Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Behördliche Datenschutzbeauftragte

Aufgabe und Funktion

Vorwort

Mit der stetigen Zunahme von Datenverarbeitung auf fast jedem Behördenarbeitsplatz sind die Anforderungen an die Datenschutzkompetenz in den Behörden gewachsen. Bei neuen, oft hoch komplexen und vernetzten Verfahren ist Fachkompetenz gefragt, um den datenschutzrechtlichen Anforderungen im Interesse der Bürgerinnen und Bürger gerecht zu werden. Hier haben sich behördliche Datenschutzbeauftragte vor Ort in den Behörden verdient gemacht und als unentbehrliche Institution erwiesen.

Seit dem Jahr 2000 sind behördliche Datenschutzbeauftragte und deren Stellvertretungen in den öffentlichen Stellen in NRW verpflichtend zu bestellen. In dieser Broschüre sollen die wichtigsten Fragestellungen rund um die Funktion der Datenschutzbeauftragten erläutert werden. Dies soll Behördenleitungen und behördlichen Datenschutzbeauftragten eine Hilfestellung sein und möglichst eine gute Zusammenarbeit bei Datenschutzthemen in den öffentlichen Stellen des Landes fördern. In diesem Sinne wünsche ich mir, dass Datenschutz in NRW ein Anliegen ist, an dem nicht nur ich mit meiner Behörde, sondern alle öffentlichen Stellen ein gemeinsames Interesse haben und konstruktiv zusammenarbeiten.

Ulrich Lepper
Landesbeauftragter für Datenschutz und Informationsfreiheit

Inhaltsverzeichnis

1. Datenschutz in öffentlichen Stellen: Verantwortung, Kontrolle, Unterstützung

Ein hohes Datenschutzniveau ist Zeichen einer bürgerfreundlichen und modernen Verwaltung. Die Bürgerinnen und Bürger haben die berechtigte Erwartung, dass die Behörden im Land bei der täglichen Verwaltungsarbeit ihre Persönlichkeitsrechte und damit auch ihr Recht auf informationelle Selbstbestimmung achten.

Die Verantwortung für den Datenschutz in einer öffentlichen Stelle trägt die Leitung der Stelle. Alle Beschäftigten sind verantwortlich für den Datenschutz in ihrem eigenen Zuständigkeitsbereich. Die Leitung stellt sicher, dass die datenschutzrechtlichen Bestimmungen in der öffentlichen Stelle eingehalten werden.

Die oder der Datenschutzbeauftragte unterstützt und kontrolliert die öffentliche Stelle dabei. Datenschutzbeauftragte entscheiden dagegen nicht selbst, wie bestimmte Verfahren durchzuführen sind, und können ihre Forderungen nicht formell durchsetzen. Vielmehr helfen sie bei der Selbstkontrolle. Sie können konzentriertes Fachwissen im Querschnittsgebiet Datenschutz anbieten, Ansprechpartner für die Leitung und die Beschäftigten sein und als "Motor" den Datenschutzbereich voran bringen. Die Bestellung von Datenschutzbeauftragten ist deshalb nicht nur eine Pflicht, sondern vor allem auch eine Chance.

2. Bestellung von Datenschutzbeauftragten

a. Welche öffentlichen Stellen müssen Datenschutzbeauftragte bestellen?

Alle öffentlichen Stellen, die personenbezogene Daten verarbeiten, haben Datenschutzbeauftragte und deren Vertretungen zu bestellen (§ 32a Abs. 1 Satz 1 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)).

Öffentliche Stellen im Sinn des DSG NRW sind

- Behörden, Einrichtungen und sonstige öffentliche Stellen des Landes,
- die Gemeinden und Gemeindeverbände,

- die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und
- deren Vereinigungen (§ 2 Abs. 1 Satz 1 DSG NRW).

Die Pflicht zur Bestellung gilt auch für die folgenden öffentlichen Wirtschaftseinrichtungen, soweit sie personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten (§ 2 Abs. 2 Satz 1 DSG NRW):

- Eigenbetriebe (wirtschaftliche Unternehmen der Gemeinden und Gemeindeverbände ohne eigene Rechtspersönlichkeit)
- Eigenbetriebsähnliche Einrichtungen (öffentliche Einrichtungen, die entsprechend den Vorschriften über Eigenbetriebe geführt werden)
- Juristische Personen des öffentlichen Rechts, die der Aufsicht des Landes unterstehen und am Wettbewerb teilnehmen

Die Pflicht zur Bestellung gilt zudem für die folgenden besonderen Organisationsformen:

- Anstalten öffentlichen Rechts (bei kommunalen Anstalten entsprechend § 2 Abs. 2 Satz 1 DSG NRW)
- Privatrechtliche Vereinigungen, z. B. AGs oder GmbHs, soweit sie
  - Aufgaben der öffentlichen Verwaltung erfüllen, das heißt Aufgaben, die der öffentlichen Verwaltung durch Gesetz oder kommunale Satzung zugewiesen sind,
  - öffentliche Stellen als Beteiligte haben (z. B. Gesellschafter oder Mitglieder) und
  - durch öffentliche Stellen beherrscht werden ("deren Vereinigungen" i.S.d. § 2 Abs. 1 Satz 1 DSG NRW)
- Öffentliche und private Träger von Krankenhäusern und Einrichtungen, soweit für die Datenverarbeitung das Gesundheitsdatenschutzgesetz Nordrhein-Westfalen gilt (§§ 2, 3 und 12 Abs. 1 GDSG NW)

Für Schulen in kommunaler und staatlicher Trägerschaft bestellt das Schulamt eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. (§ 1 Abs. 6 Satz 3 Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer)

b. Können externe Datenschutzbeauftragte bestellt werden?

Datenschutzbeauftragte sind grundsätzlich intern zu bestellen (§ 32a Abs. 1 Satz 1). "Intern" bedeutet, dass die bestellte Person bei der verantwortlichen Stelle beschäftigt ist.

Als einzige Ausnahme lässt das DSG NRW zu, dass mehrere öffentliche Stellen gemeinsam eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten bestellen können (§ 32a Abs. 1 Satz 3 DSG NRW, zu den besonderen Voraussetzungen siehe unter d).

c. Wer kann Datenschutzbeauftragte oder Datenschutzbeauftragter werden?

Datenschutzbeauftragte müssen die erforderliche Sachkenntnis und Zuverlässigkeit besitzen (§ 32a Abs. 1 Satz 2 DSG NRW) und dürfen keine andere Aufgabe wahrnehmen, die zu einer Interessenkollision führen könnte (§ 32a Abs. 2 Satz 3 DSG NRW):

i. Sachkenntnis

Datenschutzbeauftragte müssen Kenntnisse in den drei folgenden Wissensfeldern haben oder erwerben:

- o <u>Datenschutzrechtliche Grundlagen:</u>

Zu den rechtlichen Grundlagen gehören das Recht auf informationelle Selbstbestimmung, die weiteren Grundrechte mit Datenschutzbezug, die allgemeinen Datenschutzgesetze (DSG NRW und – soweit anwendbar – das Bundesdatenschutzgesetz) sowie besondere Datenschutzregelungen, die für den jeweiligen Zuständigkeitsbereich einschlägig sind. Gute Kenntnisse und Fähigkeiten in der Rechtsanwendung sind erforderlich, allgemeine Rechtskenntnisse wünschenswert.

- o <u>Informationstechnische Grundlagen:</u>

Datenschutzbeauftragte müssen Aufbau, Funktionsweise und Anforderungen von Datenverarbeitungssystemen in Grundzügen begreifen, um Verfahren bewerten und sinnvolle Sicherungs- und Schutzmaßnahmen vorschlagen zu können. Grund-

kenntnisse der Datenverarbeitung und ein technisches Grundverständnis für IT-Fragen sind deshalb erforderlich.

- Organisation der öffentlichen Stelle:

Nur wenn den Datenschutzbeauftragten die Aufgaben, die Arbeitsweise und die Abläufe in ihren öffentlichen Stellen vertraut sind, können sie ihre Aufgaben effizient wahrnehmen.

Nur wenige Personen werden alle Voraussetzungen von vorne herein erfüllen. Die Kenntnisse und Fähigkeiten müssen zudem mit den jeweiligen Aufgaben weiterentwickelt werden. Dazu bietet sich die Teilnahme an geeigneten Fort- und Weiterbildungsveranstaltungen an. Anbieter sind zum Beispiel:

- Fortbildungsakademie des Ministeriums für Inneres und Kommunales des Landes Nordrhein-Westfalen
- Landesbetrieb Information und Technik NRW
- Private Anbieter für besondere Tätigkeitsbereiche (Übersicht zum Beispiel unter www.datenschutz.de)

Wie umfangreich die Kenntnisse sein müssen, lässt sich abstrakt nicht festlegen, da dies vom Bedarf der jeweiligen Stelle abhängt. Die Menge und die Art der personenbezogenen Daten können sich ebenso unterscheiden wie Anzahl und Komplexität von Datenverarbeitungsverfahren in den verschiedenen öffentlichen Stellen.

Reichen die Kenntnisse im einzelnen Fall nicht aus, können sich Datenschutzbeauftragte auch von sachkundigen Personen oder Stellen beraten lassen.

ii. Zuverlässigkeit

Wer selbst gegen Datenschutzvorschriften verstoßen hat, ist nicht zuverlässig. Erforderlich ist aber auch, dass Datenschutzbeauftragte geeignet und bereit sind, die Konflikte zu bewältigen, die diese unabhängige Funktion mit sich bringen kann.

iii. Vereinbarkeit mit anderen Aufgaben (keine Interessenkollision)

Datenschutzbeauftragte dürfen auch andere Aufgaben wahrnehmen. Sie dürfen während ihrer Tätigkeit aber mit keiner Aufgabe betraut sein, deren Wahrnehmung zu einer Interes-

senkollision führen könnte (§ 32a Abs. 2 Satz 3 DSG NRW). Datenschutzbeauftragte dürfen sich also nicht selbst kontrollieren.

Damit ist nicht jede weitere Aufgabe ausgeschlossen, die mit der Verarbeitung von personenbezogenen Daten verbunden ist. Die Funktion von Datenschutzbeauftragten ist aber unvereinbar mit Tätigkeiten in Arbeitsbereichen, in denen eine besonders umfangreiche Verarbeitung von personenbezogenen Daten oder eine Verarbeitung von besonders sensitiven personenbezogenen Daten stattfindet. Dazu zählen besonders die folgenden Bereiche und Aufgaben:

- Personal
- Informationstechnik
- Geheimschutzbeauftragte
- Gleichstellungsbeauftragte
- IT-Sicherheitsbeauftragte

  Die Funktionen können aber dann vereinbar sein, wenn die Kompetenzen von IT-Sicherheitsbeauftragten nicht über die von Datenschutzbeauftragten hinausgehen, also IT-Sicherheitsbeauftragte nur Kontroll- und Beratungsaufgaben haben, aber keine verantwortlichen Entscheidungen treffen.

- Personalratsvorsitzende und Vertretung

  Hier sind das Verbot einer Interessenkollision und das personalvertretungsrechtliche Verbot einer Benachteiligung von Personalratsmitgliedern miteinander abzuwägen. Die Abwägung ergibt, dass die Funktion als "einfaches" Personalratsmitglied der Funktion von Datenschutzbeauftragten nicht entgegensteht. Mit dem Vorsitz und der Vertretung sind jedoch die Führung der laufenden Geschäfte und auch die Verantwortung für den Datenschutz im Personalrat verbunden, so dass insoweit das Verbot der Interessenkollision überwiegt.

Die Gefahr einer Interessenkollision kann dadurch entstehen, dass Datenschutzbeauftragte in den genannten Bereichen personenbezogene Daten selbst verarbeiten oder sonstige Ent-

scheidungen über Datenverarbeitungsverfahren – zum Beispiel in Führungsverantwortung – treffen würden.

d. Können mehrere öffentliche Stellen gemeinsam eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten bestellen?

Mehrere öffentliche Stellen können gemeinsam eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung der Aufgabe nicht beeinträchtigt wird (§ 32a Abs. 1 Satz 3 DSG NRW). Die oder der Datenschutzbeauftragte ist dann bei einer der Stellen angesiedelt.

Die folgenden Indizien sprechen gegen eine gemeinsame Bestellung, weil sonst voraussichtlich die Erfüllung der Aufgabe beeinträchtigt wird:

- o Die beteiligten Stellen sind zu groß:
  Je größer eine Stelle ist, desto aufwändiger ist regelmäßig die Aufgabe von Datenschutzbeauftragten. Für die Beurteilung spielen auch Art und Menge der verarbeiteten Daten und die Komplexität der Datenverarbeitung eine Rolle. Die Regelung wurde ursprünglich geschaffen, um kleinen Stellen die Bestellung zu ermöglichen, die sonst Schwierigkeiten hätten, geeignete Personen zu finden (Gesetzesbegründung zu § 32a Absatz 1 Satz 3 DSG NRW, Landtagsdrucksache 12/4476, S. 74).

- o Die beteiligten Stellen sind zu unterschiedlich:
  Je unterschiedlicher die Aufgaben der Stellen und demzufolge auch Zweck und Inhalt der Datenverarbeitung sind, desto schwieriger sind Kontrolle und Beratung für mehrere Stellen gleichzeitig. Die Regelung wurde ursprünglich mit dem Ziel geschaffen, dass gemeinsame Datenschutzbeauftragte bei einer gleich geordneten oder übergeordneten Stelle bestellt werden (Gesetzesbegründung zu § 32a Absatz 1 Satz 3 DSG NRW, Landtagsdrucksache 12/4476, S. 74).

- o Die beteiligten Stellen liegen zu weit auseinander:
  Je weiter die Stellen auseinander liegen, desto aufwändiger ist es für Datenschutzbeauftragte, selbst Ansprechpartnerinnen und Ansprechpartner vor Ort zu sein.

- o Die beteiligten Stellen sind zu viele:
  Je mehr Stellen gleichzeitig beraten und kontrolliert werden sollen, desto aufwändiger ist die Aufgabe.

Bei vielen oder komplexen Verfahren, einer großen Menge von Daten, weiteren Entfernungen oder mehreren beteiligten Stellen, kann es nötig sein, dass in jeder Stelle mindestens eine Ansprechpartnerin oder ein Ansprechpartner für Datenschutzfragen benannt wird, damit die Aufgabe nicht beeinträchtigt wird. Dies kann Beeinträchtigungen bis zu einem bestimmten Grad vermeiden, ist dann aber auch erforderlich. Solche Ansprechpartnerinnen und Ansprechpartner sollten eine Grundqualifikation in Datenschutzfragen haben, die nötige Arbeitszeit aufbringen können und auf die Verschwiegenheit im Sinne des § 32a Abs. 4 Satz 2 DSG NRW verpflichtet werden.

Wenn Datenschutzbeauftragte gemeinsam bestellt werden, müssen sie auch über die ausreichende Arbeitszeit verfügen, die für ihren dann größeren Aufgabenbereich nötig ist.

e. Können mehrere Datenschutzbeauftragte für eine Stelle bestellt werden?

Es können auch mehrere Datenschutzbeauftragte und Vertretungen bestellt werden (§ 32a Abs. 1 Satz 4 DSG NRW). Dies kann zum Beispiel sinnvoll sein, wenn dadurch Interessenkollisionen vermieden werden: Dann werden Datenschutzbeauftragte mit der Einschränkung bestellt, dass sie nicht für den Bereich zuständig sind, in dem sie selbst Aufgaben wahrnehmen, die eine Interessenkollision begründen. Für diesen Bereich wird eine andere Datenschutzbeauftragte oder ein anderer Datenschutzbeauftragter bestellt. Beispielsweise könnte in einer Kommune ein Ausländeramtsleiter der Datenschutzbeauftragte für alle Bereiche außer dem Ausländeramt sein und die Sozialamtsleiterin die Datenschutzbeauftragte nur für das Ausländeramt sein.

Wenn mehrere Datenschutzbeauftragte bestellt werden, ist darauf zu achten, dass es keine Überschneidungen der Zuständigkeitsbereiche gibt, da sonst Unabhängigkeit und Beratungsfunktion gefährdet sein können, wenn mehrere Datenschutzbeauftragte zu einer Frage unterschiedliche Auffassungen vertreten.

In großen Stellen kann es erforderlich sein, den Datenschutzbeauftragten zur Unterstützung weitere Beschäftigte zuzuweisen.

f. Wie werden Datenschutzbeauftragte bestellt?

Ein besonderes Verfahren für die Auswahl von Datenschutzbeauftragten ist nicht vorgegeben. Beispielsweise könnte zunächst eine Interessenabfrage stattfinden. In jedem Fall sollte eine geeignete Person, die bestellt werden soll, zunächst die Gelegenheit haben, dazu Stellung zu nehmen. Das Ziel sollte sein, Beschäftigte mit der Aufgabe zu betrauen, die sowohl geeignet als auch an der Aufgabe interessiert sind.

Der Personalrat hat bei der Bestellung mitzuwirken (§ 72 Abs. 4 Satz 1 Nr. 6 Landespersonalvertretungsgesetz).

Eine schriftliche Bestellung ist erforderlich, um Aufgaben und Rechte sicher zu dokumentieren. [Muster: Anlage 1]

g. Bekanntmachung der Bestellung

Damit Datenschutzbeauftragte ihre Aufgaben erfüllen können, sollte die Bestellung den Beschäftigten und den Bürgerinnen und Bürgern bekannt gemacht werden. Die Beschäftigten sollten direkt informiert werden [Muster: Anlage 2]. Die oder Datenschutzbeauftragte sollte auch im Geschäfts- und Organisationsplan aufgeführt sein.

h. Beendigung der Bestellung

Das DSG NRW enthält keine Regelung zur Beendigung der Bestellung. Die Beendigung steht im Spannungsverhältnis zum Verbot, Datenschutzbeauftragte wegen der Erfüllung ihrer Aufgaben zu benachteiligen (§ 32a Abs. 2Satz 2 DSG NRW), und zur Unabhängigkeit der Funktion. Eine Beendigung ist deshalb nur in den folgenden Fällen zulässig:

- o <u>Abberufung im Einvernehmen mit der oder dem Datenschutzbeauftragten</u>
  Eine Abberufung im Einvernehmen kommt beispielsweise in Betracht, wenn die oder der Datenschutzbeauftragte

mit neuen fachlichen Aufgaben betraut werden möchte, die die Fortsetzung der Tätigkeit nicht zulassen.

- o Abberufung aus wichtigem Grund
  Mängel in der Zuverlässigkeit mit Datenschutzbezug können ausnahmsweise eine Abberufung rechtfertigen. Wenn zum Beispiel ein Datenschutzbeauftragter selbst vorsätzlich gegen Datenschutzrecht verstößt, zeigt dies einen Mangel an Zuverlässigkeit, der zur Abberufung führen kann.

  Mangelnde Sachkenntnis kann durch Fortbildung verbessert werden, so dass Mängel in der Sachkenntnis regelmäßig kein Grund für eine Abberufung sondern für eine Fortbildung sind.

  Eine fehlerhafte Beratung ohne Vorsatz oder grobe Fahrlässigkeit oder eine Auffassung, die von anderen Meinungen abweicht, kann keine Abberufung rechtfertigen.

  Eine neue Aufgabenverteilung ist kein Grund, der zu einer Abberufung ohne Einvernehmen führen könnte. Falls eine neue Aufgabe zu einer Interessenkollision führen würde, darf sie Datenschutzbeauftragten nicht zugewiesen werden.

- o Ausscheiden der oder des Datenschutzbeauftragten aus der öffentlichen Stelle, die die Bestellung vorgenommen hat, oder aus dem Beschäftigungsverhältnis,
  weil die Voraussetzung einer oder eines "internen" Datenschutzbeauftragten dann nicht mehr erfüllt ist.

3. Aufgaben und Befugnisse von Datenschutzbeauftragten

Datenschutzbeauftragte sollen für die Leitung und die Beschäftigten in allen Fragen des Datenschutzes ansprechbar sein. Sie haben die folgenden Hauptaufgaben in Datenschutzfragen (§ 32a Abs. 1 Satz 5 ff. DSG NRW):

- o Unterstützung
- o Beratung
- o Überwachung

Personalräte werde von Datenschutzbeauftragten bei der Sicherstellung des Datenschutzes unterstützt, aber nicht überwacht (§ 32a, Abs. 1 Satz 8 DSG NRW). Die Einhaltung des Datenschutzes obliegt Personalräten eigenverantwortlich.

Im Einzelnen haben Datenschutzbeauftragte die folgenden Aufgaben und Befugnisse:

a. Frühzeitige Beteiligung

Datenschutzbeauftragte sind an datenschutzrelevanten Vorgängen zu beteiligen. Sie müssen über Planungen von Verfahren, Regelungen und Maßnahmen, die den Umgang mit personenbezogenen Daten betreffen, rechtzeitig informiert werden, damit sie beraten, eine Bewertung aus datenschutzrechtlicher Sicht abgeben und kontrollieren können. (§ 32a Abs. 1 Sätze 6 und 7 DSG NRW)

Von internen Rundschreiben über Antragsformulare, Richtlinien und Dienstvereinbarungen bis zu Verträgen, die Auswirkungen auf den Datenschutz haben, gibt es viele Gelegenheiten, bei denen die Beteiligung von Datenschutzbeauftragten geboten und nützlich sein kann.

b. Führung des Verfahrensverzeichnisses

Das Verfahrensverzeichnis dient dazu, den Überblick darüber zu behalten, wo sich in der öffentlichen Stelle personenbezogene Daten befinden und wie sie verarbeitet werden. Jede Daten verarbeitende Stelle, die automatisierte Verfahren zur Verarbeitung personenbezogener Daten betreibt, hat ein Verfahrensverzeichnis aufzustellen (§ 8 Abs. 1 DSG NRW), das die oder der Datenschutzbeauftragte führt (§ 32a Abs. 3 Satz 2 DSG NRW) [Muster: Anlage 3]. Die notwendigen Informationen dafür werden von der öffentlichen Stelle zur Verfügung gestellt (§ 32a Abs. 3 Satz 1 DSG NRW). Innerhalb einer öffentlichen Stelle kann die Aufgabe, Beiträge zum Verfahrensverzeichnis zu erstellen, auf einzelne Organisationseinheiten delegiert werden. Die Verantwortung dafür trägt dann weiterhin die öffentliche Stelle bzw. deren Leitung. Die Datenschutzbeauftragten bündeln einzelne Verfahrensbeschreibungen zu einem Verfahrens-

verzeichnis und achten darauf, dass es aktuell und vollständig ist.

Ein Verfahren ist eine Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen. Ein Verfahren kann also auch mehrere Anwendungen und eine Vielzahl von Dateien umfassen. Eine Verfahrensbeschreibung sollte einerseits nicht so kleinteilig sein, dass sie nicht mehr den Überblick verschaffen kann, der dem Sinn des Verfahrensverzeichnisses entspricht (z. B. nicht: Verfahren "Dienstjubiläen" oder "Geburtstagsliste"). Anderseits sollte der Verfahrensbegriff aber auch so verstanden werden, dass die Betroffenen noch erkennen können, dass in diesem Verfahren ihre Daten verarbeitet werden (z. B. nicht: Verfahren "Allgemeine innere Verwaltung", sondern Verfahren "Personalverwaltung Beamte", "Beihilfe").

Das Verfahrensverzeichnis kann grundsätzlich von jeder Person eingesehen werden. Die oder der Datenschutzbeauftragte gewährt die Einsicht und entscheidet über die im DSG NRW geregelten Ausnahmen vom Einsichtsrecht (§ 32a Abs. 3 Satz 2 ff. DSG NRW).

c. Vorabkontrolle

Wenn neue Datenverarbeitungsverfahren bereits eingeführt worden sind, lassen sich mögliche Datenschutzmängel oft nur noch mit großem Aufwand und hohen Kosten beheben. Deshalb ist vor der Entscheidung über den Einsatz oder eine wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten eine Vorabkontrolle durchzuführen (§ 10 Abs. 3 DSG NRW). Einsatz oder Änderung sind nur dann zulässig, wenn die Vorabkontrolle ergibt, dass Gefahren für das informationelle Selbstbestimmungsrecht nicht bestehen oder durch technisch-organisatorische Maßnahmen verhindert werden.

Die Vorabkontrolle führt die oder der Datenschutzbeauftragte durch (§ 32a Abs. 1 Satz 7 a. E. DSG NRW). Um die Vorabkontrolle zu erleichtern, kann ein Fragenkatalog verwendet werden, der wichtige Fragen berücksichtigt [Muster: Anlage 4]. Der Katalog ist nicht abschließend, da jeder Einzelfall Besonderheiten aufweisen kann, die zusätzlich zu berücksichtigen sind.

Bei der Vorabkontrolle prüfen Datenschutzbeauftragte, ob alle Aspekte hinreichend berücksichtigt sind, und können Empfehlungen für Verbesserungen geben. Soweit zu den Kontrollpunkten des Fragenkatalogs noch sachliche Informationen fehlen, liefert diese die öffentliche Stelle.

d. Schulung von Beschäftigten

Datenschutzbeauftragte haben Personen, die mit der Verarbeitung personenbezogener Daten befasst sind, mit den Datenschutzvorschriften vertraut zu machen (§ 32a Abs. 1 Satz 7 DSG NRW). Daneben bleibt die Aufgabe der Leitung bestehen, für die erforderlichen Kenntnisse der Beschäftigten zu sorgen. Soll diese Aufgabe schwerpunktmäßig auf Datenschutzbeauftragte delegiert werden, ist darauf zu achten, dass diesen dafür ausreichend Arbeitszeit zur Verfügung steht.

e. Ansprechpartnerinnen und Ansprechpartner für Beschäftigte

Datenschutzbeauftragte beraten Beschäftigte und können Beschwerden nachgehen, die einzelne Beschäftigte an sie herantragen. Beschäftigte der öffentlichen Stellen können sich deshalb jederzeit in Datenschutzangelegenheiten unmittelbar an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden. Datenschutzbeauftragte sind zur Verschwiegenheit verpflichtet, soweit sie davon nicht von der betroffenen Person befreit worden sind. (§ 32a DSG NRW)

f. Ansprechpartnerinnen und Ansprechpartner für Bürgerinnen und Bürger

Zwar sind die Datenschutzbeauftragten der öffentlichen Stellen nach der Regelung des DSG NRW nicht Ansprechpartnerinnen und Ansprechpartner für Bürgerinnen und Bürger. In vielen Bereichen kann es aber sinnvoll sein, ihnen auch diese Aufgabe zusätzlich zuzuweisen. Sie koordinieren und beantworten dann externe Datenschutzbeschwerden für die öffentliche Stelle, die weiterhin für die Einhaltung der Datenschutzvorschriften verantwortlich bleibt. So können Datenschutzbeauftragte zugleich für ihre Funktion wertvolle Hinweise auf mögliche Mängel erhalten. Die Gefahr einer Interessenkollision besteht insoweit nicht.

Vielmehr ist die Kombination der internen und der externen Beschwerdestelle für nicht-öffentliche Stellen nach dem Bundesdatenschutzgesetz bewährte Praxis.

g. Überwachung

Zu den Überwachungsaufgaben gehören unter anderem

- die Prüfung der technischen und organisatorischen Maßnahmen (§ 10 DSG NRW),
- die Kontrolle, ob bei einer Auftragsdatenverarbeitung durch externe Stellen die Weisungen des Auftraggebers eingehalten werden (Die Kontrollpflichten des Auftraggebers bleiben dabei bestehen.) und
- die Erstellung behördeninterner Audits für Verfahren sowie die Information der Leitung über das Prüfungsergebnis.

Es gehört dagegen nicht zu den Aufgaben von Datenschutzbeauftragten, einzelne Beschäftigte zu kontrollieren. Beispielsweise ist für die Kontrolle, ob hausinterne Regelungen zur Internet- oder E-Mail-Nutzung eingehalten werden, die Leitung verantwortlich. Datenschutzbeauftragte können dabei zu den zulässigen Kontrollverfahren beraten oder zum Beispiel aufgrund einer Dienstvereinbarung zur Überwachung solcher Kontrollen hinzugezogen werden.

4. Stellung und Rechte von Datenschutzbeauftragten

Eine unabhängige und organisatorisch herausgehobene Stellung mit besonderen Rechten ist entscheidend für eine wirkungsvolle Tätigkeit von Datenschutzbeauftragten.

a. Organisatorische Einbindung

Datenschutzbeauftragte sind in dieser Eigenschaft der Leitung der öffentlichen Stelle unmittelbar zu unterstellen (§ 32a Abs. 2 Satz 1 DSG NRW). Datenschutzbeauftragte können sich jederzeit unmittelbar an die Leitung wenden und sind in ihrer Funktion nur ihr gegenüber rechenschaftspflichtig. Damit kann die Leitung frühzeitig über Datenschutzmängel oder Verbesserungsvorschläge unterrichtet werden und schnell reagieren.

Die Leitung ist hier als Oberbegriff zu verstehen und umfasst

- die Spitze der öffentlichen Stelle (z. B. Minister, Oberbürgermeister),
- die sonstige Leitung, die gesetzlich oder nach der Verfassung berufen ist (z. B. Staatssekretär, Erster Beigeordneter) und
- die (erste) Vertretung dieser Funktionen.

b. Weisungsfreiheit

Datenschutzbeauftragte sind in dieser Funktion weisungsfrei (§ 32a Abs. 2 Satz 1 DSG NRW). Sie können selbst über den Zeitpunkt und die Art und Weise ihrer Tätigkeit entscheiden. Dies umfasst die Entscheidung, ob sie eine datenschutzrechtliche Prüfung durchführen, ebenso wie die Freiheit, sich für die Rechtsauffassung zu entscheiden, die nach ihrer begründeten Überzeugung im Einzelfall zutrifft.

Wenn Leitungen Datenschutzbeauftragten gezielt Verfahren oder Fragen zur Prüfung vorlegen, steht dem die Weisungsfreiheit grundsätzlich nicht entgegen. Vielmehr fordert sie damit die Beratungsfunktion der oder des Datenschutzbeauftragten gegenüber der Behördenleitung ab.

c. Benachteiligungsverbot

Datenschutzbeauftragte dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden (§ 32a Abs. 2 Satz 2 DSG NRW). Dieses weit gefasste Benachteiligungsverbot richtet sich nicht nur an die Behördenleitung, sondern auch an die Beschäftigten und den Personalrat. Es bedeutet zudem, dass die Tätigkeit von Datenschutzbeauftragten keine negativen Auswirkungen auf deren berufliche Entwicklung haben darf.

d. Unterstützungspflicht der verantwortlichen Stelle

Datenschutzbeauftragte können ihre Funktion nur wahrnehmen, wenn sie von der öffentlichen Stelle dabei unterstützt werden. Zur Unterstützung gehören:

- Einblick in grundsätzlich alle Unterlagen, die personenbezogene Daten enthalten oder den Umgang damit betreffen, soweit es für die Aufgabe erforderlich ist.
  Ausnahmen:
  - Personalakten:
    Datenschutzbeauftragte gehören nach den besonderen Regelungen des § 84 Abs. 1 Landesbeamtengesetz nicht zu den Zugangsberechtigten. Die Vorschrift gilt für nicht beamtete Beschäftigte entsprechend (§ 29 Abs. 2 DSG NRW). Der Einblick in Personalakten ist aber dann zulässig und zu gewähren, wenn die betroffenen Beschäftigten eingewilligt haben.
  - Unterlagen mit sensitiven Daten:
    Für die Verarbeitung von sensitiven Daten im Sinne des § 4 Abs. 3 DSG NRW gelten die dort genannten besonderen Voraussetzungen. Der Einblick ist zum Beispiel dann zulässig und zu gewähren, wenn die betroffenen Personen eingewilligt haben.
  - Sicherheitsvorgänge:
    Für bestimmte Vorgänge gibt es besondere Regelungen, die Voraussetzungen für den Einblick bestimmen. Wenn dazu zum Beispiel eine Sicherheitsüberprüfung erforderlich ist, schließt dies den Einblick durch Datenschutzbeauftragte aber nicht von vorne herein aus. Vielmehr ist bei Bedarf eine Sicherheitsüberprüfung der Datenschutzbeauftragten durchzuführen.

- Fort- und Weiterbildungen, die unter Berücksichtigung der persönlichen Qualifikation und der Aufgabenentwicklung erforderlich sind; Möglichkeit zum Erfahrungsaustausch mit Datenschutzbeauftragten von anderen Stellen

- Einrichtungen, Geräte und Mittel, die für die Aufgabe erforderlich sind

- Hilfspersonal, soweit dies – etwa bei großen Stellen – erforderlich ist

e. Arbeitszeit

Datenschutzbeauftragten muss ausreichend Arbeitszeit für die Erfüllung ihrer Aufgaben zur Verfügung stehen. Wie viel Zeit

erforderlich ist, hängt vom Bedarf der jeweiligen Stelle ab. Zum Beispiel können sich die Menge und die Art der personenbezogenen Daten ebenso auf die notwendige Arbeitszeit auswirken wie Anzahl und Komplexität von Datenverarbeitungsverfahren. Orientierungswerte können deshalb vorab nicht bestimmt werden.

f. Eingruppierung (Bezüge/Entgelt)

Aus dem Datenschutzrecht ergeben sich keine Vorgaben für die angemessene Eingruppierung von Datenschutzbeauftragten. Bei den dienst- und arbeitsrechtlichen Überlegungen wird die verantwortliche Stelle aber zu beachten haben, dass die Aufgabe mit besonderen Fachkenntnissen, Selbständigkeit und Unabhängigkeit verbunden ist. Dabei können auch der Umfang und die Komplexität der Aufgabe berücksichtigt werden, die sich nach den Anforderungen in einer konkreten öffentlichen Stelle richten.

g. Haftung

Datenschutzbeauftragte unterliegen keinen besonderen Haftungsregeln, die nicht auch für andere Beschäftigte gelten. Sie haften insbesondere nicht selbst "nach außen" gegenüber Bürgerinnen und Bürgern oder Unternehmen.

h. Beratung durch den Landesbeauftragten für Datenschutz und Informationsfreiheit

Datenschutzbeauftragte sollten zunächst versuchen, Fragestellungen mit der eigenen Kompetenz und in Zusammenarbeit mit der öffentlichen Stelle und deren Leitung im Konsens vor Ort zu lösen. Es gibt aber auch Fälle, in denen Datenschutzbeauftragte eine weitergehende Beratung brauchen oder in denen sie befürchten, dass die öffentliche Stelle entgegen ihrer Beratung gegen Datenschutzvorschriften verstößt. Dann können sie sich – wie jede und jeder – an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden. Ein Dienstweg muss dazu nicht eingehalten werden und niemand darf deswegen benachteiligt werden (§ 25 DSG NRW).

5. Muster, andere Empfehlungen und Regelungen

Die folgenden Muster sind keine gesetzliche Vorgabe. Die Verwendung ist aber empfehlenswert, damit die gesetzlichen Grundanforderungen beachtet werden. Die Muster stehen auch einzeln unter www.ldi.nrw.de zur weiteren Verwendung bereit.

Auch andere Muster, die im Detail abweichen, können geeignet sein. Beispielsweise empfiehlt der Runderlass des Innenministeriums NRW vom 12.12.2000 (MBl. NRW. 2001 S. 50) vergleichbare Muster.

Für die Polizei gilt ergänzend die "Sonderregelung für den Bereich der behördlichen Datenschutzbeauftragten bei den Polizeibehörden und -einrichtungen (PB/PE) des Landes Nordrhein-Westfalen (DSB-Richtlinie-Polizei)", RdErl. d. Innenministeriums v. 06.05.2005 (MBl. NRW. 2005 S. 632).

Anlagen:

1. Bestellung zur/zum behördlichen Datenschutzbeauftragten + Bestellung zur Vertreterin/zum Vertreter
2. Bekanntmachung/Hausmitteilung Datenschutz
3. Verfahrensverzeichnis
4. Vorabkontrolle

Anlage 1: Muster zur Bestellung

Bestellung zur / zum behördlichen Datenschutzbeauftragten

Sehr geehrte(r) Frau/Herr ....,

mit Wirkung vom ... bestelle ich Sie zur/zum behördlichen Datenschutzbeauftragten. In dieser Funktion sind Sie der Behördenleitung unmittelbar unterstellt.

Ihre Aufgabe ist es, ungeachtet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, die Behörde bei der Sicherstellung des Datenschutzes zu unterstützen. Im Einzelnen ergibt sich die Aufgabe aus § 32a Datenschutzgesetz Nordrhein-Westfalen.

Bei der Erfüllung Ihrer Aufgabe sind Sie von allen Organisationseinheiten zu unterstützen. Alle Beschäftigten der Behörde können sich jederzeit in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an Sie wenden.

Als Ihre/n Vertreter/in bestelle ich Frau/Herrn ....

Mit freundlichen Grüßen

Bestellung zur / zum Vertreter / in der / des behördlichen Datenschutzbeauftragten

Sehr geehrte(r) Frau/Herr ....,

mit Wirkung vom ... bestelle ich Sie zur/zum Vertreter/in der/des behördlichen Datenschutzbeauftragten. Im Falle einer Vertretung entspricht Ihre Rechtsstellung der/des behördlichen Datenschutzbeauftragten.

Ihre Aufgabe ist es, im Vertretungsfall ungeachtet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, die Behörde bei der Sicherstellung des Datenschutzes zu unterstützen. Im Einzelnen ergibt sich die Aufgabe aus § 32a Datenschutzgesetz Nordrhein-Westfalen.

Bei der Erfüllung Ihrer Aufgabe sind Sie von allen Organisationseinheiten zu unterstützen. Alle Beschäftigten der Behörde können sich jederzeit in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an Sie wenden.

Mit freundlichen Grüßen

Anlage 2: Muster zur Bekanntmachung

Hausmitteilung: Bestellung einer/s behördlichen Datenschutzbeauftragten sowie einer/s Vertreterin/Vertreters

Mit Wirkung vom ... wurde

Frau/Herr ...

zur/zum behördlichen Datenschutzbeauftragten

sowie

Frau/Herr ...

zur/zum Vertreterin/Vertreter der/des behördlichen Datenschutzbeauftragten bestellt. Die/der behördliche Datenschutzbeauftragte sowie ihre/sein/e Vertreterin/Vertreter sind in dieser Eigenschaft der Leitung der Behörde unmittelbar unterstellt.

Ihre/Seine Aufgabe ist es, ungeachtet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten die Behörde bei der Sicherstellung des Datenschutzes zu unterstützen. Im Einzelnen ergibt sich die Aufgabe aus § 32a Datenschutzgesetz Nordrhein-Westfalen (DSG NRW).

Bei der Erfüllung ihrer/seiner Aufgabe sind die/der behördliche Datenschutzbeauftragte sowie ihre/sein/e Vertreterin/Vertreter von allen Organisationseinheiten zu unterstützen. Soweit sie personenbezogene Daten verarbeiten, sind die Beschäftigten der Behörde verpflichtet, bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren sowie bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten die/den Datenschutzbeauftragte/n frühzeitig zu beteiligen. Alle Beschäftigten der Behörde können sich jederzeit in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an die/den behördlichen Datenschutzbeauftragte/n sowie im Vertretungsfall an die/den Vertreter/in wenden.

Auf die Regelungen in den §§ 8, 10 und 32a DSG NRW wird besonders hingewiesen.

Anlage 3: Muster für ein Verfahrensverzeichnis

Verfahrensverzeichnis

Beschreibung des einzelnen Verfahrens nach § 8 DSG NRW

Lfd. Nr.: (wird vom DSB vergeben)

☐ Neues Verfahren / Erstmeldung
☐ Wesentliche Änderung

☐ Das Verfahren ist zur Einsichtnahme bestimmt (§ 8 Abs. 2 Satz 1 DSG NRW).

☐ Das Verfahren ist nur teilweise zur Einsichtnahme bestimmt. Ausgenommen sind die Angaben nach § 8 Abs. 1 Nr. 7, 8 und 11 DSG NRW.

☐ Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§ 8 Abs. 2 Satz 2 DSG NRW).

☐ Das Verfahren ist Teil eines gemeinsamen oder verbundenen Verfahrens nach § 4 a DSG NRW.
Verantwortliche Stelle:

Daten verarbeitende Stelle	Behördlicher Datenschutzbeauftragter
Datum Unterschrift	Datum Unterschrift

Teil A Allgemeine Angaben (durch die Daten verarbeitende Stelle auszufüllen)

1 Name und Anschrift der Daten verarbeitenden Stelle

1.1 Name und Anschrift

1.2 Organisationseinheit

2 Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1 Zweckbestimmung

2.2 ggf. Bezeichnung des Verfahrens

2.3 Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterschieden)

3 Art der gespeicherten Daten

Lfd. Nr.	Feldbezeichnung	Feldinhalt
Besonders geschützte Daten nach § 4 Abs. 3 DSG NRW (bitte Lfd. Nr. angeben):		

4 Kreis der Betroffenen

Lfd.Nr. aus 3	

5 Zugriffsberechtigte Personen oder Personengruppen

Lfd.Nr. aus 3	

6 regelmäßiger Erhalt und regelmäßige Weitergabe von Daten

6.1 Herkunft der Daten bei erhaltenen Daten

Lfd.Nr. aus 3	

6.2 Empfänger der Daten bei weitergeleiteten Daten

Lfd.Nr. aus 3	

6.3 Beabsichtigte Datenübermittlung in „Drittstaaten“ (§ 17 Abs. 1 Satz 2 und Abs. 2 DSG NRW)

Lfd.Nr. aus 3	Empfänger

7 Fristen für Sperrung und Löschung

Lfd.Nr. aus 3	Sperrfrist (§ 19 Abs. 2 DSG NRW)	Löschfrist (§ 19 Abs. 3 DSG NRW)

Teil B Sicherheitskonzept (durch Daten verarbeitende Stelle bzw. Systemverwaltung auszufüllen)

1 Technische und organisatorische Maßnahmen (§ 10 DSG NRW)

Erläuterung zu den einzelnen Maßnahmen zur Gewährleistung der

Vertraulichkeit (§ 10 Abs. 2 Nr. 1 DSG NRW), z.B.

- Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern
- Benutzerkontrolle durch Passwortregelung zur Legitimation und durch automatische Bildschirmsperrung
- Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

---

Integrität (§ 10 Abs. 2 Nr. 2 DSG NRW), z.B.

- Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten
- Regelmäßige Kontrolle der Aktualität

Verfügbarkeit (§ 10 Abs. 2 Nr. 3 DSG NRW), z.B.

- Klare und übersichtliche Ordnung des Datenbestandes
- Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

Authentizität (§ 10 Abs. 2 Nr. 4 DSG NRW), z.B.

- Dokumentation der Ursprungsdaten und ihrer Herkunft
- Nachvollziehbarkeit der Verarbeitungsschritte

Revisionsfähigkeit (§ 10 Abs. 2 Nr. 5 DSG NRW), z.B.

- Festlegung klarer Zuständigkeiten und Verantwortlichkeiten
- Protokollierung der Eingabe und weiteren Verarbeitung der Daten
- Aufbewahrung der Protokolldaten

Transparenz (§ 10 Abs. 2 Nr. 6 DSG NRW), z.B.

- Vollständige, übersichtliche und jederzeit nachprüfbare Dokumentation aller wesentlichen Datenverarbeitungsvorgänge

2 Technik des Verfahrens

2.1 ☐ *Verfahren für Einzelplatzsystem*

Betriebssystem:

2.2 ☐ *Client-Server-Verfahren*

Client (Datenendgerät): ☐ Terminal/Netz-PC (ohne Laufwerke/Festplatten)

☐ PC (Arbeitsplatzrechner/Workstation)

Betriebssystem des Servers:

Client-Server-Kommunikation erfolgt über

☐ geschlossenes Netz innerhalb der Behörde (LAN)

☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises

☐ Landesverwaltungsnetz

☐ Sonstiges

☐ Offenes Netz (z.B. Internet)

☐ Sonstige eingesetzte Hardware (z.B. Chipkarte, Kartenlesegeräte etc.)

Datenspeicherung erfolgt auf

☐ Server innerhalb der Behörde

☐ Server bei anderen Institutionen

☐ PC/Arbeitsplatzrechner

Art der Daten (lfd. Nr. aus Teil A Nr. 3):

2.3 ☐ *Großrechner-Verfahren*

Client (Datenendgerät): ☐ Terminal/Netz-PC (ohne Laufwerke/Festplatten)

☐ PC (Arbeitsplatzrechner/Workstation)

Betriebssystem des Großrechners:

Kommunikation zwischen Client und Großrechner erfolgt über

☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises

- ☐ Landesverwaltungsnetz
- ☐ Sonstiges

☐ Offenes Netz (z.B. Internet)

☐ Sonstige eingesetzte Hardware (z.B. Chipkarte, Kartenlesegeräte etc.)

Datenspeicherung erfolgt auf

☐ Großrechner

☐ Server innerhalb der Behörde

☐ Server bei anderen Institutionen

☐ PC/Arbeitsplatzrechner

Art der Daten (Lfd. Nr. aus Teil A Nr. 3):

3 Eingesetzte Software (einschließlich Standardverfahren)

Name	Version/Stand/Datum

Teil C Begründetes Ergebnis der Vorabkontrolle gemäß § 10 Abs. 3 DSG NRW (durch Datenschutzbeauftragten auszufüllen)

Anlage 4: Kriterien für die Vorabkontrolle

§ 10 Abs. 3 DSG NRW sieht eine Vorabkontrolle vor. Sie ist vor Beginn oder vor wesentlichen Änderungen eines Verfahrens durchzuführen und wird als Bestandteil des von der verantwortlichen Stelle zu erstellenden Sicherheitskonzepts im Gesetz beschrieben. Die Vorabkontrolle selbst führt die oder der Datenschutzbeauftragte der verantwortlichen Stelle durch.

Die Vorstellung einer in das Sicherheitskonzept integrierten Vorabkontrolle verdeutlicht, dass es keinen starren Ablaufplan gibt, wonach zunächst ein Sicherheitskonzept zu erstellen wäre, das in einem zweiten Schritt dann die Vorabkontrolle besteht oder nicht besteht. Vielmehr handelt es sich um einen dialogischen Prozess zwischen den für den Einsatz des Verfahrens verantwortlichen Verwaltungseinheiten und der oder dem Datenschutzbeauftragten. Im Verlauf des Dialogs sind technische Nachbesserungen möglich, so dass am Ende ein positives Ergebnis der Vorabkontrolle erreicht werden kann. Nur wenn dieser Dialogprozess fehlschlägt, wird es ein negatives Ergebnis der Vorabkontrolle geben.

Ein schlüssiges Sicherheitskonzept setzt zunächst voraus, dass der Bereich, der das Verfahren zur Unterstützung seiner Verwaltungstätigkeit benötigt, die Anforderungen an das Verfahren auch in datenschutzrechtlicher Hinsicht beschreibt. Es ist also vor einem Datensicherheitskonzept zunächst ein Datenschutzkonzept zu erstellen, das zum Beispiel die Zugriffsberechtigungen gemäß den rechtlichen Vorgaben abbildet, den Umfang der zu erhebenden Daten beschreibt und die Anforderungen für die Datenlöschung oder -berichtigung fixiert.

Liegt eine umfassende Verfahrensbeschreibung einschließlich Datenschutzkonzept vor, kann die mit der technischen Umsetzung befasste Stelle das Datensicherheitskonzept entwerfen. Hierbei berücksichtigt sie den Schutzbedarf der Daten und beschreibt die aus ihrer Sicht notwendigen Maßnahmen zur Umsetzung des Datenschutzkonzepts und zur Erfüllung der Sicherheitsziele gemäß § 10 Abs. 2 DSG NRW. Insbesondere bei besonderen Kategorien von Daten gemäß § 4 Abs. 3 DSG NRW oder bei Daten, die einem gesetzlichen Geheimnisschutz unterliegen, besteht regelmäßig ein hoher Schutzbedarf, der eine zusätzliche Risiko- und Bedrohungsanalyse erfordert, um an-

gemessene Sicherheitsmaßnahmen für diese besonders zu schützenden Daten festzulegen.

Davon zu unterscheiden ist die Analyse der oder des Datenschutzbeauftragten, der im Rahmen der Vorabkontrolle überprüft, ob Gefahren für das Recht auf informationelle Selbstbestimmung bestehen. Während sich die Risiko- und Bedrohungsanalyse alleine auf den Teilaspekt des technischen Schutzes der Daten vor unbefugten Zugriffen beschränkt, betrachtet die oder der Datenschutzbeauftragte das Verfahren in seiner Gesamtheit und überprüft insbesondere, ob die datenschutzrechtlichen Verfahrensanforderungen durch geeignete technisch-organisatorische Maßnahmen umgesetzt werden.

Für die Vorabkontrolle sind besonders die folgenden Kriterien zu prüfen, die – wenn erforderlich – in besonderen Fällen noch ergänzt werden müssen:

- Datenschutz- und Datensicherheitskonzept vollständig und schlüssig?
  Das Datenschutz- und Datensicherheitskonzept muss die rechtlichen und technischen Aspekte ausreichend berücksichtigen. Das Konzept darf keine logischen Fehler enthalten.

- Datenverarbeitung zulässig und durch technisch-organisatorische Maßnahmen entsprechend umgesetzt
  Die geplante Datenverarbeitung muss durch eine Rechtsvorschrift oder durch die Einwilligung der betroffenen Person erlaubt sein (§ 4 Abs. 1 DSG NRW; bei sensitiven Daten: § 4 Abs. 3 DSG NRW). Art und Umfang der Datenverarbeitung müssen zudem den Anforderungen des DSG NRW und/oder spezieller Gesetze, die für die konkrete Datenverarbeitung maßgeblich sind, entsprechen. Im Folgenden sind die Anforderungen nach dem DSG NRW dargestellt*:

  - Erhebung: Anforderungen des § 12 DSG NRW* erfüllt?
  - Übermittlung: Anforderungen der § 14 bis 17 DSG NRW* (je nach Anwendungsfall) erfüllt?
  - Zweckbindung: Anforderungen des § 13 DSG NRW* erfüllt?

* Soweit für die Verarbeitung Spezialgesetze gelten, legen diese die Anforderungen anstelle der Vorschriften des DSG NRW fest.

- Datenvermeidung: So wenig Daten wie möglich (§ 4 Abs. 2 DSG NRW)?
- Keine Entscheidung ausschließlich aufgrund automatisierter Verfahren: Anforderungen des § 4 Abs. 4 DSG NRW erfüllt?
- Trennungsgebot: Anforderungen des § 4 Abs. 6 DSG NRW* erfüllt?
- Sicherheitsziele: Ziele nach § 10 Abs. 2 DSG NRW erreicht?
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität
  - Revisionsfähigkeit
  - Transparenz

- Rechte der betroffenen Person gesichert?

  Die Rechte nach § 5 Satz 1 Nr. 1 bis 4 DSG NRW* müssen technisch-organisatorisch vollständig umsetzbar sein. Beispielsweise würde ein Verfahren die gesetzlichen Anforderungen nicht erfüllen, bei dem Löschungsansprüche nicht umsetzbar sind, weil dies vom genutzten Programm nicht vorgesehen ist. Die Rechte müssen für betroffene Personen auch einfach geltend zu machen sein. Zum Beispiel dürfen Betroffene nicht allein auf ein technisches Verfahren verwiesen werden, das nicht barrierefrei zu nutzen ist. Die Möglichkeit, ein Recht bei der Sachbearbeitung einer verantwortlichen Stelle geltend zu machen, reicht aber grundsätzlich aus.

  - Auskunft, Einsichtnahme (§ 18 DSG NRW)
  - Widerspruch aus besonderem Grund (§ 4 Abs. 5 DSG NRW)
  - Unterrichtung (§§ 12 Abs. 2, 13 Abs. 2 Satz 2, 16 Abs. 1 Satz 2 und 3 DSG NRW)
  - Berichtigung, Sperrung, Löschung (§ 19 DSG NRW)

  - Keine Gefahr für die informationelle Selbstbestimmung

  Abschließend ist festzustellen, ob Gefahren für das Recht auf informationelle Selbstbestimmung bestehen. Nach § 10 Abs. 3 Satz 2 DSG NRW darf ein Verfahren nur eingesetzt werden, wenn diese Gefahren nicht bestehen oder

durch technisch-organisatorische Maßnahmen verhindert werden können.

- Konnte die zuständige Verwaltungseinheit für die o.a. Prüfpunkte schlüssige Lösungen darlegen, wird die oder der Datenschutzbeauftragte ein positives Ergebnis der Vorabkontrolle abgeben können. Dabei kann der oder die Datenschutzbeauftragte regelmäßig nur typische Gefahren für das Recht auf informationelle Selbstbestimmung bewerten. Sollten sich zu einem späteren Zeitpunkt völlig atypische oder nicht vorhersehbare Gefahren für das Recht auf informationelle Selbstbestimmung im laufenden Verfahren realisieren, rechtfertigt dies nicht den Rückschluss auf eine mangelhafte Vorabkontrolle.

- Sollte die Prüfung einzelner o.a. Punkte ergeben, dass keine entsprechenden technisch-organisatorischen Maßnahmen vorgeschlagen worden sind, kann die oder der Datenschutzbeauftragte keine positive Gefahrenbewertung abgeben. Ist also beispielsweise eine Löschung nicht mehr erforderlicher Daten im Verfahren gar nicht möglich, werden daraus Gefahren für das Recht auf informationelle Selbstbestimmung der Betroffenen zu erwarten sein. Denn mit der dauerhaften Verfügbarkeit nicht mehr benötigter Daten, besteht die Gefahr, dass diese Daten unzulässig genutzt oder weiter verarbeitet werden.
  In der Regel sollten solche offenen Punkte ausgeräumt werden können, bevor die oder der Datenschutzbeauftragte das Ergebnis der Vorabkontrolle dokumentiert. Hat die oder der Datenschutzbeauftragte im Dialog mit der das Verfahren konzipierenden Stelle aber vergeblich versucht, eine Lösung für ein bestehendes Problem zu erreichen, kann sie oder er am Ende nur ein negatives Ergebnis der Vorabkontrolle feststellen.

Die Verantwortung für den rechtmäßigen Einsatz eines Verfahrens trägt die verantwortliche Stelle. Verantwortliche Stellen könnten sich in der Praxis über die Einschätzung von Datenschutzbeauftragten hinwegsetzen und ein Verfahren trotz eines negativen Ergebnisses der Vorabkontrolle einsetzen. Davon ist

allerdings dringend abzuraten, da die negative Bewertung durch Datenschutzbeauftragte ein gewichtiges Argument gegen den Einsatz eines Verfahrens ist. Bei einem negativen Ergebnis sollte eine verantwortliche Stelle das Verfahren unter Beteiligung ihrer oder ihres Datenschutzbeauftragten grundsätzlich überdenken.

Die oder der Datenschutzbeauftragte vermerkt das Prüfungsergebnis im Verfahrensverzeichnis. Zur Nachvollziehbarkeit empfiehlt es sich dabei, die wesentlichen Überlegungen ebenfalls dort festzuhalten.