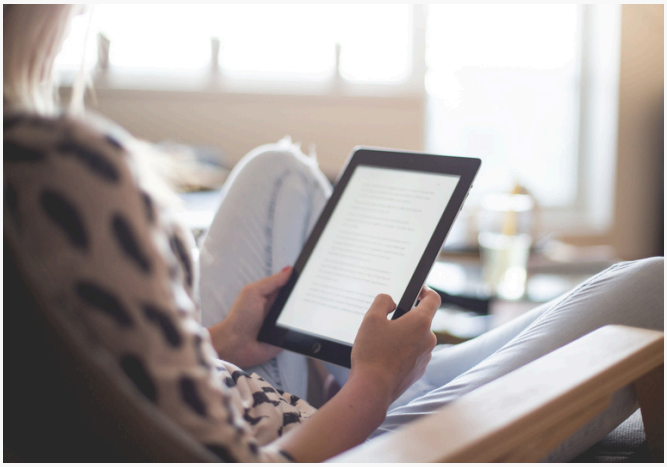
FORUM WISSEN, DAS ANKOMMT.


Leseprobe

Unsere Fachinhalte bieten Ihnen praxisnahe Lösungen, wertvolle Tipps und direkt anwendbares Wissen für Ihre täglichen Herausforderungen.

- **Praxisnah und sofort umsetzbar**: Entwickelt für Fach- und Führungskräfte, die schnelle und effektive Lösungen benötigen.
- **Fachwissen aus erster Hand**: Inhalte von erfahrenen Expertinnen und Experten aus der Berufspraxis, die genau wissen, worauf es ankommt.
- **Immer aktuell und verlässlich**: Basierend auf über 30 Jahren Erfahrung und ständigem Austausch mit der Praxis.

Blättern Sie jetzt durch die Leseprobe und überzeugen Sie sich selbst von der Qualität und dem Mehrwert unseres Angebots!

Vorlage

Bestandsaufnahme im Datenschutz

Begriffserklärungen

Datenschutzrechtliche Normierung

Für die Verarbeitungstätigkeit aller öffentlichen Institutionen gelten die datenschutzrechtlichen Normierungen der DSGVO grundsätzlich unmittelbar und haben gegenüber nationalen Normen Anwendungsvorrang. Für ausgewählte Tatbestände sieht die DSGVO jedoch vor, dass der nationale Gesetzgeber entsprechende Regelungen zu treffen hat oder zur Konkretisierung erlassen darf (Regelungsaufträge/-optionen). Welche nationale datenschutzrechtliche Normierung der Verarbeitungstätigkeit zugrunde liegt, ergibt sich zunächst aus der Institutionsform und aus der Aufgabe selbst:

- Sofern die Daten durch eine öffentliche Stelle des Bundes oder eine nicht öffentliche Stelle verarbeitet werden, findet das Bundesdatenschutzgesetz (BDSG) Anwendung.
- Öffentliche Stellen der Länder (Landesverwaltung, Kreisverwaltungen, Gemeinden, Zweckverbände und weitere der Aufsicht des Landes unterstehende Einrichtungen) wenden das jeweilige Landesdatenschutzgesetz (LDSG) an. Sonderfälle können öffentliche Stellen, die am wirtschaftlichen Leben teilnehmen, darstellen. Regelungen und Abgrenzungen finden sich in den jeweiligen LDSG.
- Sozialleistungsträger nach den §§ 12 ff. SGB I (z. B. Jugendämter, Sozialämter, Jobcenter etc.) wenden die Regelungen des Sozialdatenschutzes nach Kapitel 2 SGB X an.
- Kirchliche Einrichtungen unterliegen dem Anwendungsvorrang nicht, sofern sie zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung anwenden. Folglich gilt das jeweilige Kirchenrecht weiterhin, was in Einklang mit der DSGVO steht (DSG-EKD, KDG).

Mischformen in der Anwendung unterschiedlicher Datenschutznormen können sich dann ergeben, wenn verschiedene Aufgaben innerhalb einer Institution erfüllt werden. So kann es vorkommen, dass im kommunalen Bereich die Regelungen des LDSG Anwendung finden, während gleichzeitig für einzelne interne Stellen, die Leistungen nach einem der Bücher des SGB erbringen, das SGB X anzuwenden ist.

Oder aber nicht öffentliche bzw. kirchliche Stellen, die regulär dem BDSG/Kirchenrecht unterliegen, erfüllen im Rahmen einer Auftragsdatenverarbeitung Aufgaben für eine öffentliche Stelle, und die Anwendungen des jeweils geltenden LDSG wurden übertragen.

Eine weitere klassische Übertragung ist die Aufgabenerfüllung freier Träger der Jugendhilfe, denen durch Vertrag das Mindestniveau des Sozialdatenschutzes übertragen werden muss.

Automatisiertes Verfahren

Unter automatisierten Verfahren versteht man eine Datenverarbeitung, die durch den gesteuerten Einsatz von Technik ohne weiteres menschliches Zutun abläuft (bspw. Software-/IT-Anwendungen). Nichtautomatisierte Verfahren sind manuelle Verarbeitungstätigkeiten von personenbezogenen Daten, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen; dies betrifft auch Akten oder Aktensammlungen, sofern diese nach bestimmten Kategorien geordnet sind. Die Anforderungen sind gering, grundsätzlich muss eine Anwendbarkeit der DSGVO angenommen werden.

Verfahrensübersicht

Die Verfahrensübersicht soll dem Datenschutzbeauftragten einen Überblick verschaffen, welcher Bearbeitungsumfang zu automatisierten und nichtautomatisierten Verfahren gegeben ist. Da kaum zu erwarten ist, dass nichtautomatisierte Verfahren gänzlich ohne IT-Unterstützung ablaufen, sollte die Übersicht durch die Stelle ausgearbeitet werden, die für den IT-Betrieb verantwortlich ist, und mindestens nachfolgende Angaben enthalten. Sofern es nichtautomatisierte Verfahren gänzlich ohne Technikunterstützung gibt, sind diese durch die verantwortlichen Stellen anzugeben.

ID:

Unter der ID ist eine fortlaufende Nummer zu verstehen, die entweder durch den Datenschutzbeauftragten vergeben oder durch die IT-Abteilung in einem IT-Asset-Managementsystem geführt wird.

Bezeichnung:

An dieser Stelle ist der offiziell geführte Verfahrensname anzugeben.

Aufgabe:

Beschreibt die Aufgabe, die mit dem nicht-/automatisierten Verfahren umgesetzt werden soll. Sofern sie der Ausführung einer kraft Gesetzes übertragenen Aufgabe dient, kann auch die Norm angegeben werden.

Verantwortlichkeit:

Für jedes Verfahren ist eine bestimmte Organisationseinheit sachlich verantwortlich (nicht der IT-Bereich). Diese Verantwortlichkeit sollte hier angegeben werden.

Relevanz:

Sollte dem Datenschutzbeauftragten aufzeigen, ob dieses Verfahren datenschutzrechtliche Relevanz hat. Nahezu jedes Verfahren, welches personenbezogene Daten verarbeitet, ist relevant.

Verfahrensverzeichnis (VerfVerz):

Gibt an, ob für das Verfahren bereits ein Verzeichnis von Verarbeitungstätigkeit vorliegt.

Schutzbedarf:

Unter Schutzbedarf ist anzugeben, welche (ggf. besonderen) Anforderungen an die Sicherheit bei der Verarbeitungstätigkeit gestellt sind. Beispielweise sind Hinweise für besondere Vertraulichkeit (Gesundheitsdaten u. Ä.) oder Anforderungen an die Verfügbarkeit zu dokumentieren.

Verfahrensverzeichnis

Das Verzeichnis von Verarbeitungstätigkeiten (vormals Verfahrensverzeichnis oder -übersicht) entfaltet zwei wesentliche Funktionen. Zunächst dient die Erarbeitung und Befüllung mit Informationen der Selbstkontrolle. Die verantwortliche Stelle ist dadurch gezwungen, sich mit dem Verarbeitungsverfahren in Zusammenhang mit dem Datenschutz auseinanderzusetzen. Insbesondere die Dokumentation der technischen und organisatorischen Maßnahmen setzt voraus, dass solche definiert wurden und ein Mindestschutzniveau für das Verfahren eingeführt wurde.

Als weiterer Aspekt des Verzeichnisses kommt hinzu, dass es der datenschutzrechtlichen Transparenz dient. Die Betroffenen, also die Personen, deren Daten verarbeitet werden, haben gegenüber den Verantwortlichen ein umfangreiches Aufklärungsrecht, in welcher Art und Weise ihre Daten verarbeitet werden. Zwar entfällt die Pflicht der Stellen, das Verzeichnis den Betroffenen zur Einsicht zur Verfügung zu stellen, jedoch besteht die Pflicht zur Erstellung und zum Vorhalten, da es zumindest den Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen ist. Ferner kann die Einsichtnahme durch Betroffene hinsichtlich des Transparenzgedankens der DSGVO unterstützend zu den Informationspflichten nach Art. 13 f. DSGVO wirken.

Die Notwendigkeit zur Führung der Verzeichnisse ergibt sich aus Art. 30 DSGVO bzw. aus dem jeweiligen Kirchenrecht (§ 31 DSG-EKD, § 31 KDG).

Während bisher nicht für alle Verfahren, die personenbezogene Daten verarbeiten, Verzeichnisse zu erstellen waren, änderte sich dieser Grundsatz mit der DSGVO. Sowohl Art. 30 DSGVO als auch die kirchenrechtlichen und nationalen Bestimmungen sehen keine Ausnahmen mehr vor. Folglich ist für jede Verarbeitungstätigkeit, auch für nichtautomatisierte, ein solches Verzeichnis zu erarbeiten.

Die Zuständigkeit für die Erstellung eines Verarbeitungsverzeichnisses liegt in den Händen der Verantwortlichen. Nichtsdestotrotz sollte der Rat des Datenschutzbeauftragten bei der Erarbeitung eingeholt und jedes Verzeichnis als Kopie an diesen übergeben werden. Dies erscheint daher sinnvoll, um dem Datenschutzbeauftragten hinsichtlich seiner Kontrollpflichten einen Überblick über die Verfahren und die jeweiligen Verarbeitungstätigkeiten zu verschaffen und ihn in seinen Beratungsaufgaben gegenüber den Betroffenen zu unterstützen, indem ohne weitere Rückfragen einfache Auskünfte aus dem Verzeichnis erteilt werden können. Zu beachten ist, dass u. U. nationales Recht ein Einsichtsrecht einräumen kann (bspw. wie in § 4 Abs. 3 BbgDSG).

Die DSGVO sieht kein spezifisches Freigabeverfahren vor; teilweise sind solche Verfahren in der nationalen Gesetzgebung vorgeschrieben. Ungeachtet dessen ist die Etablierung eines förmlichen Freigabeverfahrens sinnvoll, um vor der Inbetriebnahme von Verarbeitungstätigkeiten die Wahrung der gesetzlichen Anforderungen sicherzustellen. In dem Freigabeverfahren sollte dokumentiert werden, ob

- das Verzeichnis von Verarbeitungstätigkeiten erstellt wurde,
- technische und organisatorische Maßnahmen für die Sicherheit der Verarbeitungstätigkeiten eingerichtet sind,
- sich im Falle der Notwendigkeit einer Datenschutzfolgenabschätzung ein positives Ergebnis ergeben hat,
- der Datenschutzbeauftragte an der Einführung der Verarbeitungstätigkeit beteiligt war.

Bestandsaufnahme im Datenschutz

Übergeordnete Anforderungen

	Prüffragen
☐	Die Institution hat einen Datenschutzbeauftragten bestellt.
☐	Der/Die Datenschutzbeauftragte verfügt über die erforderlichen Kompetenzen.
Es liegen Regelungen zur Organisation des Datenschutzes vor	
☐	Allgemeines (Geltungsbereich der Datenschutzanforderungen, Rechtsgrundlagen für die jeweilige Verarbeitungstätigkeit, Zweck, Verantwortlichkeiten, Zulässigkeit der Datenverarbeitung, Begriffsbestimmungen, Gewährleistungsziele)
☐	Organisation (Darstellung des Themas/Einordnung in die Ziele der Institution, Zuordnung der Funktionsträger, Aufgaben, Abgrenzung, Informationspflichten)
☐	Management ☐ **Anzeigepflichten**: Es ist sichergestellt, dass neue Aufgaben/Verfahren/Geschäftsprozesse rechtzeitig bei dem Datenschutzbeauftragten angezeigt werden und dieser zurate gezogen wird. ☐ **Verfahrensübersichten:** Es wird gewährleistet, dass mindestens jährlich eine Übersicht über alle Verarbeitungstätigkeiten übergeben wird. ☐ **Verzeichnisse von Verarbeitungstätigkeiten:** Es ist organisatorisch abgesichert, wer für die Erstellung verantwortlich ist und dass bei der Erarbeitung der Rat des Datenschutzbeauftragten eingeholt und eine Abschrift übergeben wird. ☐ **Datenschutzfolgenabschätzung:** Es ist definiert, wie eine Datenschutzfolgenabschätzung durchgeführt, zu welchem Zeitpunkt der Rat des Datenschutzbeauftragten eingeholt wird und welche Unterlagen zur Verfügung zu stellen sind. ☐ **Freigabeverfahren:** Es ist durch ein geeignetes (Freigabe-)Verfahren sichergestellt, dass vor Inbetriebnahme/Aufnahme einer Verarbeitungstätigkeit alle rechtlichen Erfordernisse erfüllt und diese dokumentiert wurden. ☐ **Besondere Verfahren:** Es gibt Regelungen, unter welchen Bedingungen besondere Verfahren, wie automatisierte Abrufverfahren, gemeinsame Verfahren, Videoüberwachungsmaßnahmen etc., zulässig sind. ☐ **Beteiligungspflichten:** Es ist gewährleistet, dass der Datenschutzbeauftragte vor dem Erlass aller datenschutzrelevanten Richtlinien zu beteiligen ist. ☐ **Sensibilisierungsmaßnahmen:** Es ist geregelt, in welchem Abstand Sensibilisierungen/Schulungen zum Datenschutz erfolgen und wer die Verantwortung trägt. ☐ **Revisionen/Beanstandungen:** Das Verfahren zur Durchführung von Datenschutzaudits und der Umgang mit Beanstandungen sind umschrieben.
☐	Technische und organisatorische Maßnahmen ☐ **Büroorganisation:** allgemeine Regelungen zum Büroalltag (Türen und Aktenschränke verschließen, keine Einsicht in Unterlagen Dritter, Beratungsgespräche in Großraumbüros, Auskünfte am Telefon) ☐ **IT-Verfahren:** Benutzung von IT, Passwortregeln, (Verbot von) Account-Sharing, Vertretungsregeln, Datensicherungsmaßnahmen, Internet-/E-Mail-Nutzung, Datenorganisation und Benennung ☐ **Protokolle:** Regelungen zu Protokollierungsmaßnahmen, Ausschluss Verhaltens- und Leistungskontrolle, Vorgehen bei Missbrauchsverdacht, Aufbewahrungsfristen ☐ **Übermittlungen:** Vorgaben für Datenübermittlungen ☐ **Weitergabe/Transport:** Transportregeln für Daten ☐ **Auftragsverarbeitung, Fern-/Wartung:** Vorlagen, Hinweise für die Vertragsgestaltung ☐ Entsorgung/Vernichtung von Daten
Die datenschutzrechtlichen Normierungen ergeben sich aus folgenden Gesetzen:	
☐	
Die automatisierten Verfahren, die personenbezogene Daten verarbeiten, sind in der folgenden Verfahrensübersicht dokumentiert:	
☐	

ID	Verfahrensname	Aufgabe	Verantwortlich	Relevanz		Relevanz		Schutzbedarf	Bemerkungen
				ja	nein	ja	ja		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		
				☐	☐	☐	☐		

Verzeichnis von Verarbeitungstätigkeiten

1. Namen, Anschrift und Kontaktdaten

Verantwortlicher

_____ _____

_____ _____

_____ _____

Datenschutzbeauftragte/-r

_____ _____

_____ _____

_____ _____

Auftragsverarbeiter (sofern zutreffend)

_____ _____

_____ _____

_____ _____

2. Bezeichnung des Verfahrens

ID: _____

Name: _____

Verantwortliche Organisationseinheit: _____

Zweckbestimmung und Rechtsgrundlage der Verarbeitung

Zweckbestimmung: _____

Rechtsgrundlage: _____

3. Betroffene Personengruppen und die diesbezüglichen Daten und Datenkategorien

Kreis der Betroffenen (falls möglich, sollte zusätzlich die Anzahl der betroffenen Personen – ggf. als Schätzung – angegeben werden.):

_____

Art der gespeicherten Daten oder Datenkategorien:

_____

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden:

_____

Werden Daten an ausländische und internationale Stellen übermittelt?: ☐ ja ☐ nein

Wenn ja, an die Stellen welcher Länder werden Daten übermittelt:

_____

_____

_____

Länder _____

Fristen für die Sperrung/Löschung der Daten

regelmäßige Prüffristen: _____

Löschfristen: _____

4. Beschreibung der technischen und organisatorischen Maßnahmen

Zugriffsberechtigte Personen:

_____

_____

_____

Allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der verwendeten Software

Allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen:

_____

Verwendete Software: _____

5. Vorabkontrolle und Freigabeerklärung

Das Verfahren unterlag der Datenschutzfolgenabschätzung, welche ein positives Ergebnis geliefert hat: ☐ ja ☐ nein

Das Verfahren wurde am _____ freigegeben. Die Freigabeerklärung ist als Anlage beigefügt.

_____ , den	_____
(Ort)	(Datum)
_____	_____
(Festlegende Stelle)	(Unterschrift)

WISSEN, DAS ANKOMMT.

Bestelloptionen

Formularmappe Datenschutz in öffentlichen und kirchlichen Einrichtungen

Sie haben Fragen zum Produkt oder benötigen Unterstützung bei der Bestellung? Unser Kundenservice ist für Sie da:

08233 / 381-123 (Mo - Do 7:30 - 17:00 Uhr, Fr 7:30 - 15:00 Uhr)

service@forum-verlag.com

Oder bestellen Sie bequem über unseren Online-Shop:

Jetzt bestellen

FORUM VERLAG HERKERT GMBH, Mandichostraße 18, 86504 Merching,
Tel.: (08233) 381 123, E-Mail: service@forum-verlag.com, Web: shop.forum-verlag.com