



Der Landesbeauftragte für den  
**DATENSCHUTZ** und die  
**INFORMATIONSFREIHEIT**  
Rheinland-Pfalz

**Best-Practice-Empfehlungen  
des LfDI Rheinland-Pfalz  
zum Datenschutz in der Kommunalverwaltung**



Stand: 20. Juni 2017

Herausgeber

Der Landesbeauftragte für den Datenschutz  
und die Informationsfreiheit Rheinland-Pfalz

Hintere Bleiche 34

55116 Mainz

[www.datenschutz.rlp.de](http://www.datenschutz.rlp.de)

[poststelle@datenschutz.rlp.de](mailto:poststelle@datenschutz.rlp.de)



**Best-Practice-Empfehlungen  
des LfDI Rheinland-Pfalz  
zum Datenschutz in der Kommunalverwaltung**

1. [Rahmenbedingungen für die Ausübung der Funktion der/des Datenschutzbeauftragten](#)
2. [Kriterien für die Auswahl einer/eines Datenschutzbeauftragten](#)
3. [Unterstützung der/des Datenschutzbeauftragten bei der Aufgabenwahrnehmung](#)
4. [Qualitätsmerkmale für die Tätigkeit der/des Datenschutzbeauftragten](#)
5. [Kommunikation und Netzwerkarbeit](#)
6. [Nachhaltigkeit des Datenschutzes in der Kommunalverwaltung](#)

[Anlagen](#)



## **Datenschutz in der Kommunalverwaltung**

Best-Practice-Empfehlungen des LfDI Rheinland-Pfalz (Stand: 20. Juni 2017)

---

### **Vorbemerkung**

Die Wahrung des 1983 durch das Volkszählungsurteil des Bundesverfassungsgerichts geschaffenen Grundrechts auf informationelle Selbstbestimmung ist verfassungsrechtlich geboten. Dementsprechend haben die Verwaltungen von Bund, Ländern und Kommunen im Rahmen des Gesetzesvollzugs die Vorgaben des Datenschutzes zu beachten. Hierbei kommt der Funktion des Datenschutzbeauftragten eine zentrale Bedeutung zu.

Ungeachtet dessen stellte der LfDI in der Vergangenheit im Rahmen seiner Beratungs- und Prüfungstätigkeit wiederholt fest, dass die Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben in der Landes- und Kommunalverwaltung im Praxisalltag nicht immer in vollem Umfang gewährleistet werden konnte. Verantwortlich waren nach Überzeugung des LfDI hierfür nicht nur individuelle Mängel bei der Rechtsanwendung, sondern auch strukturelle Defizite beim Datenschutzmanagement innerhalb der betroffenen Verwaltungen wie z.B. die fehlende oder zu späte Einbindung der/des eigenen Datenschutzbeauftragten, Zeitmangel oder Unkenntnis geeigneter Hilfestellungen. Zudem wurde das Beratungspotential des LfDI oft nur unzureichend ausgeschöpft.

Da aus Sicht des LfDI den Kommunalverwaltungen aufgrund der Vielzahl der dort zu erfüllenden Sachaufgaben eine besondere Bedeutung zur Sicherstellung des Datenschutzes zukommt, initiierte er im Herbst 2016 ein Projekt zur strukturierten Aufarbeitung der dargestellten Defizite. Ziel war es, gemeinsam mit vier ausgewählten Kommunalverwaltungen die wesentlichen Hürden bei der Beachtung des Datenschutzes im Verwaltungsalltag zu identifizieren und darauf aufbauend praktikable und inhaltlich abgestimmte Empfehlungen zur Stärkung des Datenschutzes und zur Verbesserung des Datenschutzmanagements zu entwickeln. Zugleich sollte damit ein Beitrag zur Vorbereitung der Verwaltungen auf die Anforderungen der Europäischen Datenschutz-Grundverordnung geleistet werden, die im Mai 2018 wirksam werden wird.

Die nun vorliegenden Best-Practice-Empfehlungen wurden im Juni 2017 veröffentlicht. An deren Erstellung waren neben dem LfDI die vier Projektkommunen (Landkreis Bad Kreuznach, Stadt Trier, Stadt Neuwied, Verbandsgemeinde Bad Bergzabern) beteiligt. Eine Unterstützung des mit den Empfehlungen verfolgten Anliegens durch die kommunalen Spitzenverbände des Landes, den Landesrechnungshof sowie das rheinland-pfälzische Innenministerium wird seitens des LfDI angestrebt.

---



## 1. Rahmenbedingungen für die Ausübung der Funktion der/des Datenschutzbeauftragten

Abhängig von der Größe und Aufgabenvielfalt der jeweiligen Kommunalverwaltung muss die Funktion der/des Datenschutzbeauftragten mit den für eine angemessene Aufgabenerfüllung erforderlichen Personal- und Sachressourcen ausgestattet werden. Die Kombination mit der Funktion des Informationssicherheitsbeauftragten sowie kommunale Kooperationen bei der Bestellung von Datenschutzbeauftragten können sinnvoll sein.

In der Praxis bedeutet dies:

- ♦ In Landkreisen, kreisfreien und großen kreisangehörigen Städten hat die Funktion der/des Datenschutzbeauftragten mindestens einen Personalbedarf in Höhe von 50 % einer Vollzeitstelle des 3. Einstiegsamtes. [Näheres hierzu im Dokument [„Stellenbemessung und Stellenbewertung der Funktion des kommunalen Datenschutzbeauftragten“](#)] In Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen kann der Personalbedarf davon abweichen. Für die Personalbemessung ist die aktuelle Beschreibung der Aufgaben der/des Datenschutzbeauftragten in der Kommunalverwaltung zugrunde zu legen, die der LfDI veröffentlicht hat [vgl. [Orientierungshilfe des LfDI zu den Aufgaben des behördlichen Datenschutzbeauftragten in der Kommunalverwaltung](#)].
- ♦ Es sollten Vorkehrungen getroffen werden, in welcher Weise die Aufgaben der/des Datenschutzbeauftragten wahrgenommen werden, falls die Stelleninhaberin bzw. der Stelleninhaber vorübergehend oder dauerhaft abwesend ist. Regelmäßig empfiehlt es sich, in diesem Zusammenhang eine Vertreterregelung zu treffen.
- ♦ Sofern eine Zusammenlegung der Funktionen der/des Datenschutzbeauftragten und der/des Informationssicherheitsbeauftragten erwogen wird, wäre dies nur unter Beibehaltung der jeweils benötigten Ressourcen denkbar. Insbesondere sollten keine Abstriche an dem für die Wahrnehmung der Funktion des Datenschutzbeauftragten veranschlagten Zeitbudgets vorgenommen werden.
- ♦ Für Verbandsgemeinde- und verbandsfreie Gemeindeverwaltungen sollten die Vorteile einer Kooperation mit anderen gleichartigen Kommunen bei der Bestellung von Datenschutzbeauftragten mit dem damit einhergehenden Aufwand abgewogen werden [Näheres hierzu im Dokument [„Kooperationsmöglichkeiten von Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen bei der Ausübung der Funktion des Datenschutzbeauftragten“](#)].



## 2. Kriterien für die Auswahl einer/eines Datenschutzbeauftragten

Angesichts der vielfältigen und bedeutsamen Aufgaben, die mit der Funktion der/des Datenschutzbeauftragten einer Kommunalverwaltung verbunden sind, sollten im Vorfeld einer Bestellung verschiedene Kriterien bei der Personalauswahl berücksichtigt werden. Dies betrifft sowohl fachliche als auch persönliche Anforderungen. Zudem ist es für eine optimale Wahrnehmung der Funktion von entscheidender Bedeutung, im Vorfeld mögliche Interessenkollisionen mit sonstigen Aufgaben zu vermeiden. Die Benennung externer Personen ist rechtlich zwar möglich, nutzt aber nicht den Vorteil, dass kommunale Beschäftigte die Besonderheiten der eigenen Verwaltung am besten kennen und darauf aufbauend zügig sachnahe und passgenaue Lösungen entwickeln können.

In der Praxis bedeutet dies:

- ◆ In rechtlicher Hinsicht sollte der/die Bewerber/in bereit und in der Lage sein, datenschutzrelevante Rechtsvorschriften zu erkennen und zu verstehen und diese in der kommunalen Praxis anzuwenden. Dabei sollte er/sie auch fähig sein, in sachlichen Zusammenhängen, die ihm/ihr zunächst fremd sind, mit datenschutzrelevanten Inhalten umzugehen und insbesondere sachgerechte und praktikable Lösungen anzustoßen. [Näheres hierzu im Dokument [„Anforderungsprofil für kommunale Datenschutzbeauftragte“](#)].
- Das Anforderungsprofil der/des Datenschutzbeauftragten setzt mittelfristig Grundkenntnisse in den Bereichen Informations-/Telekommunikationstechnik und Verwaltungsorganisation voraus. Eine Bewerberin bzw. ein Bewerber sollte daher zumindest die Bereitschaft und die Fähigkeit haben, sich mit diesen Themenfeldern zu befassen. Ziel ist es, Verwaltungsvorgänge und deren IT-gestützte Bearbeitung nachvollziehen und ggf. bestehende datenschutzrechtliche Fragestellungen identifizieren zu können [Näheres hierzu im Dokument [„Anforderungsprofil für kommunale Datenschutzbeauftragte“](#)].
- ◆ Von einer zu vermeidenden Interessenkollision ist regelmäßig auszugehen bei Beschäftigten aus den Bereichen Organisation, IT-Administration oder IT-Anwendungsbetreuung und den dafür Verantwortlichen. Diese sollten daher nicht ausgewählt werden. Dagegen kommen z.B. in der Revision tätige Mitarbeiter/innen, Sicherheitsbeauftragte, Beschäftigte des Rechnungsprüfungsamtes oder der Kämmerei, Bedienstete mit Aufgaben der jeweiligen Fachverwaltung grundsätzlich als Bewerber/innen in Betracht.



- ♦ Darüber hinaus sollten Bewerber über ein sicheres Auftreten, Durchsetzungsvermögen, Kommunikations- und Kooperationsfähigkeiten, ein gutes Ausdrucksvermögen und eine grundlegende Aufgeschlossenheit für das Anliegen des Datenschutzes und damit zusammenhängender neuer Entwicklungen verfügen.
- ♦ Soweit eine Bestellung externer Personen erwogen wird, ist zu bedenken, dass diese die Strukturen und Abläufe der Verwaltung nicht so gut kennen wie eigene Mitarbeiter und zudem deren Präsenz und Verfügbarkeit vor Ort leider nur eingeschränkt gewährleistet ist. Dies kann sich in der Praxis als bedeutsames Hindernis bei der Wahrnehmung der Aufgaben des Datenschutzbeauftragten herausstellen. Zumindest in Landkreisen, kreisfreien und großen kreisangehörigen Städten sollte daher wenn möglich auf die Benennung nicht in der Verwaltung beschäftigter Personen verzichtet werden.



### 3. Unterstützung der/des Datenschutzbeauftragten bei der Aufgabenwahrnehmung

Die Verwaltungsspitze hat die Person der/des Datenschutzbeauftragten im Rahmen ihrer Tätigkeit umfassend zu unterstützen. Ein regelmäßiger Austausch mit der Leitungsebene ist hierbei unerlässlich. Da ohne eine funktionierende Kooperation der Beschäftigten mit der/dem Datenschutzbeauftragten die Funktion nicht erfolgreich ausgeübt werden kann, müssen die verwaltungsinternen Arbeitsprozesse dies sicherstellen.

#### In der Praxis bedeutet dies:

- ◆ Nach der Bestellung der/des Datenschutzbeauftragten sollte die Verwaltungsspitze alle Beschäftigten umgehend über die beauftragte Person, deren Kontaktdaten (insbesondere eigene Funktionsmailadresse) und deren Aufgaben unterrichten. Zugleich sollten die Beschäftigten auf die hervorgehobene Stellung der Funktion hingewiesen und zur Kooperation aufgefordert werden. Die Folgen einer bewussten Missachtung datenschutzrechtlicher Vorgaben oder einer Weigerung, mit der/dem Datenschutzbeauftragten zu kooperieren, sollten intern bekannt gemacht werden.
- ◆ Sobald eine Person als Datenschutzbeauftragte/r bestellt wurde, sollten ihr/ihm sämtliche zur Wahrnehmung der Funktion notwendigen Unterlagen, Informationen und Sachmittel zur Verfügung gestellt werden. Dies umfasst auch das seitens des LfDI zu diesem Zweck erstellte Informationspaket („Starterkit“) [Näheres hierzu im Dokument [„Starterkit für neue Datenschutzbeauftragte“](#)].
- ◆ Entsprechend der Stellung der/des Datenschutzbeauftragten sollte ein regelmäßiger Austausch mit der Verwaltungsspitze („jour fixe“) vereinbart werden, bei dem die/der Datenschutzbeauftragte über ihre/seine Tätigkeit berichtet.
- ◆ Zur Vermeidung von Interessenkollisionen sollte die Tätigkeit als Datenschutzbeauftragte/er deutlich von sonstigen hierarchiegebundenen Aufgaben der beauftragten Person getrennt werden. Dies gilt insbesondere für die einzuhaltenden Dienstwege. In diesem Zusammenhang getroffene Maßnahmen wie z.B. Verfahrensanweisungen sollten verwaltungsintern bekannt gemacht werden.
- ◆ Zur Sicherstellung einer rechtzeitigen und umfassenden Einbindung der/des Datenschutzbeauftragten in datenschutzrelevante Sachverhalte sollten geeignete organisatorische Vorkehrungen wie z.B. die Festlegung von Workflows getroffen werden.
- ◆ Dem erkennbaren Fort- und Weiterbildungsbedarf der/des Datenschutzbeauftragten sollte angemessen entsprochen werden.





#### 4. Qualitätsmerkmale für die Tätigkeit der/des Datenschutzbeauftragten

Die Einrichtung eines erfolgreichen Datenschutzmanagements ist die zentrale Aufgabe der/des Datenschutzbeauftragten. Dazu gehört, die Beschäftigten auf ihre Verantwortung zum Schutz personenbezogener Daten aufmerksam zu machen, ihnen die für ihre Tätigkeit relevanten Informationen zum Datenschutz zur Verfügung zu stellen sowie in konkreten datenschutzrelevanten Sachverhalten zu beraten. Es empfiehlt sich, die Effektivität des praktizierten Datenschutzmanagements regelmäßig zu überprüfen. Eine enge Zusammenarbeit mit den Organisationseinheiten, die verwaltungsintern für die Bereiche „Organisation“ und „IT“ zuständig sind, ist ratsam.

##### In der Praxis bedeutet dies:

- ♦ Die/der Datenschutzbeauftragte sollte den Beschäftigten in leicht zugänglicher Form allgemeine Informationen bereitstellen, die die Verantwortlichkeit der Verwaltung für den Schutz personenbezogener Daten erläutern. Hierzu gehören auch die von der Verwaltung getroffenen technisch-organisatorischen Maßnahmen zum Datenschutz wie z.B. Dienstanweisungen oder Dienstvereinbarungen sowie ein Hinweis auf die Aufgaben der/des Datenschutzbeauftragten. Die Möglichkeiten der elektronischen Unterrichtung z.B. durch das hausinterne Intranet sollten genutzt werden.
- ♦ Für die Wahrnehmung der Beratungsaufgabe der/des Datenschutzbeauftragten kommt es wesentlich auf deren/dessen Einbindung in die datenschutzrelevanten Verwaltungsvorgänge an. Neben einer allgemeinen Sensibilisierung der Beschäftigten durch die Leitungsebene sollte auch die/der Datenschutzbeauftragte um ihre/seine Beteiligung aktiv und regelmäßig in der Verwaltung werben. Unmittelbare Kontaktaufnahmen mit Organisationseinheiten können zur Ermittlung des Beratungsbedarfs hilfreich sein.
- ♦ Aufgrund ihrer zentralen Bedeutung bei der Gewährleistung des Datenschutzes in der Kommunalverwaltung sollte die/der Datenschutzbeauftragte einen regelmäßigen Austausch mit den Organisationseinheiten, die für die Bereiche „Organisation“ und „IT“ verantwortlich sind, pflegen.
- ♦ Über das Bestehen datenschutzrechtlicher Grundkenntnisse in den einzelnen Fachbereichen der Verwaltung, bei denen regelmäßig personenbezogene Daten verarbeitet werden, sollte sich die/der Datenschutzbeauftragte aktiv und in geeigneter Form einen Überblick verschaffen. Soweit diesbezüglich oder aufgrund der besonderen Schutzbedürftigkeit der in einem einzelnen Fachbereich verarbeiteten Daten von einem konkreten Schulungsbedarf der Beschäftigten ausgegangen werden kann, sollte die/der



Datenschutzbeauftragte die hierfür geeigneten Maßnahmen anstoßen. In Betracht kommen dafür neben professionellen Fortbildungen, die primär der allgemeinen Wissensvermittlung dienen, auch hausinterne Veranstaltungen, bei denen zeitlich kompakt beispielsweise Rechtsgrundlagen dargestellt oder konkrete Fragestellungen erörtert werden. Abhängig von der Größe und Vielfalt der Verwaltung kann die Erstellung eines Schulungskonzepts hilfreich sein.

- ♦ Die/der Datenschutzbeauftragte sollte die Wirksamkeit des in der Verwaltung betriebenen Datenschutzmanagements durch geeignete Instrumente überprüfen und gemeinsam mit der Verwaltungsspitze evaluieren. Dies betrifft sowohl die eigene Tätigkeit der/des Datenschutzbeauftragten als auch die seitens der Verwaltung getroffenen Maßnahmen. Gerade angesichts der im Mai 2018 wirksam werdenden Europäischen Datenschutz-Grundverordnung, die der Funktion der/des Datenschutzbeauftragten deutlich mehr Kontrollaufgaben verleihen wird, sollten sich die Verwaltungen frühzeitig auf derartige Anforderungen einstellen. Es empfiehlt sich, die zur Evaluierung des Datenschutzmanagements vorgesehenen Maßnahmen im Vorfeld festzulegen und intern bekannt zu machen. In Frage kommen z.B. anlasslose Besuche in den Fachbereichen, stichprobenweise Überprüfungen konkreter Maßnahmen oder allgemein Feedback-Gespräche. Auch die regelmäßigen Austausche mit der Leitungsebene und bestimmten Organisationseinheiten sollten diesem Zweck dienen.



## 5. Kommunikation und Netzwerkarbeit

Die Erfüllung der Aufgaben einer/eines Datenschutzbeauftragten hängt insbesondere von einer regelmäßigen, offenen und unmittelbaren Kommunikation der/des Beauftragten mit den einzelnen Stellen der Verwaltung ab. Dies muss sichergestellt werden. Im Hinblick auf die Zusammenarbeit mit dem LfDI als zuständiger Datenschutzaufsicht ist es ratsam, die Kommunikationswege intern transparent festzulegen und bekannt zu machen. Schließlich bietet eine Teilnahme an Netzwerken zum Datenschutz die Chance, aus den Erfahrungen anderer Stellen zu profitieren.

### In der Praxis bedeutet dies:

- ♦ Die/der Datenschutzbeauftragte sollte unmittelbare Kommunikationskanäle mit der Leitungsebene und den Organisationseinheiten, die für die Bereiche „Organisation“ und „IT“ verantwortlich sind, aufbauen und pflegen.
- ♦ Bezüglich der sonstigen Fachbereiche sollte die/der Datenschutzbeauftragte geeignete und praktikable Kommunikationswege vereinbaren. Abhängig von der Datenschutzrelevanz der jeweiligen Aufgabenstellungen empfiehlt es sich, konkrete Ansprechpartner in einzelnen Fachbereichen zu benennen, die zugleich als Multiplikator herangezogen werden können.
- ♦ In Übereinstimmung mit der ab Mai 2018 wirksam werdenden Datenschutz-Grundverordnung sollte verwaltungsintern festgelegt werden, dass die Kommunikation zwischen der Kommunalverwaltung und dem LfDI in seiner Funktion als Aufsichtsbehörde regelmäßig unter Einbindung des/der Datenschutzbeauftragten erfolgt.
- ♦ An Netzwerken zum Datenschutz sollte wenn möglich teilgenommen werden. Dies gilt insbesondere für das vom LfDI für die Netzwerkarbeit verwendete Forum. Zugleich sollte eine Teilnahme an den Netzwerktreffen des LfDI ermöglicht werden.
- ♦ Der Aufbau regionaler Datenschutz-Netzwerke kann insbesondere Verbandsgemeinde- und sonstigen Gemeindeverwaltungen bei der Sicherstellung des Datenschutzes behilflich sein.



## 6. Nachhaltigkeit des Datenschutzes in der Kommunalverwaltung

Der Schutz des informationellen Selbstbestimmungsrechts muss auch im Bereich der Kommunalverwaltungen nachhaltig sein. Deshalb ist eine Dokumentation der in diesem Zusammenhang ergriffenen Maßnahmen und Tätigkeiten geboten. Zugleich kann dadurch ein eigener Wissenspool aufgebaut werden, der sowohl künftigen Datenschutzbeauftragte als auch Beschäftigte bei der Beachtung des Datenschutzes unterstützt.

### In der Praxis bedeutet dies:

- ♦ Die/der Datenschutzbeauftragte sollte sämtliche in dieser Funktion durchgeführten Aktivitäten in einer angemessenen und sicheren Form dokumentieren. Es empfiehlt sich, die Art und Weise der Dokumentation einschließlich der beabsichtigten Struktur und Zugriffsmöglichkeiten mit der Verwaltungsspitze abzustimmen. Benötigte technische oder organisatorische Unterstützungen sollten gewährt werden.
- ♦ Auf der Basis dieser Dokumentation sollte in regelmäßigen Abständen durch die/den Datenschutzbeauftragten eine Übersicht über die in einem bestimmten Zeitintervall erfolgten Tätigkeiten erstellt werden (Tätigkeitsbericht). Form und Umfang des Tätigkeitsberichtes sollten in angemessener Weise und unter Berücksichtigung der zur Verfügung stehenden Ressourcen erfolgen. Der Tätigkeitsbericht sollte mit der Verwaltungsspitze erörtert werden.
- ♦ Die/der Datenschutzbeauftragte sollte klären, ob und ggf. in welcher Form der Aufbau eines verwaltungseigenen Wissenspools zum Datenschutz, der für alle Beschäftigten zugänglich wäre, unter Nutzung der erstellten Tätigkeitsberichte erforderlich ist und realisiert werden kann. Die Möglichkeiten der vorhandenen elektronischen Informations- und Kommunikationssysteme (z.B. Intranet) sollten dabei genutzt werden.



## **Ausblick**

Mit dem Wirksamwerden der Europäischen Datenschutz-Grundverordnung am 25. Mai 2018 wird das Datenschutzrecht innerhalb der Mitgliedstaaten der Europäischen Union vereinheitlicht. Für das Datenschutz-Management bei den Stellen der öffentlichen Verwaltung hat dies gravierende Auswirkungen, da die Grundverordnung hier wesentliche Verschärfungen gegenüber dem bisherigen Recht vorsieht. So werden einerseits die Aufgaben und Befugnisse der/des internen Datenschutzbeauftragten deutlich ausgeweitet und andererseits die dazu korrespondierenden Pflichten der verantwortlichen Stellen merklich verstärkt.

Die vorliegenden Best-Practice-Empfehlungen sollen den rheinland-pfälzischen Kommunalverwaltungen die Möglichkeit geben, sich frühzeitig auf die Anforderungen der im Mai 2018 eintretenden Rechtsänderungen einzustellen. Ziel ist es, bei den Verwaltungen schon jetzt die Wahrung des Datenschutzes als zwingenden gesetzlichen Auftrag bei der eigenen Aufgabenerfüllung bewusst zu machen und zugleich die Bereitstellung der hierfür notwendigen und angemessenen Ressourcen sicherzustellen. Da der Funktion der/des Datenschutzbeauftragten künftig eine noch wichtigere Bedeutung bei der Sicherstellung des Datenschutzes zukommen wird, sollten die Verwaltungen schon jetzt die bereits bestehenden Möglichkeiten zur Verbesserung des internen Datenschutz-Managements nutzen. Hierzu geben die Best-Practice-Empfehlungen nützliche Hilfestellungen.

Der LfDI wird die Inhalte der Best-Practice-Empfehlungen permanent auf ihre Aktualität und Geeignetheit überprüfen und bei Bedarf anpassen. In diesem Zusammenhang stehende Anregungen oder Hinweise werden gerne entgegengenommen.



**Anlagen zu den  
Best-Practice-Empfehlungen  
des LfDI Rheinland-Pfalz  
zum Datenschutz in der Kommunalverwaltung**

- ♦ [Papier zur Stellenbemessung und Stellenbewertung der Funktion des kommunalen Datenschutzbeauftragten](#)  
(Stand: 20. Juni 2017)
- ♦ [Orientierungshilfe zu den Aufgaben des behördlichen Datenschutzbeauftragten in der rheinland-pfälzischen Kommunalverwaltung](#)  
(Stand: 20. Juni 2017)
- ♦ [Papier zu den Kooperationsmöglichkeiten von Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen bei der Ausübung der Funktion des Datenschutzbeauftragten](#)  
(Stand: 20. Juni 2017)
- ♦ [Papier zum Anforderungsprofil für kommunale Datenschutzbeauftragte](#)  
(Stand: 20. Juni 2017)
- ♦ [Übersicht zum „Starterkit“ für neue Datenschutzbeauftragte](#)  
(Stand: 20. Juni 2017)



## **Anlage 1**

### **Stellenbemessung und Stellenbewertung der Funktion des kommunalen Datenschutzbeauftragten (Stand: 20. Juni 2017)**

---

#### **Vorbemerkung**

Der Personalbedarf eines kommunalen Datenschutzbeauftragten (DSB) ist sowohl quantitativ (Stellenbemessung) als auch qualitativ (Stellenbewertung) durch die personalverantwortliche Stelle individuell für die eigene Organisation zu ermitteln. In seiner Beratungs- und Prüfungstätigkeit stellte der LfDI vermehrt fest, dass der bislang von den Kommunalverwaltungen zugrunde gelegte Personalbedarf für die Funktion des Datenschutzbeauftragten deutlich unter dem bereits derzeit gesetzlich gebotenen Bedarf liegt. Aus diesem Grund wurden in dem vom LfDI zwischen November 2016 und Juni 2017 durchgeführten Projekt „Datenschutz-update in der Kommunalverwaltung“ folgende Hilfestellungen für die Kommunalverwaltungen zur Stellenbemessung und Stellenbewertung kommunaler Datenschutzbeauftragte entwickelt. Der Berechnung liegt die Aufgabenbeschreibung für kommunale Datenschutzbeauftragte zugrunde, die der LfDI ebenfalls im Rahmen des Projektes im Juni 2017 veröffentlicht hat.

Vorab sei darauf hingewiesen, dass eine Personalbedarfsberechnung lediglich dann sinnvoll ist, wenn zuvor die zugehörigen Geschäftsprozesse (Arbeitsvorgänge) entsprechend den Best-Practice-Empfehlungen des LfDI optimiert worden sind. Zudem müssten nach Einschätzung des LfDI bei einer verbindlichen Personalbedarfsfeststellung im nachfolgenden Sinne die Stellenpläne der betroffenen Kommunalverwaltungen modifiziert werden.

Mit den vorgelegten Empfehlungen werden erstmals die für eine Wahrnehmung der gesetzlichen Aufgaben eines Datenschutzbeauftragten erforderlichen Rahmenbedingungen, soweit es um den Personalbedarf geht, konkretisiert. Dies ist vor dem Hintergrund der bislang nur unzureichenden Personalausstattung kommunaler Datenschutzbeauftragter im Lande geboten, zumal im Bereich der Informationssicherheit bereits seit geraumer Zeit vergleichbare Empfehlungen seitens des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) existieren. Die vorgeschlagenen Richtwerte haben ausschließlich empfehlenden Charakter und dienen als Diskussionsgrundlage im Zusammenhang mit der Erfüllung der künftigen durch die Europäische Datenschutz-Grundverordnung auch den Kommunalverwaltungen zugewiesenen Pflichten. Vor diesem Hintergrund wird der LfDI diesbezüglich einen zeitnahen Konsens mit den kommunalen Spitzenverbänden des Landes, dem Landesrechnungshof sowie dem rheinland-pfälzischen Innenministerium anstreben.

---



## 1. Stellenbemessung

Für die Berechnung des Zeitanteils des DSB ist die methodische Stellenbemessung heranzuziehen. Diese dient grundsätzlich der Feststellung des Arbeitsaufwandes, der angemessenen Arbeitsmenge je Mitarbeiter und der benötigten Stellen je Organisationseinheit. Für die Feststellung der anfallenden Arbeitsmenge sind die **Tätigkeiten** festzulegen (siehe Aufgabenbeschreibung des DSB) und die **Fallzahlen** sowie die **Mittlere Bearbeitungszeit (mBz)** zu schätzen oder zu messen. Für die Schätzung bzw. Messung maßgeblich sind u.a. folgende Aspekte:

- Art der Verwaltung/Aufgabenspektrum
- Einwohnerzahl der Gemeinde
- Anzahl der Bediensteten
- Anzahl der IT-gestützten Arbeitsplätze und
- Art und Umfang der Verarbeitung personenbezogener Daten.

So sind regelmäßig in Landkreisen, kreisfreien und großen kreisangehörigen Städten aufgrund des breiteren Aufgabenzuschnitts die Fallzahlen und die mBz höher. Zu den erweiterten Aufgaben mit besonderem datenschutzrechtlichem Bezug zählen hier beispielsweise die Aufgaben nach den SGB (spezialgesetzliche Datenschutzregelungen), Einrichtung von Eigenbetrieben (z.B. Abfallwirtschaftsbetrieb), Schulträgerschaften und das Gesundheitswesen (besondere Arten personenbezogener Daten).

In datenschutzsensiblen Bereichen ist mit mehr Fallzahlen und längeren Bearbeitungszeiten (z.B. Begleitung der Einführung eines datenschutzrechtlich anspruchsvollen Verfahrens) zu rechnen.

Bei zeitlich vorübergehenden Arbeitsspitzen kann eine flexible Handhabung der Freistellung sinnvoll sein.

Vereinfachte Personalbedarfsberechnungsformel:

$$P = \frac{\text{Arbeitsmenge}}{\text{Zeitliche Verfügbarkeit einer Kraft}}$$

$$P = \frac{\sum(Fz * mBz) + nft}{NAK - pbA}$$





- P = Personalbedarf
- Fz = Fallzahlen
- mBz = mittlere Bearbeitungszeit
- pbA = persönlich bedingter Arbeitsausfall
- nFT = nicht fallbezogene Tätigkeiten<sup>1</sup>
- NAK = Arbeitszeit einer Normalarbeitskraft
- JAM = Jahresarbeitsminuten

Für die Arbeitszeit einer Normalarbeitskraft (NAK) kann auf die NAK-Richtwerte der KGSt zurückgegriffen werden. Diese betragen für Beamte 98.300 Minuten und für Beschäftigte 94.700 Minuten. Nach Empfehlung der KGSt ist hiervon ein pbA in Höhe von 8.500 Minuten abzuziehen, um die zeitliche Verfügbarkeit einer Kraft zu erhalten.

Beispielberechnung:

Aufgabe	Kommunalverwaltung X		
	Fz	mBz	JAM
Beratung von Mitarbeitern/Organisationseinheiten schriftlich			
Beratung von Mitarbeitern/Organisationseinheiten mündlich			
Abstimmung mit Multiplikatoren			
Abstimmung IT/Organisation (Rechtevergabe)			
Vorabkontrolle gem. § 9 Abs. 5 LDSG			
Dokumentation der Beratungstätigkeit			
Information der Verwaltungsspitze			
Aufbau/Pflege Intranetauftritt/Wissenspool			
Eigene Fortbildung			
Anlassbezogene Kommunikation mit LfDI Rheinland-Pfalz			
Beteiligung an Netzwerkarbeit, Forenteilnahme und Regionaltreffen			
Schulung von Mitarbeitern			
Qualitätsmanagement (Aufsuchen der Fachbereiche)			
Führung Verfahrensverzeichnis gem. § 10 LDSG neue Verfahren Updates			
Eingaben/Betroffenenrechte			
Sonstiges			
.....			
.....			

<sup>1</sup>bei der Berechnung des Zeitanteils des DSB nicht relevant; für die Gesamtberechnung der angemessenen Arbeitsmenge je Mitarbeiter allerdings schon



Im Hinblick auf die kommende Europäische Datenschutz-Grundverordnung (DS-GVO), in der die Stellung der DSB nochmals aufgewertet und weitere Tätigkeiten wie erweiterte Kontrollaufgaben, die aufwändigeren Dokumentationspflichten bei der Beratungs- und Prüftätigkeit hinzukommen und der Tatsache, dass momentan zugrundeliegende Fallzahlen den Stand vor der Optimierung der Verwaltungsprozesse abbilden, ist aus Sicht des LfDI davon auszugehen, dass der Personalbedarf deutlich höher liegen wird. In Landkreisen, kreisfreien und großen kreisangehörigen Städten hat die Funktion der/des DSB mindestens **einen Personalbedarf in Höhe von 50 Prozent einer Vollzeitstelle** des dritten Einstiegsamtes (früher: gehobener Dienst). In Verbandsgemeinde- und sonstigen Gemeindeverwaltungen kann der Personalbedarf davon abweichen.

## 2. Stellenbewertung

Unter der Stellenbewertung versteht man das Bewerten der mit der Wahrnehmung einer Stelle verbundenen Anforderungen und deren Zuordnung zu einer Besoldungs- oder Entgeltgruppe, je nachdem, ob es sich um eine Beamtenstelle oder die Stelle eines/r tariflich Beschäftigten handelt. Grundlage der Stellenbewertung ist die Stellenbeschreibung, in der die mit der Stelle verbundenen Aufgaben festgeschrieben sind. Objekt der Stellenbewertung ist die Tätigkeit, die der Stelle hinsichtlich der Anforderungen das Gepräge gibt.

Rechtliche Grundlagen für die Stellenbewertung der Beamten begründen § 18 Bundesbesoldungsgesetz (BBesG) sowie § 21 Landesbesoldungsgesetz (LBesG). Für Beschäftigte treffen der TVöD sowie die einschlägige Rechtsprechung die Grundregelungen.

Die Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt) hat in ihren Gutachten aus den Jahren 1970/1982/1988/1998 und letztmals in 2009 ein in der Praxis allgemein anerkanntes und angewandtes analytisches, anforderungsorientiertes Stellenbewertungsverfahren **für Beamte** entwickelt.

In dem Verfahren werden Einzelanforderungen für sich erfasst und bewertet. Das Verfahren findet nach dem Wertzahlverfahren statt. Das Bewertungsmodell enthält 6 unterschiedliche Anforderungen; für jede dieser Anforderungen besteht eine Stufenskala, die den Grad der Anforderungen jeweils auf 4 – 10 Stufen differenziert. Jede dieser Stufen führt zu einer festgelegten Punktzahl. Größtes Gewicht ist den Bewertungsmerkmalen „Schwierigkeitsgrad der Informationsverantwortung“ und „Grad der Verantwortung“ beigemessen, das geringste Gewicht hat der „Grad der Erfahrung“. Grundsätzlich maßgeblich sind die höchsten Anforderungen mit



Ausnahme des „Schwierigkeitsgrades der Informationsverarbeitung“, da die Tätigkeiten hier mehr als 50% der Arbeitszeit erfordern müssen.

Für einen **DSB einer Kreisverwaltung** könnte die Stellenbewertung nach dem Stellenbewertungsverfahren der KGSt folgendermaßen aussehen:

Name, Vorname: N.N.  
Organisationseinheit: Behördlicher Datenschutzbeauftragter (unmittelbar dem Landrat unterstellt)  
Funktion: Behördlicher Datenschutzbeauftragter  
Bes.-Gr.: neu

Bewertungsstufe	Stufenbeschreibung	Wertzahl
<b>1. Schwierigkeitsgrad der Informationsverarbeitung (25%)</b>		
6	Die zu verarbeitenden Informationen des DSB sind umfangreich (Stufe 5), da rechtsgebietsübergreifend auf die Einhaltung des Datenschutzes hinzuwirken ist. Hierbei sind vielfach auch Überlegungen zum methodischen Vorgehen anzustellen. Sachverhalte sind datenschutzrechtlich zu bewerten und in ein rechtliches Ergebnis zu verarbeiten (vgl. Stufe 7 Satz 2). Insgesamt ist daher die Zwischenstufe 6 anzusetzen.	125
<b>2. Schwierigkeitsgrad der dienstlichen Beziehungen (10%)</b>		
4	Zur Wahrnehmung der Aufgaben sind typischerweise Gespräche und Kontakte mit sämtlichen Organisationseinheiten der Verwaltung im Zuge der Einbindung in datenschutzrelevante Vorgänge, regelmäßige Gespräche mit der Behördenleitung (unmittelbaren Unterstellung, Berichtswesen) sowie insbesondere regelmäßige Kontakte mit der IT und der Organisation zu führen und zu pflegen. Diese sind sicherlich häufig auch konflikträftig im Sinne der Stufe 4, insbesondere auch wenn es um die Überprüfung des in der Verwaltung betriebenen Datenschutzmanagements (durch anlasslose Besuche, Überprüfung konkreter Maßnahmen oder Feedback-Gespräche) geht. Bei gegensätzlichen Vorstellungen soll der/die Stelleninhaber/in unter schwieriger Argumentation die Gesprächspartner vom eigenen Standpunkt überzeugen. Somit ist hier die Stufe 4 anzusetzen.	55
<b>3. Grad der Selbstständigkeit - Ermessen – (10%)</b>		
4	Die Aufgabenerfüllung des/r Stelleninhabers/in ist nur teilweise durch Vorgaben bestimmt. Der Inhalt der Arbeit ist häufig nicht festgelegt. Es besteht oft Handlungsspielraum hinsichtlich der Wege zur Aufgabenerfüllung. Diese sind weitestgehend selbstständig und eigenverantwortlich zu finden, insbesondere sind auch eigene Konzeptionen im Bereich des Datenschutzes zu erarbeiten (z.B. Schulungskonzept, Rollen- und Berichtigungskonzept). Somit ist auch hier die Stufe 4 anzusetzen.	55



<b>4. Grad der Verantwortung (Ausführungsverantwortung) (25%)</b>		
4	Das Arbeitsverhalten im Einzelfall hat mittlere bis große Auswirkungen; es bezieht sich in der Regel auf einen kleineren Personenkreis, kann sich aber im Einzelfall - zum Beispiel bei der Begleitung der Einführung eines Softwareprodukts - auf die ganze Verwaltung auswirken. Es kommt mithin die Zwischenstufe 4 zum Tragen.	78
<b>(alternativ: Grad der Verantwortung (Stelle mit Leitungsverantwortung)</b>		
	(Unter Umständen relevant bei größeren Verwaltungen, in denen die Funktion des DSB nach der Personalbedarfsberechnung mehrere Stellen erfordert)	
<b>5. Grad der Vor- und Ausbildung (22%)</b>		
3	Die Wahrnehmung der Funktion des DSB erfordert für Kreisverwaltungen, kreisfreien und großen kreisangehörigen Städten mindestens die Laufbahnbefähigung für das dritte Einstiegsamt (geh. Dienst). Bei größeren Verwaltungen, in denen die Funktion des DSB nach der Personalbedarfsberechnung mehrere Stellen erfordert, kann mit entsprechender Leitungsverantwortung des DSB auch eine Eingruppierung im vierten Einstiegsamt (höherer Dienst) angemessen sein.	134
<b>6. Grad der Erfahrung (8%)</b>		
1	Der/Die DSB sollte mit der Organisation und den Verwaltungsabläufen einer öffentlichen Verwaltung in den Grundzügen vertraut sein. Zusätzliche Kenntnisse und Fertigkeiten auf einer anderen Stelle sollten daher vorhanden sein.	8
<b>Gesamtsumme</b>		<b>455</b>
<b>Besoldungsgruppe</b>		<b>A11</b>

Die Bewertung der Stelle ergibt eine Gesamtpunktzahl von 455 Punkten. Dies entspricht für dieses Beispiel gemäß der Dienstpostentabelle der Besoldungsgruppe A 11.



## **Anlage 2**

### **Aufgaben des behördlichen Datenschutzbeauftragten in der rheinland-pfälzischen Kommunalverwaltung**

Orientierungshilfe des LfDI Rheinland-Pfalz (Stand: 20. Juni 2017)

---

#### **1. Allgemeines**

Rechtsgrundlage für die Aufgaben des behördlichen Datenschutzbeauftragten in den rheinland-pfälzischen Kommunalverwaltungen ist § 11 Abs. 3 Landesdatenschutzgesetz (LDSG). Hiernach hat der behördliche Datenschutzbeauftragte die Aufgabe, die öffentlichen Stellen bei der Ausführung des Landesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen.

Die Regelung beschreibt anschließend in § 11 Abs. 3 Satz 2 LDSG konkrete Tätigkeitsfelder, die den pauschalen gesetzlichen Unterstützungsauftrag konkretisieren und deshalb zwingend von den behördlichen Datenschutzbeauftragten im Rahmen ihrer Funktion wahrzunehmen sind. Dieser Aufgabenkatalog ist jedoch nicht abschließend. Er benennt lediglich die aus Sicht des Gesetzgebers besonders wichtigen Tätigkeiten eines behördlichen Datenschutzbeauftragten (so auch Hartig/Klink/Eiermann, Kommentar zum LDSG Rheinland-Pfalz, Nr. 4.2 zu § 11). Darüber hinaus können durchaus weitere Aufgaben und Tätigkeiten von dem Handlungsauftrag des behördlichen Datenschutzbeauftragten umfasst sein.

Die nachfolgenden Aufgabenbeschreibungen sollen den Leitungen der rheinland-pfälzischen Kommunalverwaltungen sowie den dort tätigen Beschäftigten, insbesondere aber den dort bestellten Datenschutzbeauftragten eine Hilfestellung geben bei der Ausübung dieser Funktion. Im Vordergrund steht dabei die Nutzbarkeit der Orientierungshilfe für die Praxis. Es wurde deshalb nicht die in § 11 Abs. 3 LDSG enthaltene Struktur und Begrifflichkeit übernommen, sondern die daraus resultierenden konkreten Arbeitsaufträge praxisnah formuliert.

Das Papier wurde im Projekt „Datenschutz-update in der Kommunalverwaltung“, das der LfDI Rheinland-Pfalz gemeinsam mit vier rheinland-pfälzischen Kommunen zwischen November 2016 und Juni 2017 durchgeführt hat, erarbeitet. Dem Ministerium des Innern und für Sport, dem Landesrechnungshof sowie den kommunalen Spitzenverbänden wurde die Orientierungshilfe mit der Bitte zugeleitet, diese inhaltlich mitzutragen.

---



## 2. Aufgaben eines kommunalen Datenschutzbeauftragten

- ◆ Unterrichtung und Beratung der Verwaltungsspitze in datenschutzrechtlichen Angelegenheiten

Nach der gesetzlichen Konstruktion, die sich auch in der ab Mai 2018 wirksamen Europäischen Datenschutz-Grundverordnung fortsetzen wird, arbeitet der behördliche Datenschutzbeauftragte unmittelbar mit der Behördenleitung zusammen (§ 11 Abs. 1 Satz 2 LDSG). Hintergrund hierfür ist die der Leitung zukommende Verantwortlichkeit für die Einhaltung des Datenschutzes durch die von ihr geführte Stelle (§ 10 Abs. 1 LDSG). Dementsprechend ist es geboten, dass der behördliche Datenschutzbeauftragte in regelmäßigen Abständen den Leiter der Kommunalverwaltung über seine Tätigkeit unterrichtet und bei Bedarf in datenschutzrechtlichen Angelegenheiten berät.

### Praxistipp:

Vereinbarung eines jährlichen Jour Fixe mit Besprechung des von dem Datenschutzbeauftragten zu diesem Zweck erstellten Tätigkeitsberichts

- ◆ Beratung aller Organisationseinheiten der Verwaltung und der dort tätigen Beschäftigten, soweit diese personenbezogene Daten verarbeiten

Schwerpunkt der Aufgaben, die dem behördlichen Datenschutzbeauftragten gesetzlich zugewiesen sind, ist die rechtzeitige Beratung der Mitarbeiter zu allen Angelegenheiten mit Datenschutzbezug (§ 11 Abs. 3 Satz 2 Nr. 1 und Nr. 5 LDSG). Dabei soll der Datenschutzbeauftragte im Ergebnis auf die Einhaltung der Datenschutzvorschriften hinwirken. Dies setzt eine frühzeitige Einbindung durch die einzelnen Organisationseinheiten voraus. Der Datenschutzbeauftragte muss daher verwaltungsintern bekannt und erreichbar sein. Zudem sollte er – möglicherweise gemeinsam mit der Verwaltungsspitze – seine Beteiligung an datenschutzrelevanten Arbeitsabläufen sicherstellen. Möglicherweise ist es dabei hilfreich klarzustellen, in welchen Fällen ein Datenschutzbezug besteht.

### Praxistipp:

Hausinterne Kommunikation der Aufgaben des behördlichen Datenschutzbeauftragten sowie die Notwendigkeit seiner Beteiligung in datenschutzrelevanten Angelegenheiten; dabei Nutzung der Möglichkeiten der elektronischen Kommunikation



- ◆ Regelmäßige Abstimmung mit den Bereichen „Informationstechnik/EDV“ und „Organisation“

Der Einsatz elektronischer Datenverarbeitungsverfahren sowie die Durchführung technischer-organisatorischer Maßnahmen zum Datenschutz haben für die Tätigkeit des behördlichen Datenschutzbeauftragten eine zentrale Bedeutung (§ 11 Abs. 3 Satz 2 Nr. 1 und Nr. 3 LDSG). Denn damit werden die Rahmenbedingungen der Verarbeitung personenbezogener Daten durch die einzelnen Organisationseinheiten der Verwaltung wesentlich gestaltet. Aufgrund dessen sollte sich der Datenschutzbeauftragte regelmäßig und auch anlassunabhängig mit den Bereichen „Informationstechnik/EDV“ und „Organisation“, bei denen die o.g. Inhalte betreut werden, austauschen und soweit möglich eine gemeinsame Vorgehensweise abstimmen. Dabei sollte insbesondere eine frühzeitige Einbindung des Datenschutzbeauftragten in datenschutzrelevante Angelegenheiten vereinbart werden.

Praxistipp:

Vereinbarung von regelmäßigen Gesprächsmöglichkeiten

- ◆ Durchführung von Vorabkontrollen und Führen des Verzeichnisses

Derzeit hat der behördliche Datenschutzbeauftragte noch Vorabkontrollen durchzuführen (§ 11 Abs. 3 Satz 2 Nr. 3 LDSG) und das Verzeichnisses zu führen (§ 11 Abs. 3 Satz 2 Nr. 4 LDSG). Dies wird sich mittelfristig nach Wirksamwerden der Europäischen Datenschutz-Grundverordnung im Mai 2018 verändern. Beide Aufgaben erfordern eine enge und rechtzeitige Zusammenarbeit mit den Bereichen „Informationstechnik/EDV“ und „Organisation“. Da die Verarbeitung besonderer personenbezogener Daten wie z.B. Gesundheitsdaten der Hauptanknüpfungsfälle für die Notwendigkeit einer Vorabkontrolle nach § 9 Abs. 5 LDSG ist, sollte sich der behördliche Datenschutzbeauftragte gemeinsam mit dem Bereich „Organisation“ einen Überblick über die Organisationseinheiten verschaffen, in denen diese Daten verarbeitet werden. Im Hinblick auf das Verzeichnisses ist es hinnehmbar, wenn federführend der Bereich „Informationstechnik/EDV“ tätig wird und der Datenschutzbeauftragte einen ungehinderten Zugang zu dem aktuellen Verzeichnisses erhält.

Praxistipp:

Festlegung der Vorgehensweise mit den Bereichen „Informationstechnik/EDV“ und „Organisation“ und verwaltungsinterne Bekanntmachung



- ◆ Bearbeitung von Eingaben und Anfragen

Betroffene können sich jederzeit an den behördlichen Datenschutzbeauftragten wenden (§ 11 Abs. 5 Satz 3 LDSG). Der Datenschutzbeauftragte sollte sich daher auf den Umgang mit derartigen Eingaben einstellen und insbesondere Rahmenbedingungen für die Bearbeitung formulieren (z.B. Erreichbarkeit, Gewährleistung der Verschwiegenheitspflicht (§ 11 Abs. 2 LDSG), Vorgangsbearbeitung, Dokumentation).

Praxistipp:

Abstimmung der Vorgehensweise mit Behördenleitung und Bereich „Organisation“.

- ◆ Verwaltungsinterne Bereitstellung von Informationen und Empfehlungen zum Datenschutz

Der Datenschutzbeauftragte hat die Kommunalverwaltung bei der Beachtung der datenschutzrechtlichen Vorgaben zu unterstützen. Hierzu gehört neben einer arbeitsintensiveren fallbezogenen Beratung insbesondere die Bereitstellung geeigneter Hinweise, Empfehlungen und Informationen (§ 11 Abs. 3 Satz 2 Nr. 5 LDSG). Darüber hinaus obliegt es dem Datenschutzbeauftragten, die bei der Verarbeitung personenbezogener Daten in der Verwaltung tätigen Personen mit den Vorgaben des Datenschutzes vertraut zu machen (§ 11 Abs. 3 Satz 2 Nr. 2 LDSG). Beide Aufgaben können zumindest in einem ersten Schritt durch die Bereitstellung bedarfsgerechter und leicht zugänglicher Informationen erfüllt werden. Wichtig ist in diesem Zusammenhang die Ermittlung der bestehenden Informationsbedarfe sowie die Einrichtung einer von allen Beteiligten gut nutzbaren Informations- und Kommunikationsform. Soweit über die Bereitstellung von Informationen hinaus konkreter Fortbildungs- und Schulungsbedarf bei den Beschäftigten der Verwaltung besteht, sollte ausgelotet werden, in welcher Form (intern/extern) diesem entsprochen werden kann.

Praxistipp:

Aufbau eines Bereichs zum Datenschutz im Intranet; dabei Bereitstellung von Informationen und Kommunikation mit den Beschäftigten





- ◆ Erfolgskontrolle und Evaluierung

Die Bestellung eines behördlichen Datenschutzbeauftragten dient nach der Vorstellung des Gesetzgebers einer besseren Beachtung der datenschutzrechtlichen Vorgaben durch die jeweilige Verwaltung (§ 11 Abs. 3 Satz 1 LDSG). Angesichts der Bedeutung des zugrunde liegenden Grundrechts auf informationelle Selbstbestimmung und des darauf basierenden in § 11 Abs. 3 LDSG enthaltenen Arbeitsauftrages für die Datenschutzbeauftragten ist es geboten, deren konkrete Tätigkeit einer permanenten Erfolgskontrolle und Evaluierung zu unterziehen, um bestehendes Verbesserungspotential zu nutzen. Der Datenschutzbeauftragte sollte deshalb auf der Basis einer Dokumentation seiner Beratungstätigkeit und der darin vereinbarten Ergebnisse die Umsetzung der datenschutzrechtlichen Vorgaben in der Verwaltung durch geeignete Maßnahmen überprüfen. Zudem sollte er – möglicherweise gemeinsam mit der Verwaltungsspitze – bestehendes Verbesserungspotential bei der Erfüllung seiner Aufgaben identifizieren.

Praxistipp:

Festlegung konkreter Schritte, mit denen festgestellt werden kann, ob und ggf. in welchem Maße die Verwaltung bei der Verarbeitung personenbezogener Daten datenschutzrechtliche Vorgaben beachtet; ggf. Feststellung der Hinderungsgründe

- ◆ Eigene fachliche Fort- und Weiterbildung

Die Erfüllung der Aufgaben des behördlichen Datenschutzbeauftragten hängt neben der zur Verfügung zu stellenden ausreichenden Personalressourcen insbesondere von der vorhandenen Fachkunde des Stelleninhabers ab. Aus diesem Grund müssen die erforderlichen Fort- und Weiterbildungen gewährt werden (§ 11 Abs. 5 Satz 2 LDSG).

Praxistipp:

Jährliche Klärung des Fortbildungsbedarfs mit der Verwaltungsspitze



### **3. Ausblick**

Mit dem Wirksamwerden der Europäischen Datenschutz-Grundverordnung am 25. Mai 2018 werden sich auch die Aufgaben der behördlichen Datenschutzbeauftragten in den rheinland-pfälzischen Kommunalverwaltungen gravierend verändern. Anders als bislang werden künftig zeitaufwändige risikoorientierte Management- und Compliance-Aufgaben den Alltag des Datenschutzbeauftragten wesentlich prägen. Datenschutz wird nach dem Verständnis des europäischen Verordnungsgebers endgültig zur Chefsache. Der damit einhergehende Bedeutungsgewinn dieser Funktion wird die verwaltungsinternen Arbeitsprozesse nicht unberührt lassen. Dem vielfältigen Aufgabenkatalog des internen Datenschutzbeauftragten auf der einen Seite stehen umfassende Unterstützungspflichten der verantwortlichen Stelle auf der anderen Seite gegenüber. Besonders hervorzuheben sind in diesem Zusammenhang die Pflicht zur Bereitstellung ausreichender Ressourcen sowie die Sicherstellung eines unmittelbaren Austauschs mit den Verwaltungsleitungen als höchster Managementebene.

Der LfDI Rheinland-Pfalz wird rechtzeitig vor ihrem Wirksamwerden eine an die Vorgaben der Datenschutz-Grundverordnung angepasste Version dieser Orientierungshilfe veröffentlichen.



### Anlage 3

#### Kooperationsmöglichkeiten von Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen bei der Ausübung der Funktion des Datenschutzbeauftragten (Stand: 20. Juni 2017)

---

§ 11 Abs. 1 S. 5 LDSG lässt die Bestellung eines externen behördlichen Datenschutzbeauftragten zu. Eine Option ist dabei die Benennung von Bediensteten einer öffentlichen Stelle für mehrere andere öffentliche Stellen.

Aus Sicht des LfDI kann eine Kooperation von mehreren Verbandsgemeinde- und verbandsfreien Gemeindeverwaltungen sinnvoll sein, wenn es für einzelne Verwaltungen aufgrund ihrer Struktur aus wirtschaftlichen oder personellen Gründen nicht möglich ist, die Funktion angemessen aus eigenen Ressourcen zu besetzen. Gleiches gilt, wenn die nötige Fachkunde zur Ausübung der Funktion des kommunalen Datenschutzbeauftragten in den Verwaltungen nicht dauerhaft vorgehalten werden kann. Allerdings darf mit einer derartigen Kooperation keine Verschlechterung des Datenschutzniveaus einhergehen.

Der Bayerische Landesbeauftragte für den Datenschutz hat in seinem 27. Tätigkeitsbericht (Berichtszeitraum 2015/2016) zwei solcher in Frage kommender Modelle aus der kommunalen Praxis in **Bayern** vorgestellt (vgl. Nr. 6.4 des 27. Tätigkeitsberichtes, verfügbar im Internet unter [https://www.datenschutz-bayern.de/inhalte/taetig\\_t.htm](https://www.datenschutz-bayern.de/inhalte/taetig_t.htm)). Insbesondere die gemeinsame Bestellung eines Datenschutzbeauftragten mit einem „Vor-Ort-Vertreter“ bei jeder der beteiligten öffentlichen Stellen kann geeignet sein, um die o.g. Anforderungen vor Ort gesetzeskonform zu erfüllen. Darüber hinaus berichtet die einschlägige Fachliteratur (Beitrag in Kommune21, Ausgabe 3/2017; [www.kommune21.de](http://www.kommune21.de)) über eine Kooperation in Sachen Datenschutz aus dem **Saarland**. Hiernach haben zehn saarländische Kommunen im Rahmen einer interkommunalen Zusammenarbeit ihre Anstrengungen zur Gewährleistung des Datenschutzes gebündelt. Mit Unterstützung von Experten aus der IT-Branche seien insbesondere alle in den Kommunen zur Datenverarbeitung eingesetzten Verfahren mittels standardisierter Verzeichnisse rechtskonform, wirtschaftlich und effektiv dokumentiert worden. Fachverfahren, die von mehreren Kommunen eingesetzt werden, müssten nur einmal für das Verzeichnisse beschrieben werden und könnten von den Kommunen übernommen werden. Zudem sei geplant, ein datenschutzkonformes Management- und Steuerungssystem, beginnend bei der Zutrittsberechtigung für bestimmte Räume oder der Zugriffsberechtigung auf Server, aufzubauen.



Sofern mehrere der o.g. Kommunalverwaltungen eine Kooperation mit anderen Verwaltungen zur Ausübung der Funktion des Datenschutzbeauftragten in Betracht ziehen sollten, ist der LfDI gerne bereit, die beteiligten Verwaltungen zu beraten.



## Anlage 4

### Anforderungsprofil für kommunale Datenschutzbeauftragte (Stand: 20. Juni 2017)

---

Für die Erfüllung der Aufgaben der bzw. des kommunalen Datenschutzbeauftragten sind neben rechtlichen Kenntnissen auch Grundkenntnisse in den Bereichen Informations- und Telekommunikationstechnik sowie Verwaltungsorganisation erforderlich. Diese müssen nicht zu administrativen Tätigkeiten oder dem Erstellen von Organisationsuntersuchungen befähigen, sondern sollen dem Verständnis von Verwaltungsvorgängen, deren datenschutzrechtlichen und technisch-organisatorischen Bewertung sowie der Einordnung von Begrifflichkeiten dienen. Für die praktische Arbeit ist insbesondere eine enge Zusammenarbeit mit der IT-Administration und der Organisationsstelle geboten. Kommunale Datenschutzbeauftragte sollten in der Lage sein, datenschutzrelevante Problemstellungen in Verwaltungsvorgängen und IT-Verfahren zu erkennen und anzusprechen.

#### Rechtliche Grundlagen

Kenntnisse in folgenden Bereichen sollten bestehen oder zeitnah erworben werden:

- Erfahrungen und Grundkenntnisse im Verwaltungsrecht
- Vertiefte Kenntnisse im allgemeinen Datenschutzrecht (LDiSG) und Grundkenntnisse in dessen verfassungsrechtlichen Vorgaben
- Überblick über die Aufgaben der eigenen Verwaltung und der zugrunde liegenden Rechtsgrundlagen
- Grundkenntnisse im besonderen Datenschutzrecht (Fachgesetze)
- Fähigkeit, sich in die europarechtlichen Vorgaben des Datenschutzrechts einzuarbeiten

#### Informationstechnik

Kenntnisse in folgenden Bereichen sollten bestehen oder zeitnah erworben werden:

- Grundkenntnisse über die Funktionalität von IT-Systemen
  - Unterschiede zwischen System- und Anwendungssoftware
  - Grundlagen Systemberechtigungen, administrative und sonstige Benutzerrollen, „Revisorenrolle“ z.B. für den DSB
  - Unterschiede zwischen Client und Server
  - Protokollierung von System- und Datenbankzugriffen
  - Grundlagen Netzwerke; Einordnung LAN, WAN; Netzwerksegmentierung, -sicherheit
  - Grundlagen Verschlüsselung, elektronische Signatur
-



### Verwaltungsorganisation

Kenntnisse in folgenden Bereichen sollten bestehen oder zeitnah erworben werden:

- Verwaltungsaufbau sowohl lokal als auch im Verhältnis zu Landes- und Bundesbehörden (Hierarchieebenen, Weisungs- und Zeichnungsbefugnisse); vgl. Rollen- und Berechtigungskonzepte;
- Ablauforganisation insb. bei Beschaffung von Hard- und Softwarekomponenten; Einbindung bereits in der Planungsphase zur Definition von Berechtigungskonzepten
- Kenntnisse in organisationsübergreifende Abläufe, sowohl innerhalb der lokalen Verwaltung (z.B. Schnittstellen zwischen Fachabteilung und Kasse) als auch zu anderen Behörden (z.B. Bußgeldstelle zum KBA wg. Halterermittlungen)
- Kenntnisse über regelmäßig stattfindende Datenübermittlungen zwischen unterschiedlichen Verwaltungseinheiten und zu externen Stellen



## Anlage 5

### „Starterkit“ für neue Datenschutzbeauftragte (Stand: 20. Juni 2017)

---

Der LfDI bietet den Datenschutzbeauftragten zahlreiche Informationen und praktische Handreichungen für die tägliche Arbeit. Um den Zugang zu diesen Informationen für neu in die Funktion gekommene Datenschutzbeauftragte zu erleichtern, hat der LfDI die wichtigsten Hinweise in einem „Starterkit“ zusammengestellt. Sobald sich die oder der neue Datenschutzbeauftragte in der Geschäftsstelle des LfDI meldet, wird ihm das „Starterkit“ – in elektronischer Form – übersandt. Das „Starterkit“ umfasst regelmäßig folgende Materialien:

- ❖ Begrüßungsschreiben des LfDI (persönlich) mit kurzen Hinweisen auf verfügbare Materialien und Ansprechpartner sowie Hinweis auf Aufnahme in Verteiler des LfDI
- Orientierungshilfe zu den Aufgaben der behördlichen Datenschutzbeauftragten in der Kommunalverwaltung
- Best Practice-Empfehlungen einschließlich weiterführender Dokumente zur Stellenbemessung und Stellenbewertung und zum Anforderungsprofil kommunaler Datenschutzbeauftragter; bei VGV und verbandsfreien Gemeindeverwaltungen zusätzlich Papier zu Kooperationsmöglichkeiten bei der Ausübung der Funktion des Datenschutzbeauftragten
- Anmeldungen zum Datenschutzregister: Hinweise + Formular im Internet
- Hinweise zum Verfahrensverzeichnis (auch Formular)
- Übersicht über die bereits beim LfDI angemeldeten Verfahren
- Regelungsbeispiele für eine Dienstanweisung nach § 9 LDSG
- Verpflichtung auf das Datengeheimnis
- Checkliste Vorabkontrolle nach § 9 Abs. 5 LDSG
- Hinweise zur Meldung einer Datenpanne
- Verhaltensempfehlungen zu sozialen Netzwerken
- Musterdienstanweisung Videoüberwachung
- Hinweise zur Datenverarbeitung im Auftrag



- Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
  
- Hinweis auf Internetangebot des LfDI
- Informationen zum Forum und ggf. Zugangsdaten
- Informationen zur Fallbörse im Kommunalbereich
- Hinweis auf Netzwerktreffen
- Hinweis auf Newsletter
  
- Literaturliste
- Prüfungsschema für datenschutzrechtliche Fallgestaltungen
- Hinweise auf Fortbildungsmöglichkeiten (extern)
- Materialien für interne Fortbildungsmöglichkeiten