gepflegt wird.

## **§ 21. Meldung von Verletzungen des Schutzes personenbezogener Daten**

- (1) Im Falle einer Verletzung des Schutzes personenbezogener Daten, die voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt, meldet der Verantwortliche dies unverzüglich und möglichst binnen 72 Stunden dem Datenschutzrat.
- (2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.
- (3) Die Meldung gemäß Absatz 1 enthält insbesondere eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten und der mutmaßlichen Folgen der Verletzung des Schutzes.
- (4) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten samt den ergriffenen Abhilfemaßnahmen zu dokumentieren.

## **§ 22. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person**

- (1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung.
- (2) Die Benachrichtigung der betroffenen Person hat in klarer und einfacher Sprache zu erfolgen und enthält zumindest die in § 21 Absätze 3 und 4 genannten Informationen und Maßnahmen.
- (3) Von der Benachrichtigung der betroffenen Person kann abgesehen werden, wenn eine der folgenden Bedingungen erfüllt ist:
  - a) Der Verantwortliche hat durch nachträgliche Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
  - b) der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden 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;

- c) die Benachrichtigung ist mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine Bekanntmachung in einem Publikationsinstrument des Bundes oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

## § 23. Datenschutz-Folgenabschätzung

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

1. umfangreiche Verarbeitung besonderer personenbezogener Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten und
2. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(3) Die Folgenabschätzung umfasst insbesondere:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der verantwortlichen Stelle verfolgten berechtigten Interessen;
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4. 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 die datenschutzrechtlichen Regelungen eingehalten werden.

(4) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des dezentral Beauftragten ein, sofern ein solcher benannt wurde.

## VIERTER ABSCHNITT: AUFSICHTSGREMIEN UND BEAUFTRAGTE FÜR DEN DATENSCHUTZ

### § 24. Bestellung und Stellung des Bundesbeauftragten für Datenschutz

- (1) Die Geschäftsführende Bundesleitung des Bundes bestellt einen Bundesbeauftragten für Datenschutz per Beschluss.
- (2) Die Bestellung wird in der Regel auf fünf Jahre befristet. Die erneute Bestellung ist zulässig.
- (3) Der Bundesbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens bestellt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in § 25 genannten Aufgaben.
- (4) Der Bundesbeauftragte kann Beschäftigter des Bundes sein oder seine Aufgaben auf der Grundlage eines Dienstvertrags oder Dienstleistungsvertrags erfüllen.
- (5) Die Arbeitszweige und Einrichtungen des Bundes stellen sicher, dass der Bundesbeauftragte frühzeitig über Projekte für Verfahren, bei denen es zur Verarbeitung von personenbezogener Daten kommen wird, informiert wird, falls diese keinen Betriebsbeauftragten für den Datenschutz bestellt haben.
- (6) Die Geschäftsführende Bundesleitung des Bundes unterstützt den Bundesbeauftragten, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.
- (7) Die Geschäftsführende Bundesleitung des Bundes stellt sicher, dass der Bundesbeauftragte bei der Erfüllung seiner bzw. ihrer Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Bundesbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.
- (8) Der Bundesbeauftragte für Datenschutz berichtet dem Datenschutzrat.
- (9) Der Bundesbeauftragte für Datenschutz ist jederzeit zur Anrufung der Geschäftsführenden Bundesleitung des Bundes berechtigt.
- (10) Betroffene Personen können den Bundesbeauftragten für Datenschutz zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zurate ziehen. Vorrangig ist die Anrufung des Betriebsbeauftragten für Datenschutz gemäß § 26.
- (11) Der Bundesbeauftragte für Datenschutz ist bei der Erfüllung seiner Aufgaben an die Wahrung des Datengeheimnisses und der Vertraulichkeit gebunden.
- (12) Der Bundesbeauftragte für Datenschutz kann andere Aufgaben und Pflichten wahrnehmen. Die Geschäftsführende Bundesleitung des Bundes stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
- (13) Die Vertretung ist zu regeln.
- (14) Die Abberufung des Bundesbeauftragten ist nur mit Zustimmung des Bundestages zulässig. Eine vorläufige Suspendierung durch die Geschäftsführende Bundesleitung des Bundes ist nur aus wichtigem Grund möglich. In diesem Fall nimmt der Vertreter die Rechte und Pflichten des Bundesbeauftragten wahr. Die Suspendierung ist schriftlich zu begründen und längstens bis zum nächsten Bundestag wirksam.

(15) Sitz des Bundesbeauftragten ist in der Regel das Bundeshaus.

## § 25. Aufgaben und Befugnisse des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für Datenschutz sensibilisiert, informiert und berät die verantwortlichen Stellen und internen Auftragsverarbeiter über Fragen und maßgebliche Entwicklungen des Datenschutzes sowie über die Vermeidung von Risiken.

(2) Er unterrichtet betroffene Personen auf Anfrage über deren persönliche Rechte aus dieser Ordnung.

(3) Er nimmt Beschwerden von betroffenen Personen und von bei Stellen des Bundes Beschäftigten entgegen und übergibt sie dem Datenschutzrat zur Bearbeitung.

(4) Prüfungen werden durch den Bundesbeauftragten für Datenschutz oder ein Mitglied des Datenschutzrats unter folgenden Bedingungen durchgeführt:

- a) Der Prüfer wird vom betroffenen Verantwortlichen bei der Erfüllung seiner bzw. ihrer Aufgaben unterstützt. Auf Verlangen ist ihm bzw. ihr Auskunft sowie Einsicht in alle Unterlagen und Akten über die Verarbeitung personenbezogener Daten zu geben, und es sind alle diesbezüglich gespeicherten Daten bereitzustellen;
- b) der Prüfer teilt die Ergebnisse seiner Prüfungen dem betroffenen Verantwortlichen und dem Datenschutzrat mit. Damit können Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung personenbezogener Daten und eine Aufforderung zur Stellungnahme verbunden sein;
- c) Aufzeichnungen gemäß § 4 sowie personenbezogene Daten, die dem Arztgeheimnis unterliegen, sind von solchen Prüfungen ausgenommen;
- d) Die Schlichtungsstelle unterliegt der Prüfung durch den Datenschutzrat nur, soweit es in eigenen Angelegenheiten als Verwaltung tätig wird.

(5) Der Bundesbeauftragte kann Musterverträge und Standards zur Verarbeitung personenbezogener Daten erstellen, deren Einsatz und Umsetzung überprüfen und die Ergebnisse veröffentlichen.

(6) Der Bundesbeauftragte ist beratendes Mitglied im Ständigen Ausschuss des Bundestages und im Bundestag des Bundes.

## § 26. Betriebsbeauftragte für den Datenschutz

(1) Die Bundesbereiche und Einrichtungen des Bundes, bestellen einen Betriebsbeauftragten für Datenschutz, wenn bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten betraut sind. Anderenfalls ist eine freiwillige Bestellung jederzeit möglich.

(2) Eine befristete Bestellung soll für mindestens drei Jahre erfolgen. Die erneute Bestellung ist zulässig.

(3) Die Bestellung kann sich auf mehrere Verantwortliche erstrecken.

(4) Zu Betriebsbeauftragten für Datenschutz dürfen nur Personen bestellt werden, die das zur Erfüllung ihrer Aufgaben erforderliche Fachwissen und die notwendige Zuverlässigkeit besitzen.

(5) Zu Betriebsbeauftragten für Datenschutz sollen diejenigen nicht bestellt werden, die mit der Leitung der Datenverarbeitung beauftragt sind oder denen die Leitung einer Stelle des Bundes obliegt.

- (6) Die Bestellung von Betriebsbeauftragten für Datenschutz erfolgt schriftlich und ist dem Datenschutzrat anzuzeigen.
- (7) Der Verantwortliche stellt sicher, dass der oder die Betriebsbeauftragte für Datenschutz frühzeitig über Projekte für Verfahren, bei denen es zur Verarbeitung von personenbezogener Daten kommen wird, informiert wird.
- (8) Betroffene Personen und Beschäftigte können sich unmittelbar an die örtlichen Betriebsbeauftragten für Datenschutz wenden.
- (9) Die Betriebsbeauftragten für Datenschutz sind der Leitung der jeweiligen Stelle des Bundes unmittelbar zu unterstellen. Der oder die Betriebsbeauftragte für Datenschutz berichtet an die Leitung.
- (10) Der oder die Betriebsbeauftragte für Datenschutz sind im Rahmen ihrer Aufgaben weisungsfrei. Sie dürfen wegen dieser Tätigkeit nicht benachteiligt werden. Sie können Auskünfte verlangen, Einsicht in Unterlagen nehmen und erhalten Zugang zu personenbezogenen Daten und den Verarbeitungsvorgängen. Die Stelle des Bundes unterstützt die Betriebsbeauftragten für Datenschutz bei der Erfüllung ihrer Aufgaben.
- (11) Zur Erlangung und zur Erhaltung des erforderlichen Fachwissens hat der Verantwortliche den Betriebsbeauftragten für Datenschutz die Teilnahme an Fortbildungsveranstaltungen zu ermöglichen und die Kosten zu tragen.
- (12) Ist der oder die Betriebsbeauftragte für Datenschutz Beschäftigter bzw. Beschäftigte einer Stelle des Bundes, so ist die Abberufung nur aus wichtigem Grund zulässig.
- (13) Der Betriebsbeauftragte für Datenschutz verwaltet die Personenverpflichtungen seiner Stelle des Bundes.

## § 27. Aufsichtsgremium

- (1) Über die Einhaltung dieser Ordnung wacht ein unabhängiges Aufsichtsgremium für den Datenschutz (Datenschutzrat).
- (2) Der Datenschutzrat wird vom Bundesbeauftragten für den Datenschutz geleitet und nach außen vertreten.
- (3) Der Bundesbeauftragte für den Datenschutz wählt die Mitglieder des Datenschutzrats unter Berücksichtigung von Fachwissen, Zuverlässigkeit und Erfahrung aus. Der Datenschutzrat besteht aus mindestens zwei Mitgliedern. Die Bestellung der Mitglieder erfolgt für mindestens zwei Jahre. Die Mitwirkung im Datenschutzrat erfolgt in der Regel ehrenamtlich.
- (4) Die Bestellung eines Mitglieds des Datenschutzrats ist erst wirksam, wenn die Geschäftsführende Bundesleitung des Bundes die Bestellung bestätigt hat.
- (5) Ein Mitglied des Datenschutzrats wird vom Bundesbeauftragten für Datenschutz zu seinem Vertreter bestellt. Er ist gleichzeitig Vertreter der Leitung des Datenschutzrats.
- (6) Der Datenschutzrat handelt bei der Erfüllung seiner Aufgaben und bei der Ausübung seiner Befugnisse völlig unabhängig. Er unterliegt weder direkter noch indirekter Beeinflussung von außen und nimmt keine Weisungen entgegen.
- (7) Der Datenschutzrat erstellt in der Regel einmal pro Jahr einen Tätigkeitsbericht. Der Tätigkeitsbericht wird der Geschäftsführenden Bundesleitung des Bundes übermittelt, dem Bundestag zur Kenntnis gegeben und im Berichtsheft zum Bundestag veröffentlicht. Er kann eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen enthalten.

(8) Der Datenschutzrat kann Verwaltungsaufgaben auf die Geschäftsführende Bundesleitung des Bundes übertragen.

(9) Dem Datenschutzrat werden seitens des Bundes die Finanzmittel zur Verfügung gestellt, um seine Aufgaben effektiv wahrnehmen zu können.

(10) Werden dem Datenschutzrat Verstöße gegen die Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bekannt, so beanstandet er dies gegenüber der verantwortlichen Stelle oder gegenüber dem Auftragsverarbeiter und fordert zur Stellungnahme innerhalb einer gesetzten Frist auf. Von einer Beanstandung kann abgesehen werden, wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Mit der Aufforderung zur Stellungnahme können Vorschläge zur Beseitigung der Mängel oder zur sonstigen Verbesserung des Datenschutzes verbunden werden. Die Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung des Datenschutzrats getroffen worden sind.

(11) Der Datenschutzrat ist befugt, bei Bedarf anzuordnen:

1. Verarbeitungsvorgänge auf bestimmte Weise in Einklang mit dieser Ordnung zu bringen;
2. Verarbeitungsvorgänge vorübergehend oder dauerhaft zu beschränken oder zu unterlassen;
3. personenbezogene Daten zu berichtigen, zu sperren oder zu löschen;
4. die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen.

(12) Der Datenschutzrat gibt sich eine Geschäftsordnung.

(13) Die Mitglieder des Datenschutzrates sind bei der Erfüllung ihrer Aufgaben an die Wahrung des Datengeheimnisses und der Vertraulichkeit gebunden. Dies gilt nicht für Mitteilungen zwischen den Mitgliedern. Ehemalige Mitglieder dürfen sich zu Angelegenheiten, die während ihrer Mitgliedschaft der Verschwiegenheit unterlagen, ohne Genehmigung des Datenschutzrates nicht äußern.

## § 28. Geldbußen

(1) Verstößt ein Verantwortlicher oder Auftragsverarbeiter, der Stelle des Bundes ist, vorsätzlich oder fahrlässig gegen Bestimmungen dieser Ordnung, so kann der Datenschutzrat Geldbußen verhängen oder für den Wiederholungsfall androhen.

(2) Der Datenschutzrat stellt sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig, abschreckend und geboten ist.

(3) Geldbußen werden je nach den Umständen des Einzelfalls verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Höhe ist insbesondere Folgendes zu berücksichtigen:

1. Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
2. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
3. jegliche von der verantwortlichen Stelle oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
4. etwaige einschlägige frühere Verstöße der verantwortlichen Stelle oder des Auftragsverarbeiters;



5. die Bereitschaft zur Zusammenarbeit mit dem Aufsichtsgremium, um dem Verstoß abzuhelpfen und seine möglichen nachteiligen Auswirkungen zu mindern;
6. die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
7. die Art und Weise, wie der Verstoß dem Aufsichtsgremium bekannt wurde.
8. jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall.

(4) Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen von bis zu 100.000 Euro verhängt. Nimmt die Stelle nicht als Unternehmen am Wettbewerb teil, so gelten als Höchstgrenze 50.000 Euro.

(5) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Maßnahmen nach § 27 Absatz 11 verhängt.

(6) Die gegebenenfalls vereinnahmten Gelder werden auf Beschluss des Datenschutzrats Stellen des Bundes zur Verwendung in Mission oder Diakonie zur Verfügung gestellt.

## § 29. Recht auf Beschwerde

(1) Jede Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an den Datenschutzrat wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein.

(2) Der Datenschutzrat unterrichtet die betroffene Person über den Stand und das Ergebnis der Beschwerde.

(3) Niemand darf wegen der Mitteilung von Tatsachen, die geeignet sind, den Verdacht aufkommen zu lassen, diese Ordnung oder eine andere anzuwendende Rechtsvorschrift über den Datenschutz sei verletzt worden, gemäßregelt oder benachteiligt werden. Beschäftigte müssen für Mitteilungen an den Datenschutzrat nicht den Dienstweg einhalten.

(4) Gegen Entscheidungen des Datenschutzrats kann bei der Schlichtungsstelle für Datenschutz des Bundes Einspruch erhoben werden.

## § 30 Schlichtungsstelle für Datenschutz

(1) Die Schlichtungsstelle tritt zusammen, wenn gegen die Entscheidung des Datenschutzrats Einspruch erhoben wurde.

(2) Die Schlichtungsstelle setzt sich zusammen aus dem Datenschutzrat oder einer Abordnung dieser, der Geschäftsführenden Bundesleitung oder einer Abordnung dieser und einer Person der Stelle des Bundes, die von den Maßnahmen des Datenschutzrates betroffen sind.

(3) Die Schlichtungsstelle hat den Auftrag im Einvernehmen der Parteien die Angelegenheit zu regeln. Entsteht keine Einigung, gelten die Entscheidungen des Datenschutzrates.

## § 31. Schadensersatz durch Verantwortliche

(1) Jede Person, der wegen einer Verletzung der Regelungen dieser Ordnung ein Schaden entstanden ist, hat einen Anspruch auf Schadensersatz gegen den Verantwortlichen. Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

- (2) Ein Verantwortlicher wird von der Haftung gemäß Absatz 1 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
- (3) Auf das Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuches und auf die Verjährung sind die Verjährungsfristen für unerlaubte Handlungen des Bürgerlichen Gesetzbuches entsprechend anzuwenden.
- (4) Mehrere Ersatzpflichtige haften als Gesamtschuldner im Sinne des Bürgerlichen Gesetzbuches.
- (5) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.
- (6) Beansprucht ein Betroffener Schadensersatz, so soll zunächst der Datenschutzrat des Bundes eine Anhörung vornehmen.

## FÜNFTER ABSCHNITT: VORSCHRIFTEN FÜR BESONDERE VERARBEITUNGSSITUATIONEN

### § 32. Verarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen

- (1) Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch für Zwecke der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Vertrag oder eine Dienstvereinbarung dies vorsieht.
- (2) Im Zusammenhang mit dem Verdacht auf Straftaten und Amtspflichtverletzungen, die durch Beschäftigte begangen wurden, insbesondere zum Schutz möglicher Betroffener, dürfen unter Beachtung des Verhältnismäßigkeitsgrundsatzes personenbezogene Daten von Beschäftigten verarbeitet werden, solange der Verdacht nicht ausgeräumt ist und die Interessen von möglichen Betroffenen dies erfordern.
- (3) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder der Verantwortliche und die beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Verantwortliche hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären.
- (4) Eine Offenlegung der Daten von Beschäftigten an Strafverfolgungsbehörden ist zulässig, wenn sie zur Aufdeckung einer Straftat oder Amtspflichtverletzung oder zum Schutz möglicher Betroffener erforderlich erscheint.
- (5) Die Offenlegung an künftige Dienst- oder Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig.
- (6) Verlangt der Verantwortliche zur Begründung oder im Rahmen eines Beschäftigungsverhältnisses notwendige Bescheinigungen oder medizinische oder psychologische Untersuchungen und Tests zur

Feststellung der Eignung des Bewerbers, dann darf der Verantwortliche lediglich die Offenlegung des Ergebnisses der Begutachtung verlangen.

(7) Personenbezogene Daten, die vor Begründung eines Beschäftigungsverhältnisses erhoben wurden, sind spätestens ein Jahr, nachdem feststeht, dass ein solches nicht zustande kommt, zu löschen. Dies gilt nicht, soweit überwiegende berechnigte Interessen der verantwortlichen Stelle der Löschung entgegenstehen oder die betroffene Person in die weitere Speicherung einwilligt.

(8) Für die Verarbeitung von Sozialdaten gemäß Sozialgesetzbuch gelten die Bestimmungen dieses Gesetzbuchs.

(9) Nach Beendigung eines Beschäftigungsverhältnisses sind personenbezogene Daten zu löschen, falls diese Daten nicht mehr benötigt werden.

### § 33. Verarbeitung personenbezogener Daten für forschende und statistische Zwecke

(1) Für Zwecke der historischen oder wissenschaftlichen Forschung, sowie der Statistik erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Zweck dies erfordert.

(3) Die Veröffentlichung personenbezogener Daten, die für Zwecke wissenschaftlicher oder historischer Forschung sowie der Statistik übermittelt wurden, ist zulässig, wenn

- a) die betroffene Person eingewilligt hat oder
- b) dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist, es sei denn, dass die Geschäftsführende Bundesleitung des Bundes beschließt, dass Grund zu der Annahme besteht, dass durch die Veröffentlichung der Auftrag des Bundes gefährdet würde.

(4) Die Offenlegung personenbezogener Daten an andere als Stellen des Bundes für Zwecke der wissenschaftlichen oder historischen Forschung, sowie der Statistik ist nur zulässig, wenn diese sich verpflichten, die offengelegten Daten nicht für andere Zwecke zu verarbeiten und die Vorschriften der Absätze 2 und 3 einzuhalten. Der Auftrag der Stellen des Bundes darf durch die Offenlegung nicht gefährdet werden.

(5) Die in den §§ 11, 12, 14 und 16 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß § 11 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

### § 34 Verarbeitung personenbezogener Daten für journalistische Zwecke

(1) Führt eine Verarbeitung gemäß § 5 Absatz 2 Buchstabe h) zur Veröffentlichung von Gendarstellungen der betroffenen Person, so sind diese Gendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Wird jemand durch eine Berichterstattung gemäß § 5 Absatz 2 Buchstabe h) in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die berichtenden oder einsendenden Personen oder die Gewährsleute von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann.

### § 35. Veranstaltungen von Gemeinden des Bundes

(1) Die Aufzeichnung oder Übertragung von Gottesdiensten oder anderen öffentlichen Veranstaltungen mittels audiovisueller Medien und die Veröffentlichung der Daten ist zulässig, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden.

(2) Betroffene können Widerspruch gemäß § 16 erheben, wenn schutzwürdige Interessen der Betroffenen das Interesse des Verantwortlichen überwiegen.

### § 36. Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Bereiche innerhalb und außerhalb von Dienstgebäuden mittels optisch-elektronischer Einrichtungen ist nur zulässig, soweit sie

1. in Ausübung des Hausrechts einer Stelle des Bundes oder
2. zum Schutz von Personen und Sachen

erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Interesse an der nicht überwachten Teilnahme an Veranstaltungen von Gemeinden des Bundes ist besonders schutzwürdig.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten der verantwortlichen Stelle sind gegebenenfalls durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(4) Die gespeicherten Daten dürfen von der verantwortlichen Stelle an eine Strafverfolgungsbehörde übermittelt werden, falls diese die Daten anfordert.

(5) Die Daten sind spätestens nach 1 Monat oder unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

## SECHSTER ABSCHNITT: DATENSCHUTZ IN RECHTLICH SELBSTSTÄNDIGEN EINRICHTUNGEN UND GEMEINDEN

### § 37. Geltung der Datenschutzordnung für selbstständige Einrichtungen

(1) Unterwirft sie sich ein Bundeswerk durch schriftliche Erklärung gegenüber der Geschäftsführenden Bundesleitung des Bundes den Regelungen dieser Ordnung, so gilt das Bundeswerk als Stelle des Bundes und die Regelungen dieser Ordnung gelten gegebenenfalls sinngemäß.

(2) Einrichtungen gemäß Absatz 1 regeln die Verantwortlichkeit für die Einhaltung dieser Ordnung und der allgemein gültigen Regelungen und Gesetze zum Datenschutz innerhalb ihrer jeweiligen Organisation.

(3) Einrichtungen gemäß Absatz 1 müssen einen Beauftragten für den Datenschutz im Sinne von § 26 bestellen. Der Beauftragte muss nicht Mitglied bzw. Beschäftigter der Einrichtung sein.

(4) Der Bund führt eine Übersicht über die Einrichtungen, für die die Datenschutzordnung entsprechend Absatz 1 gilt. In die Übersicht sind auf Basis der Mitteilung der Einrichtung jeweils aufzunehmen:

1. Name und Anschrift der Einrichtung und
2. Name und Anschrift des für den Datenschutz der Einrichtung Verantwortlichen und des Beauftragten für Datenschutz.

### § 38. Geltung der Datenschutzordnung für selbstständige Gemeinden

Für rechtlich selbstständige Gemeinden des Bundes gilt diese Ordnung entsprechend.

## SIEBENTER ABSCHNITT: SCHLUSSBESTIMMUNGEN

### § 39. Ergänzende Bestimmungen

(1) Die Geschäftsführende Bundesleitung des Bundes kann mit Zustimmung des Datenschutrates Durchführungsbestimmungen zu dieser Ordnung und ergänzende Bestimmungen zum Datenschutz beschließen. Diese dürfen dieser Ordnung nicht widersprechen.

(2) Die Stellen des Bundes können im Rahmen ihrer Befugnisse für ihren Bereich Durchführungsbestimmungen zu dieser Ordnung und ergänzende Bestimmungen zum Datenschutz beschließen. Diese dürfen dieser Ordnung nicht widersprechen. Die von der Geschäftsführenden Bundesleitung des Bundes beschlossenen Bestimmungen sind vorrangig.

(3) Soweit personenbezogene Daten von Sozialleistungsträgern offengelegt werden, gelten zum Schutz dieser Daten ergänzend die staatlichen Bestimmungen entsprechend.

## § 40. Übergangsregelungen

(1) Bisherige Bestellungen des Datenschutzbeauftragten des Bundes gemäß des § 12 der Datenschutzordnung des Bundes vom 8. August 2008 bleiben unberührt. Für diese Bestellung gelten die Regelungen des § 25 mit Inkrafttreten dieser Ordnung.

(2) Die Erstellung der Verfahrensverzeichnisse nach § 19 dieser Ordnung hat bis zum 30. Juni 2019 zu erfolgen.

## § 41. Gleichstellung

Wird in dieser Ordnung die männliche sprachliche Form der Personenbeschreibung verwendet, erlaubt dieses keinen Rückschluss auf das Geschlecht einer Person.

## § 42. Inkrafttreten, Außerkrafttreten

Diese Ordnung tritt am 24. Mai 2018 in Kraft. Gleichzeitig tritt die Datenschutzordnung des Bundes vom 08. August 2008 außer Kraft.

### **Datenschutz im Bund FeG**

**[datenschutz.feg.de](http://datenschutz.feg.de) | [datenschutz@feg.de](mailto:datenschutz@feg.de)**