RUHRFUTUR

Daten & Analyse

HANDBUCH Datenschutz und kommunales Bildungsmonitoring

Karsten Neumann

Datenschutz und kommunales Bildungsmonitoring: Anforderungen und Lösungen

Vorwort

Von Dr. Markus Küpker und Julia Balke, RuhrFutur

Was hat Bildungsmonitoring mit Datenschutz zu tun? Betrachtet man Bildungsmonitoring als Grundlage für datenbasierte Steuerung im Bildungsbereich, dann wird es klar: **Es geht um Daten und um den Umgang mit ihnen.** Was auf den ersten Blick vielleicht nicht so selbstverständlich erscheint, ist, dass datenbasierte Steuerung und Datenschutz sich nicht gegenseitig ausschließen, auch wenn das eine den Zugriff auf Daten impliziert, während das andere den Zugriff häufig unterbindet.

Datenschutz verhindert nicht den Zugriff auf Daten schlechthin, sondern regelt vielmehr den Umgang mit bestimmten, nämlich personenbezogenen Daten – das sind Informationen jeglicher Art, die dazu geeignet sind, Auskunft über eine bestimmte natürliche Person zu geben. Dahinter steht das im Grundgesetz verankerte Recht auf informationelle Selbstbestimmung, ein unveräußerliches Grundrecht. Nicht zuletzt wegen dieser verfassungsmäßigen Verankerung gehört das deutsche Datenschutzrecht zu den strengsten weltweit. Datenschutz wird in Deutschland sehr ernst genommen.

Es ist aber zugleich auch ein schwieriges Thema, weil es sich als Querschnittsthema durch viele Gesetzbücher zieht und nicht nur auf das Bundesdatenschutzgesetz beschränkt ist: Die ärztliche Schweigepflicht, das Bankgeheimnis, die Verschwiegenheitspflicht von Anwälten und Notaren oder das Verbot von Vorratsdatenspeicherung durch Telekommunikationsanbieter und Telemedienanbieter sind alltägliche Beispiele von datenschutzrechtlichen Bestimmungen in unterschiedlichen Gesetzesbeständen. Hinzu kommen die datenschutzrechtlichen Bestimmungen für das Land und die Kommunen, die als „Lex Specialis“ das Verwaltungshandeln sehr detailliert regeln.

Auch Bildungsmonitoring ist wichtig. Bildungsmonitoring, verstanden als Aufgabe der kontinuierlichen Zusammenführung, Auswertung und Aufbereitung steuerungsrelevanter Bildungsinformationen und seine Produkte – allen voran die Bildungsberichte – sind in den vergangenen zehn Jahren immer mehr zur Anforderung an staatliches Handeln geworden. Dies entspringt zum einen der Tatsache, dass aufgrund immer breiterer Datengrundlage, methodischen Wissens und verfügbarer Technologien datenbasierte Steuerung insgesamt und auch in der Bildung möglich ist. Die schon längst datenbasiert handelnde Wirtschaft demonstriert, dass empirische Fundierung sinnvoll und lohnend ist.

Und die gesellschaftliche Diskussion zeigt zum anderen, dass datenbasierte Steuerung im Sinne der Transparenz staatlichen Handelns erwartet wird und geboten ist.

Aus der Perspektive des Bildungsmanagements ist Datenbasierung aber auch aus einem anderen Grund dringlich: Der Bildungsbegriff hat in unserer Gesellschaft in den letzten ein bis zwei Jahrzehnten in mehrfacher Hinsicht bedeutende Erweiterungen erfahren und an Komplexität gewonnen: Begriffe wie „lebenslanges Lernen“ zeigen, dass Lernen immer mehr als Synonym für Leben betrachtet wird, dass das Lernen mit der Geburt beginnt und keinesfalls mit dem Schulabschluss endet. Und Bildung findet nicht nur in der Schule statt: Gelernt wird auch in der Kindertagesstätte, im Museum, im Schwimmbad, im Sportverein, der Stadtbibliothek, der Volkshochschule, am Arbeitsplatz, im Skatepark und im nahegelegenen Wald.

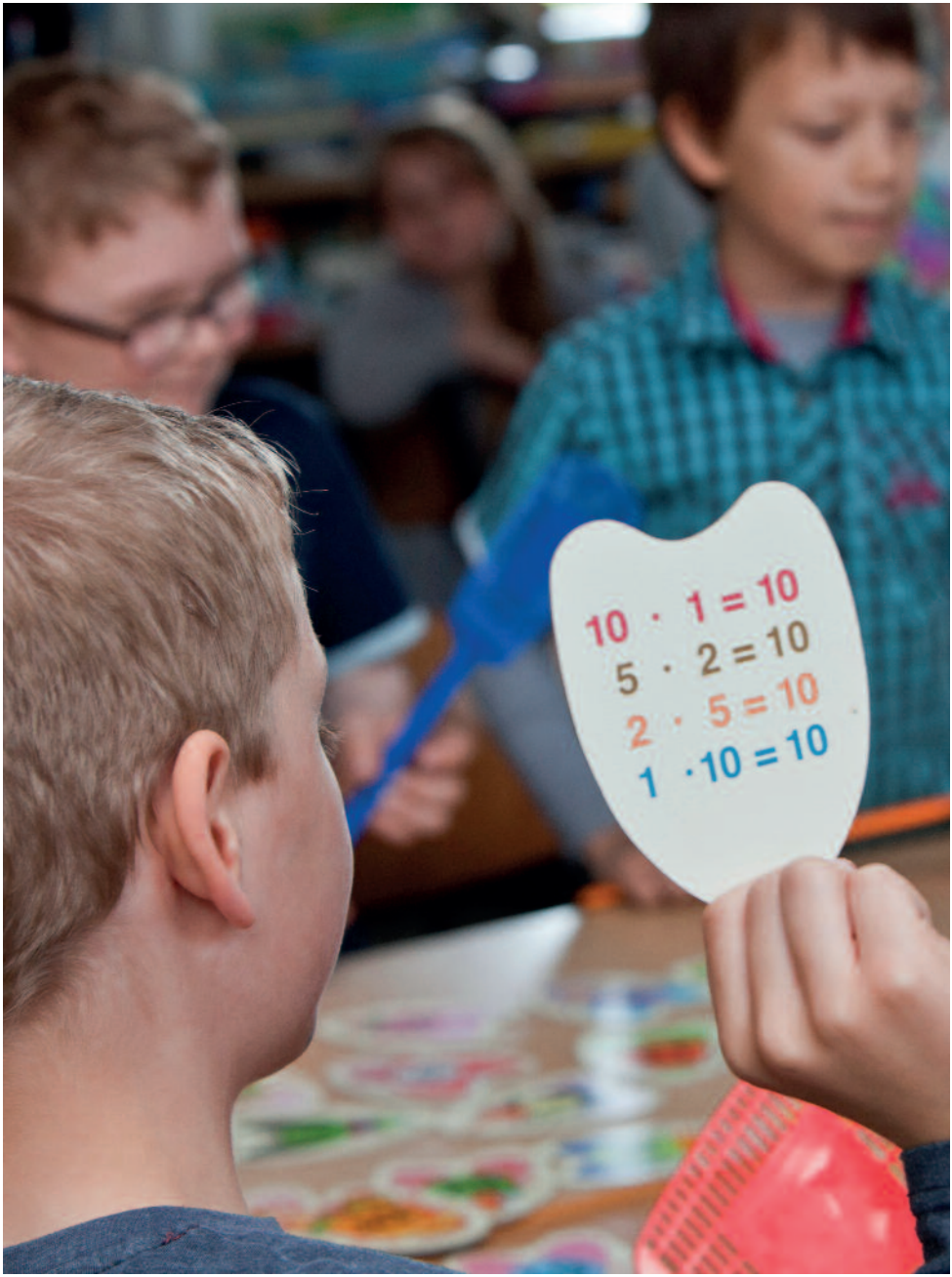
Datenschutz verhindert nicht den Zugriff auf Daten, sondern regelt den Umgang mit personenbezogenen Daten.

Bildung betrifft alle und findet fast überall und fast immer statt. Damit fällt sie auch zwangsweise in unterschiedliche Verantwortungsbereiche, allen voran in diejenigen von Kommunen und Land, aber auch in die von Eltern, zivilgesellschaftlichen und wirtschaftlichen Institutionen sowie die des Bundes. Daten helfen hier, den Überblick zu behalten, Strukturen und Missstände zu erkennen, die Auswirkungen des bildungspolitischen Handelns zu bewerten und ggf. zu revidieren und letzten Endes knappe Ressourcen effizient und effektiv einzusetzen und zu nutzen.

Diese Aspekte sind nicht trivial, denn Bildung wird immer wichtiger: Überall wo es heute um die Zukunft unserer Gesellschaft geht, ist Bildung ein zentraler Begriff. Bildung ist der Schlüssel für gesellschaftliche Teilhabe unabhängig von sozialer Herkunft. Bildung versetzt Menschen in die Lage, sich in der Welt zu orientieren und ihr Leben eigenständig zu gestalten. Und Bildung ist eine Voraussetzung für berufliche Perspektive sowie nicht zuletzt eine zentrale Ressource für die Wirtschaft. Vor diesem Hintergrund ist zu erwarten, dass die Bedeutung und die Möglichkeiten von Bildungsmonitoring weiter wachsen werden.

Zur Umsetzung eines Bildungsmonitorings werden dabei oftmals gar keine personenbezogenen Daten benötigt; nicht selten stützt es sich auf aggregierte amtliche Datenbestände, die datenschutzrechtlich unbedenklich sind.

Manchmal sind die zugänglichen (meist aggregierten) Daten jedoch wenig aussagekräftig; in anderen Fällen sind Datenbestände zwar aussagekräftig, aber nicht zugänglich, und manchmal liegen Daten auch in einer Form vor, in der sie nicht verwendbar sind. Standards, die eine Vergleichbarkeit ermöglichen könnten, finden zudem erst in jüngerer Zeit eine größere Verbreitung. Manchmal fehlen geeignete


10 · 1 = 10
5 · 2 = 10
2 · 5 = 10
1 · 10 = 10

Daten völlig und es scheint geboten, eine eigene Erhebung vorzunehmen.

Das alles tangiert Datenschutz, denn überall dort, wo es um die Zusammenführung, den Austausch oder die Erhebung von Daten aus unterschiedlichen Bereichen der Bildungslandschaft geht, muss sichergestellt sein, dass datenschutzrechtliche Belange gewahrt bleiben. Dadurch kann sich ein Spannungsfeld zwischen den Bedarfen datenbasierter Steuerung einerseits und den Erfordernissen des Datenschutzes andererseits ergeben.

Die vorliegende Handreichung richtet sich an alle, die mit Bildungsmonitoring befasst sind. In der Regel ist dies die Aufgabe eines kommunalen Bildungsbüros oder der Statistikstelle einer Kommune. Betroffen sind aber auch die Mitarbeiterinnen und Mitarbeiter im Qualitätsmanagement der Hochschulen, in der Bildungsforschung oder in anderen Bildungseinrichtungen. Ihnen allen möchte die vorliegende Handreichung als ein erster Zugang zum Thema Datenschutz dienen. Angesichts der thematischen Komplexität beantwortet sie nicht die spezifischen Detailfragen einer bestimmten Kommune oder Bildungseinrichtung. Nichtsdestotrotz kann sie aber zu einem grundlegenden Verständnis des Themas führen und im Idealfall den Leser und die Leserin in die Lage versetzen, die richtigen Fragen zu stellen, sich damit an den zuständigen Datenschutzbeauftragten zu wenden und vielleicht sogar eine Idee für einen möglichen Lösungsweg in Grundzügen vor Augen zu haben. Damit versteht sich die vorliegende Handreichung als konstruktiver Beitrag zum Umgang mit Datenschutz im Kontext von Bildungsmonitoring.

Ein solcher Beitrag ist RuhrFutur ein zentrales Anliegen. Denn datenbasiertes Handeln ist der gemeinsamen Bildungsinitiative von Stiftung Mercator, Landesregierung Nordrhein-Westfalen, Kommunen, Hochschulen und Regionalverband Ruhr für die Metropole Ruhr in zweierlei Hinsicht als zentrales Thema in die Wiege

gelegt worden: Zum einen ist RuhrFutur als Konsequenz aus den Erkenntnissen des Bildungsberichts Ruhr von 2012 ins Leben gerufen worden, dem ersten regionalen Bildungsbericht in Deutschland. Damit entspringt RuhrFutur indirekt einer regionalen Monitoringperspektive. Zum anderen folgt das Design von RuhrFutur dem in den USA entwickelten und dort mittlerweile weit verbreiteten Konzept des Gemeinsamen Wirkens (Collective Impact).

Dabei geht es im Kern darum, das Engagement von Akteuren aus unterschiedlichen Bereichen auf die Bearbeitung einer gemeinsamen gesellschaftlichen Herausforderung auszurichten, die einzelne Akteure nur schwerlich oder gar nicht alleine lösen können, um auf diese Weise eine größere und nachhaltige gesellschaftliche Wirkung, einen Impact, zu erzielen. Ein zentrales Element des Konzepts ist der Aufbau und die Pflege einer gemeinsamen Datenbasis als Grundlage für die Bildung gemeinsamer Zielindikatoren als System der Erfolgsmessung.

In den USA können die Akteure dabei auf eine ganze Reihe öffentlich verfügbarer Daten und standardisierter landesweiter Tests zugreifen, deren Existenz nicht zuletzt auch auf eine andere Kultur im Umgang mit personenbezogenen Daten sowie einer liberaleren Datenschutzgesetzgebung zurückzuführen ist.

In Deutschland und im Ruhrgebiet sind die Rahmenbedingungen wie beschrieben deutlich andere. Da sich die Verantwortung für den Bildungsbereich in der modernen Bildungslandschaft mit ihrem weiten und differenzierten Verständnis von Bildung als lebenslanger Aufgabe und unterschieden nach formaler, non-formaler und informeller Bildung auf viele Schultern verteilt, verteilen sich auch die Daten, die über die Leistungsfähigkeit des Bildungssystems Auskunft geben können. Das alles ist eine Herausforderung für die Umsetzung von Collective Impact unter deutschen Rahmenbedingungen.

Zielt man hierbei nicht nur auf die kommunale, sondern auf eine regionale Ebene, wie es RuhrFutur tut, so wird die skizzierte Komplexität um eine weitere Ebene ergänzt.

Die Bedeutung von Bildungsmonitoring verschiebt sich auf der regionalen Ebene: Bildungsmonitoring wird weniger zur Grundlage von Steuerung als von Governance: Es schafft die Grundlage für ein gemeinsames Handeln verschiedener, insbesondere kommunaler Akteure auf Augenhöhe. Ein Handeln, das auf eine nachhaltige Verbesserung der Bildungs- und Teilhabechancen von Kindern, Jugendlichen und jungen Erwachsenen abzielt und dabei deren Recht auf informationelle Selbstbestimmung schützt.

Bildungsmonitoring schafft die Grundlage für gemeinsames kommunales Handeln auf Augenhöhe.

Datenschutz und kommunales Bildungsmonitoring: Anforderungen und Lösungen

1. Kurze Einführung in das Datenschutzrecht

Karsten Neumann

Datenschutz und kommunales Bildungsmonitoring: Anforderungen und Lösungen

1. Kurze Einführung in das Datenschutzrecht

Ohne moderne Informations- und Kommunikationsmittel ist in den meisten Zusammenhängen eine (Zusammen-)Arbeit kaum noch denkbar. Dies trifft auch auf das kommunale Bildungsmonitoring zu, bei dem die Zusammenführung und Nutzung vieler Daten aus unterschiedlichen Verantwortungsbereichen und Quellen erforderlich ist, um eine sinnvolle Steuerung von Ressourcen zu ermöglichen. Einige dieser Daten unterliegen jedoch datenschutzrechtlichen Bestimmungen und somit Grenzen für ihre Verwendung – aus gutem Grund, denn es geht darum, Grundrechte von Bürgerinnen und Bürgern zu schützen. Die Frage der zulässigen Nutzung solcher Daten für Zwecke der statistischen Auswertung, der Planung und Steuerung stellt sich daher in fast allen Projekten, und immer wieder tauchen dabei tatsächliche oder vermeintliche datenschutzrechtliche Hürden auf.

Diese Handreichung will Lösungswege im Umgang mit Datenschutz aufzeigen und den Fachleuten im Bildungsmonitoring hierfür Strukturwissen des Datenschutzrechtes vermitteln. Was ist beim Bildungsmonitoring zu berücksichtigen, wenn vorhandene Datenbestände genutzt oder neue Daten erhoben werden sollen?

Jede Kommune, Körperschaft oder sonstige Behörde hat einen **Datenschutzbeauftragten. Dieser ist der erste Ansprechpartner** für jede Problemlösung und sollte deshalb frühzeitig – also bereits in der Planungsphase – einbezogen werden. So können Hindernisse frühzeitig erkannt und überwunden werden.

Das Datenschutzrecht wandelt sich. Mit der EU-Datenschutzgrundverordnung wird erstmals europaweit einheitlich das Datenschutzniveau für alle Unternehmen und Behörden geregelt. Einige der hier angesprochenen Regeln werden in den nächsten Jahren angepasst werden müssen. Die Grundprinzipien des deutschen Datenschutzrechtes finden sich jedoch in dieser

Datenschutzgrundverordnung wieder und werden Bestand haben.

Darf ich das?
Ist Datenschutz einfach? Sicherlich nicht. Aber es ist auch zu einfach, Datenschutzregeln als Vorwand für jedes „Nein“ zu gebrauchen, wenn es um die Frage geht, ob personenbezogene Daten erhoben, genutzt, verarbeitet oder weitergegeben werden dürfen. Das Datenschutzrecht verbietet nicht den Umgang mit personenbezogenen Daten, sondern es regelt diesen aktiv im Interesse der Betroffenen. Datenschutzrecht schützt die Daten von Menschen vor einem möglichen Missbrauch, nicht vor dem sinnvollen Gebrauch.

Der Weg zur datenschutzrechtlichen Beantwortung der Frage „Darf ich das?“ ist einfach: „Nur“ fünf Schritte – und wir sind schon (fast) am Ziel. Nachdem in einem ersten Schritt grundsätzlich die Frage nach der Anwendbarkeit des Datenschutzrechtes zu klären ist, geht es um **die „vier W“**, nämlich: **Wer** verarbeitet, **welche** Daten zu **welchem** Zweck auf **welcher** Rechtsgrundlage?

1.1 Ist das Datenschutzrecht überhaupt anwendbar?

Das Datenschutzrecht findet nur Anwendung, wenn personenbezogene Daten im Sinne des Gesetzes verarbeitet werden.

Personenbezogene Daten sind Einzelangaben über bestimmte oder bestimmbare natürliche Personen. Es geht also in der Regel nur um Daten der Kinder, ihrer Eltern oder auch der Mitarbeitenden. NICHT umfasst sind beispielsweise: Betriebs- oder Unternehmensdaten, statistische Daten wie die Höhe der Ausgaben einer Kommune für Bildung oder andere ausschließlich anonyme statistische Zahlen.

Alle Einzelangaben, die direkt oder indirekt (beispielsweise durch die Hinzuziehung weiterer Informationsquellen) einer natürlichen Person zugeordnet werden können, sind personenbezogene Daten und dürfen nur verwendet werden, wenn es gesetzlich erlaubt ist. Das heißt, dass auch ursprünglich personenbezogene Daten, die wirksam anonymisiert wurden, ab dem Zeitpunkt der Anonymisierung nicht mehr unter das Datenschutzrecht fallen.

Damit sind alle in Publikationen oder auf offiziellen Webseiten veröffentlichte Daten der kommunalen, der Bundes- oder Landesstatistik in der Regel keine personenbezogenen Daten.

Die datenschutzrechtliche Verantwortung für die Zulässigkeit der Veröffentlichung dieser Daten – und damit der Zulässigkeit der weiteren Nutzung dieser Daten durch Dritte – trägt allein die veröffentlichende Stelle.

FALLBEISPIEL 1

Eine Schule erhebt die Schülerdaten „Anschrift und Alter“ zur Erfüllung der Aufgabe „Unterrichtsdurchführung“. Mit Ende des Schulbesuchs ist dieser Zweck erfüllt, die Daten sind zu löschen. Nun will die Kommune zu Planungszwecken für die Berufsbildung wissen, wie viele Schülerinnen und Schüler in welchem Alter sind.

Zu diesem Zweck übermittelt die Schule anonyme Daten an die Kommune:
43 Kinder sind 16 Jahre alt.

➜ Das Datenschutzrecht findet keine Anwendung, die Übermittlung ist zulässig.

Wenn nur ein Kind in der Schule 17 Jahre alt ist, wäre eine Übermittlung der Daten unzulässig, da eine Zuordnung zu einer Person möglich ist. Um dieses Problem zu umgehen wäre die Bildung einer Gruppe möglich: 44 Kinder sind 16 –17 Jahre alt.

Wenn das Datenschutzrecht angewendet werden muss, stellen sich **folgende nächste Fragen**:

1.2 Die vier „W"-Fragen

WER verarbeitet die Daten? 1.

Das Datenschutzrecht wendet sich immer an die jeweilige „verantwortliche Stelle". Wer ist verantwortlich für die Datenverarbeitung? Dabei geht es nicht um Technik oder Finanzen, sondern um die Frage: „Der Erfüllung wessen Aufgabe dient die Datenverarbeitung?" Anknüpfungspunkt ist immer die gesetzlich definierte Aufgabe der jeweiligen Stelle, die die Daten erstmalig erhebt bzw. erhoben hat. Die Verantwortlichkeit kann aber natürlich wechseln.[1]

FALLBEISPIEL 2

Eine Schule erhebt die Schülerdaten „Anschrift und Alter" zur Erfüllung der Aufgabe „Unterrichtsdurchführung".

➜ **Mit Ende des Schulbesuchs ist dieser Zweck erfüllt, die Daten sind zu löschen.**

Das Schulamt will im Rahmen seiner gesetzlichen Aufgaben die Anschriftendaten nun nutzen, um die Eltern der Schüler über eine bevorstehende Schulschließung und deren Folgen zu unterrichten. Zu diesem Zweck übermittelt die Schule die Daten an das Schulamt.

Ab Zugang der Daten beim Schulamt ist nun dieses die datenschutzrechtlich verantwortliche Stelle für die Datenverarbeitung. Mit der Änderung des Zwecks der Datenverarbeitung wechselt hier auch die Verantwortlichkeit – und damit die Zuständigkeit für die datenschutzrechtlich zulässige Nutzung und spätere Löschung der Daten – von der Schule auf das Schulamt.

[1] Mit der neuen EU-Datenschutzgrundverordnung wird man hierfür ab 2018 auch andere Lösungen als sog. „gemeinsam Verantwortliche" finden können.

Hieraus ergibt sich die nächste Frage: WELCHES DATENSCHUTZRECHT ist anwendbar? 2.

Anhand der verantwortlichen Stelle unterscheidet das Datenschutzrecht grundsätzlich zwischen „öffentlichen" und „nicht-öffentlichen Stellen". Die Unterscheidung zwischen Behörden als öffentlicher Stelle und Unternehmen als nicht-öffentlicher Stelle fällt noch relativ leicht. Es gibt hier aber viele Mischformen mit grundsätzlichen Unterschieden zu beachten. Nach dem jeweiligen Träger entscheidet sich das Spielfeld und somit auch die Frage, welches Datenschutzrecht anwendbar ist.

In Frage kommen
a) spezialgesetzliche Vorschriften (z.B. für konfessionelle Einrichtungen oder Krankenhäuser),
b) die Landesdatenschutzgesetze (für kommunale oder Landesbehörden) oder
c) das Bundesdatenschutzgesetz (für Bundesbehörden und Unternehmen, Vereine sowie Verbände des öffentlichen Rechts).

Da immer die Rechtsvorschrift vorrangig Anwendung findet, die den konkreten Sachverhalt spezieller (also konkreter) regelt, reicht die Kenntnis des Bundes- oder Landesdatenschutzgesetzes nicht aus, um alle Fälle richtig zu beurteilen. Alle gesetzlichen Regelungen folgen aber im Grunde vergleichbaren Regeln und Prinzipien.

Innerhalb der jeweiligen gesetzlichen Regelungen sind einige Sonderfälle besonders zu berücksichtigen – so die sogenannten „besonderen Arten personenbezogener Daten".

WELCHE DATEN werden verarbeitet? 3.

Je nach der Art der zu verarbeitenden Daten sind unterschiedliche Regelungen zu beachten.

Die moderne Informations- und Kommunikationstechnik führt aus mehreren Gründen dazu, dass immer mehr Daten „personenbeziehbar" sind oder werden, also einer konkreten natürlichen Person zugeordnet werden können. So werden Daten zu personenbezogenen Daten, deren Personenbezug der einzelne Verwender vielleicht gar nicht erkennen kann – wie zum Beispiel die IP-Adresse eines Rechners bei der Nutzung des Internets.

Die allgegenwärtige Verfügbarkeit großer Datenmengen aus verschiedenen Lebensbereichen erhöht somit die Gefahr der Personenbeziehbarkeit von Daten.

Die möglichen negativen Auswirkungen einer rechtswidrigen Datenverarbeitung können sich nach der Art der verarbeiteten Daten erheblich unterscheiden.

Deshalb schützt das Datenschutzrecht „besondere Arten personenbezogener Daten" auch besonders.

Angaben über
- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,

- Gewerkschaftszugehörigkeit,
- Gesundheit oder Sexualleben

haben ein höheres Potenzial, in die Freiheitsrechte des Einzelnen einzugreifen, als andere Arten von Daten. Für diese Daten gelten deshalb (oft) höhere Anforderungen, als für andere personenbezogene Daten.

Mit Hilfe der jeweiligen gesetzlichen Norm kann nun die Frage geprüft werden, ob die konkret vorgesehene Datenverarbeitung zulässig ist.

ZU WELCHEM ZWECK werden Daten verarbeitet? 4.

Der Zweck einer Datenverarbeitung bestimmt deren rechtliche Zulässigkeit (Zweckbindungsprinzip). Alle datenschutzrechtlichen Normen knüpfen an diesen konkreten Zweck an. Man kann also nicht sagen, dass eine bestimmte Datenkategorie immer zulässig oder unzulässig ist: Natürlich darf und soll ein Arzt Gesundheitsdaten personenbezogen erheben und nutzen, ein Personalchef im Einstellungsgespräch aber in der Regel nicht.

Der Zweck der Datenverarbeitung muss vor Beginn konkret festgelegt werden und zulässig sein.

„Wofür brauchen Sie diese Angaben?“ – mit dieser einfachen Frage beginnt die Prüfung der Zulässigkeit jeder Datenübermittlung an Dritte – also alle, die nicht zur verantwortlichen Stelle gehören.

Personenbezogene Daten „auf Vorrat“ zu sammeln, ohne bei der Erhebung bereits festzulegen, wofür diese Daten genutzt werden sollen, macht einen Schutz vor Missbrauch unmöglich. Eine Datenverarbeitung ohne einen konkret bestimmten zulässigen Zweck ist eine sogenannte Vorratsdatenspeicherung („Es könnte ja sein, dass man die Daten mal gebrauchen kann…“) und gesetzlich sowie verfassungsrechtlich unzulässig (wie das Bun-

FALLBEISPIEL 3

Die Schule erhebt die Schülerdaten „Anschrift und Alter“ zur Erfüllung der Aufgabe „Unterrichtsdurchführung“. Dieser Zweck bestimmt die zulässige Nutzung der Daten während des Schulbesuchs. Mit Ende des Schulbesuchs ist dieser Zweck erfüllt, die Daten sind zu löschen.

Die Schule will die Anschriftendaten nun an die Kommune übermitteln, „falls man diese Daten mal für die Ortschronik oder ein Jahrgangstreffen gebrauchen kann”.

➜ Für eine solche Übermittlung gibt es keine Rechtsgrundlage, sie ist somit unzulässig.

desverfassungsgericht und der europäische Gerichtshof mehrfach betonen mussten).

Werden Daten zu einem bestimmten Zweck erhoben, dürfen sie nur für diesen Zweck genutzt werden und nicht für andere Zwecke – und seien diese noch so begrüßenswert. Dies gilt vor allem immer dann, wenn sich die Datenerhebung auf eine konkrete und informierte Einwilligung der Betroffenen bezieht. Bei einer solchen Einwilligung muss wie bei jeder Erhebung der Zweck der vorgesehenen Datenverarbeitung benannt werden. Dieser kann nachträglich nicht geändert werden. Werden beispielweise Schülerindividualdaten für Leistungsbewertungen mit Einwilligung von Schulkindern bzw. ihrer gesetzlichen Vertreterinnen und Vertreter erhoben und ausgewertet, dürfen zwar die veröffentlichten anonymi-

FALLBEISPIEL 4

Die Kommune will zur Durchführung einer Wissensolympiade die Anschriften der drei besten Matheschülerinnen und -schüler von den ortsansässigen Schulen bekommen, um sie zu der Veranstaltung einzuladen.

Hier handelt es sich um personenbezogene Daten der Schülerinnen und Schüler: Anschrift und Leistungsdaten. Die Weitergabe der Daten an die Kommune wäre eine „Übermittlung personenbezogener Daten an einen Dritten“, denn die Kommune wird hier nicht im Rahmen ihrer Aufgabe als Schulträger tätig. Damit ist die Übermittlung nur mit einer gesetzlichen Erlaubnis zulässig. Diese könnte sich aus einem Spezialgesetz – zum Beispiel dem Schulgesetz – ergeben. Eine solche Rechtsvorschrift gibt es jedoch nicht. Für den Zweck der Durchführung von Veranstaltungen der Kommune hat der Gesetzgeber der Schule keine gesetzliche Erlaubnis eingeräumt.

Also gibt es nur noch eine andere Möglichkeit: **die Einwilligung der Betroffenen** – also der Schülerinnen und Schüler. In diesem Fall übermittelt die Schule die Daten nur dann, wenn ihr die Einwilligung der Betroffenen bzw. ihrer gesetzlichen Vertreter schriftlich vorliegt. Die Schule ist verantwortliche Stelle für die Datenverarbeitung und muss deshalb die Einwilligung auch im Zweifel zum Nachweis der Erlaubnis vorlegen können.

Oder die Schule übergibt die Einladungen selbst – das wäre nicht nur der einfachere, sondern auch der datenschutzrechtlich „saubere“ Weg. Wenn die Schülerinnen und Schüler sich dann bei der Kommune angemeldet haben, ist die Kommune die verantwortliche Stelle für die Datenverarbeitung zum Zweck der Durchführung der Veranstaltung.

sierten Daten auch für ein Bildungsmonitoring verwendet werden, nicht jedoch die ursprünglichen Daten. Diese müssten ohnehin nach der Auswertung gelöscht worden sein.

Auch eine solche zweckändernde Übermittlung ist nur möglich, wenn der ursprüngliche Zweck der Datenerhebung zulässig war, der neue Zweck nach einem Gesetz zulässig wäre und die Stelle die Daten an die andere Stelle übermitteln darf.

Jede Datenübermittlung an Dritte braucht zu ihrer Zulässigkeit drei verschiedene Rechtsgrundlagen:

Stelle A	erhebt die Daten auf Grund der gesetzlichen Erlaubnis	„Rechtsgrundlage 1"
Stelle B	will die Daten für die Erfüllung der gesetzlichen Aufgabe nutzen	„Rechtsgrundlage 2"
Stelle A	übermittelt die Daten an die Stelle B aufgrund einer gesetzlichen Erlaubnis (Übermittlungsnorm)	„Rechtsgrundlage 3"

Ohne eine Übermittlungsnorm wäre eine Übermittlung der Daten durch die Stelle A rechtswidrig, selbst wenn die Stelle B die Daten selbst erheben dürfte. Hier würde gegen einen Transparenzgrundsatz verstoßen – die Bürgerinnen und Bürger könnten über kurz oder lang nicht mehr wissen, wer welche Daten über sie gespeichert hat.

Mit der Klärung dieser fünf Fragen wird festgelegt, ob das Datenschutzrecht überhaupt angewendet werden muss und welches Datenschutzrecht konkret Anwendung findet. In den folgenden Kapiteln soll nun Bezug darauf genommen werden, welche Relevanz diese Fragen und das Datenschutzrecht für ein Bildungsmonitoring haben und welche Folgen hieraus entstehen können. Zudem geht es darum, mögliche Stolpersteine für ein Bildungsmonitoring aus der Sicht des Datenschutzes frühzeitig zu antizipieren und – soweit möglich – zu vermeiden. Darüber hinaus werden Fragen der Datenverarbeitung und des Schutzes der Daten aufgegriffen.

2. Rechtlicher Rahmen beim Umgang mit Daten im Bildungsmonitoring

2. Rechtlicher Rahmen beim Umgang mit Daten im Bildungsmonitoring

In den meisten Fällen verwendet (kommunales) Bildungsmonitoring keine personenbezogenen Daten. Wenn jedoch im Rahmen des (kommunalen) Bildungsmonitorings personenbezogene Daten erhoben, genutzt oder verarbeitet werden sollen und dieser Zweck von einer Rechtsgrundlage gedeckt ist – also ein vom Parlament verabschiedetes Gesetz die Verarbeitung von personenbezogenen Daten durch die verantwortliche Stelle zu diesem Zweck erlaubt – dann steht dem Vorhaben schon fast nichts mehr im Wege.

Dieses Gesetz gilt es zu finden. Die meisten Standardprozesse von Datenverarbeitungen sind gesetzlich geregelt – und damit auch die Voraussetzungen und Rahmenbedingungen der dafür erforderlichen Datenverarbeitung.

Allerdings wird sich das Bildungsmonitoring in der Regel auf von verschiedenen Stellen bereits zulässig erhobene Daten stützen. Dabei ist diese Datennutzung im Rahmen eines Bildungsmonitorings für gewöhnlich für die Erfüllung der ursprünglichen Aufgabe des Trägers im rechtlichen Sinne nicht erforderlich. Die Betreuung in der Kindertagesstätte oder die Durchführung von Unterricht ist auch ohne Bildungsmonitoring möglich. Das bedeutet aber, dass der im vorhergehenden Kapitel behandelte Fall einer sogenannten „zweckändernden Nutzung“ durchaus vorkommen kann, d.h. der Fall, dass die für einen konkreten Zweck erhobenen personenbezogenen Daten nun für einen anderen Zweck – das Monitoring – genutzt werden sollen. Auch wenn die angestrebte Qualitätssicherung oder -verbesserung durch das Monitoring im Zusammenhang mit dem ursprünglichen Zweck steht, so wäre die Nutzung der Daten hierfür allenfalls hilfreich, aber nicht unbedingt notwendig. Daher ist es zwingend erforderlich, dass diese Zweckänderungen entweder gesetzlich erlaubt sind, eine Einwilligung aller Betroffenen vorliegt oder ausschließlich eine anonymisierte Verarbeitung stattfindet.

Daher ist der im Bildungsbereich zuständige Landesgesetzgeber gut beraten, die Nutzung personenbezogener Daten für das Bildungsmonitoring gesetzlich zu regeln. Ein kommunaler Beschluss kann eine fehlende Rechtsgrundlage ebenso wenig ersetzen, wie eine Anweisung durch einen Vorgesetzten.

2.1 Datenübermittlung in Amtshilfe ist immer unzulässig!

Im Rahmen von Bildungsmonitoring stellt sich aber nicht nur die Frage, ob die Nutzung vorhandener personenbezogener

Daten eine Zweckänderung darstellt, sondern auch, ob ggf. die Übermittlung und Zusammenführung personenbezogener Daten beispielsweise von einem Amt durch ein anderes zulässig ist.

Bereits mit seinem grundlegenden Urteil zum Datenschutz als Grundrecht im Jahr 1983 hat das Bundesverfassungsgericht festgestellt, dass es verfassungsrechtlich geboten ist, einen „amtshilfefesten Schutz der Daten" zu gewährleisten. Diese Anforderungen sind sowohl im allgemeinen Datenschutzrecht, als auch im Sozialdatenschutz und allen anderen spezialgesetzlichen Regelungen umgesetzt. Eine Datenübermittlung im Rahmen der Amtshilfe ist zwischen Behörden und auch innerhalb einer Behörde nur zulässig, wenn es gesetzlich ausdrücklich erlaubt ist. Dabei braucht es eine zweiseitige Erlaubnisnorm: Die übermittelnde Stelle muss die Daten haben dürfen, übermitteln dürfen und die empfangende Stelle muss die Daten erheben dürfen. Diese Fälle sind spezialgesetzlich abschließend geregelt. Als verantwortliche Stelle ist dabei die kleinste funktionale Einheit zu verstehen, die mit der Erfüllung der jeweiligen Aufgabe betraut ist. Das kann auch mal ein einzelner Beamter sein, wenn nur dieser für eine bestimmte Aufgabenerfüllung zuständig ist.

Jede Weitergabe von personenbezogenen Daten an andere Mitarbeiter derselben Behörde, aber außerhalb der funktional zuständigen Stelle, ist als Übermittlung von personenbezogenen Daten an Dritte nur bei Vorliegen einer gesetzlichen Erlaubnis zulässig. Dies schließt die Übermittlung von Daten an Vorgesetzte ein – auch diese dürfen die Daten nicht für einen anderen Zweck verwenden. Dies stellt besondere Anforderungen an Mitarbeiter kleiner Verwaltungen, die mehrere Aufgaben wahrnehmen – ohne gesetzliche Befugnis dürfen sie ggf. Informationen zur Erfüllung der einen Aufgabe nicht verwenden, die sie in Wahrnehmung einer anderen Aufgabe zulässigerweise erhalten haben.

TIPP *Wenn ein Mitarbeiter eines anderen Amtes oder einer anderen Behörde die Mitteilung von Daten verlangt, die er zur Erfüllung seiner Aufgaben benötigt, fragen Sie diesen nach der Rechtsvorschrift, die es Ihnen erlaubt, diese Daten herauszugeben. Und dann lesen Sie die Rechtsvorschrift – oder fragen Sie Ihren Datenschutzbeauftragten.* ***Es ist immer ein Parlamentsgesetz erforderlich!***

Wenn es einen Bedarf für die Nutzung von personenbezogenen Daten zu einem gesellschaftlich akzeptablen Zweck gibt, ist es die Aufgabe des Parlamentes, für die erforderliche Datenverarbeitung eine verfassungskonforme Rechtsgrundlage zu schaffen. Diese Aufgabe hat das Bundesverfassungsgericht den Parlamenten bereits 1983 mit guten Gründen ins Hausaufgabenheft geschrieben (das sog. Volkszählungsurteil).

Ein Parlament entscheidet, ob und unter welchen Bedingungen das grundgesetzliche Recht jedes Einzelnen, selbst zu bestimmen, wer welche Daten von ihm bekommt, eingeschränkt werden darf.

Nur wenn das öffentliche Interesse schwerer wiegt als das Persönlichkeitsrecht der Bevölkerung, und wenn das Gesetz Maßnahmen zum Schutz dieser Daten vor einem Missbrauch anordnet, wird es einer verfassungsgerichtlichen Prüfung standhalten. Das vom Bundesverfassungsgericht aufgestellte Prinzip, jede Datenerhebung sei verboten, es sei denn, ein Gesetz erlaubt diese (sog. Verbot mit Erlaubnisvorbehalt), führt damit für die Praktizierenden zu einer Suchaufgabe: Die einschlägigen Datenschutzvorschriften finden sich oft nicht nur an einer Stelle, sondern an vielen Stellen.

TIPP *Erst wenn Sie eine spezialgesetzliche Rechtsgrundlage ausschließen können, können Sie zu einem weiteren Mittel greifen: die Einwilligung der Betroffenen. Diese ist aber rechtlich anspruchsvoller, als viele Praktikerinnen und Praktiker meinen. Jede Einwilligung kann jederzeit wieder zurückgezogen werden – und dann besteht eine Löschpflicht. Greifen Sie deshalb nicht leichtfertig und ohne „Not" auf eine Einwilligung zurück.*

2.2 Bildungsmonitoring als Aufgabe der Kommunen

Bildungsmonitoring als kontinuierlicher, überwiegend datengestützter Beobachtungs- und Analyseprozess des Bildungssystems insgesamt sowie einzelner seiner Bereiche dient dem Zweck der Information von Bildungspolitik und Öffentlichkeit über Rahmenbedingungen, Verlaufsmerkmale, Ergebnisse und Erträge von Bildungsprozessen (so die Definition des Projektes KBM – Kommunales Bildungsmonitoring – im Rahmen des BMBF-Programms „Lernen vor Ort").

Dieses Ziel soll im Wesentlichen durch die Nutzung der vorhandenen Datenbestände der amtlichen Statistik und durch Datengewinnungsstrategien bzw. Strategien zur kommunalspezifischen Entwicklung von Kennzahlen und Indikatoren erreicht werden, wenn die verfügbaren Daten nicht ausreichen.

Die amtliche Statistik wurde bereits im Volkszählungsurteil des Bundesverfassungsgerichtes im Jahr 1983 mit besonderen Rechten ausgestattet, denen aber auch besondere Pflichten für die Organisation und Beschränkungen bei der Datenverwendung entsprechen.

Für den öffentlichen Bereich in NRW sind diese Anforderungen an die kommunale Statistik in den §§ 31 und 32 Datenschutzgesetz Nordrhein-Westfalen (im Weiteren: DSG NRW) gesetzlich definiert.

2.3 Nutzung vorhandener Daten der Verwaltung

In der Praxis geht es in der Regel um die Frage, ob Daten für statistische Auswertungen genutzt werden dürfen, die für einen anderen Zweck erhoben wurden.

Die Daten, die in kommunalen Fachdiensten im Rahmen ihrer Zuständigkeit zulässi-

gerweise erhoben und gespeichert werden, dürfen generell nur für den Zweck genutzt werden, für den sie erhoben wurden. Sie unterliegen dem sog. internen Trennungsgebot. Ein Fachdienst darf diese Daten keinem anderen Fachdienst zugänglich machen, auch wenn beide der gleichen Kommune oder dem gleichen Fachamt angehören, vgl. § 13 Abs. 1 Satz 2 DSG NRW.

Zu dieser Regel sieht das Datenschutzgesetz aber bestimmte Ausnahmen vor, die in § 13 Abs. 2 Satz 1 DSG NRW abschließend aufgezählt sind.

Das DSG NRW stellt aber auch in § 13 Abs. 3 klar:
„Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient."

Damit wurde gesetzgeberisch definiert, dass die Nutzung von Verwaltungsdaten für Zwecke der Organisationsuntersuchung vom ursprünglichen Erhebungszweck umfasst ist. Somit können alle in der Kommune zur Aufgabenerfüllung anfallenden Daten auch für Organisationsuntersuchungen genutzt werden.

Zu diesem Zweck ist gem. § 14 Abs. 1 DSG NRW die Übermittlung dieser Daten innerhalb des öffentlichen Bereichs (also innerhalb der Kommune, aber auch von einer Kommune an eine andere Kommune oder von einer Landeseinrichtung an die Kommune) „zur Wahrnehmung von Aufgaben nach § 13 Abs. 3" zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

Dreh- und Angelpunkt der datenschutzrechtlichen Zulässigkeit ist mithin die Erforderlichkeit der Daten zur Erfüllung der Aufgabe „Organisationsuntersuchung". Mit einem Konzept zum kommunalen Bildungsmonitoring im Sinne einer „Organisationsuntersuchung" – am besten abgesichert durch einen Beschluss der Kommunalvertretung – definiert die Kommune, welche vorliegenden Daten zur Umsetzung des Bildungsmonitorings erforderlich sind.

Ist diese Voraussetzung erfüllt, können alle erforderlichen Daten sowohl einer einzelnen Stelle innerhalb der Kommune, aber auch einer anderen öffentlichen Stelle zum Zweck des Bildungsmonitorings übermittelt werden, um dann dort zu anonymisierten Daten weiterverarbeitet zu werden. Diese Daten unterliegen ab diesem Zeitpunkt einer besonderen Zweckbindung: Sie dürfen ausschließlich für das Bildungsmonitoring genutzt werden.

Das interne Trennungsgebot verbietet die Übermittlung von personenbezogenen Daten von einem Fachamt an ein anderes Fachamt, solange es hierzu keine gesetzliche Erlaubnis gibt. Die Nutzung der Daten für Zwecke der statistischen Auswertung oder der Organisationsuntersuchung bildet hiervon eine Ausnahme: Die Daten dürfen übermittelt werden, aber nur als „Einbahnstraße".

In Nordrhein-Westfalen ist die Zulässigkeit der Nutzung von Verwaltungsdaten für die Erstellung von Statistiken detailliert in den §§ 31 und 32 DSG NRW geregelt:
„Für die Erstellung von Statistiken dürfen öffentliche Stellen personenbezogene Daten weiterverarbeiten, soweit diese bei der rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben angefallen sind. Die Veröffentlichungen dürfen keine Angaben enthalten, die den Bezug auf eine bestimmte Person zulassen."

In § 32 DSG NRW werden dann konkrete Anforderungen an die technische und personelle Ausgestaltung der „für die Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände" – sog. „Abgeschottete Statistikdienststellen" – definiert. Diese müssen „organisatorisch und räumlich von den anderen Verwaltungsstellen der Körperschaft getrennt" sein, mit eigenem Personal ausgestattet (das mit keinen anderen Verwaltungsaufgaben betraut sein darf, Gewähr für Zuverlässigkeit und Verschwiegenheit bietet und auf das Statistikgeheimnis verpflichtet werden muss) und gegen den Zutritt Unbefugter besonders geschützt sein.

2.4 Eigenerhebung auf Basis der Einwilligung der Betroffenen

Stehen keine oder nicht alle erforderlichen Daten in der Verwaltung zur Verfügung, kann alternativ auf die Eigenerhebung solcher Daten zurückgegriffen werden. Hier gilt es, den sog. Direkterhebungsgrundsatz zu beachten: Daten sind grundsätzlich bei den Betroffenen zu erheben (direkt) und nicht bei Dritten (das wäre dann eine Übermittlung von Daten).

Nach den Regelungen der Datenschutzgesetze ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das jeweilige Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die Betroffenen eingewilligt haben. Die Anforderungen an die Wirksamkeit der Einwilligung ist nach vielen Missbrauchsfällen durch den Gesetzgeber sehr konkret beschrieben worden.

Die Betroffenen (bzw. im Falle von Minderjährigen die gesetzlichen Vertreterinnen und Vertreter) müssen vollumfänglich über die geplante Datenverwendung unterrichtet sein, die Einwilligung muss eindeutig und freiwillig sein. Voraussetzung für die Wirksamkeit ist die Möglichkeit für die Betroffenen, die Einwilligung jederzeit zu widerrufen. Die Einwilligung muss schriftlich erfolgen.

TIPP *Regeln Sie immer wiederkehrende Fälle von Datenerhebungen auf Einwilligungsbasis möglichst einheitlich im Rahmen der Erarbeitung der Verfahrensbeschreibungen (siehe Kapitel 3.2). Nach einer Abstimmung mit den zuständigen Datenschutzbeauftragten schaffen Sie somit Handlungssicherheit für Mitarbeiterinnen und Mitarbeiter sowie für alle Betroffenen.*

3. Bedingungen für eine zuverlässige Datenverarbeitung im Bildungsmonitoring

3. Bedingungen für eine zulässige Datenverarbeitung im Bildungsmonitoring

Wenn eine Datenverarbeitung grundsätzlich zulässig ist, beginnt die zweite Hälfte der Arbeit: der Schutz der Daten vor einem möglichen Missbrauch. Dieser Schutz erfolgt einerseits durch organisatorische Vorgaben des Gesetzgebers, andererseits durch technische Maßnahmen.

Diese Vorgaben gelten in der Regel für eine gesamte Stelle oder auch nur für einzelne Bereiche mit besonderen Schutzbedarfen.

3.1 Bestellung einer/eines Datenschutzbeauftragten

Die Bestellung einer oder eines Datenschutzbeauftragten (und einer Stellvertretung im öffentlichen Bereich in NRW) muss schriftlich erfolgen. Diese Mitarbeiterinnen und Mitarbeiter müssen entsprechend geschult werden und nehmen ihre Aufgabe in fachlicher Unabhängigkeit wahr. Die Datenschutzbeauftragten sind der Leitung der Einrichtung unmittelbar zu unterstellen, dürfen alle Dateien und Aufzeichnungen zu Prüfzwecken einsehen und sind zur Verschwiegenheit über alle Angelegenheiten besonders verpflichtet. Sie sind für die regelmäßige Datenschutzschulung der Mitarbeiterinnen und Mitarbeiter verantwortlich. Sie prüfen und überwachen die Datenverarbeitung und nehmen die Vorabkontrolle der Verfahren vor – sind also für die Prüfung von geplanten Datenverarbeitungen vor deren Beginn zuständig. Deshalb sind die Datenschutzbeauftragten von Anfang an in die Konzeption geplanter Datenerhebungen, -verarbeitungen oder -übermittlungen einzubeziehen.

3.2 Erstellung eines Verfahrensverzeichnisses

Alle Verfahren automatisierter Verarbeitung personenbezogener Daten sind in einem so genannten Verfahrensverzeichnis zu dokumentieren. Verantwortlich dafür ist die Leitung der jeweiligen verantwortlichen Stelle. Es bietet sich an, alle internen Prozesse zu beschreiben, in denen personenbezogene Daten (z.B. von Kindern, Eltern bzw. Betreuenden und Mitarbeitenden einer Kindertagesstätte, Schulkindern und Eltern sowie Lehrenden oder Studierenden und Lehrpersonal) schriftlich, telefonisch oder elektronisch erfasst oder übermittelt werden.

Auch im Rahmen der Erstellung eines Bildungsmonitorings sollten alle Verfahren zur Erhebung oder Nutzung personenbezogener Daten für diesen Zweck in einem Verfahrensverzeichnis zusammengefasst werden.

Das Verfahrensverzeichnis muss gemäß § 8 DSG NRW folgende Mindestinhalte umfassen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens, einschließlich der eingesetzten Hard- und Software,
9. Fristen für die Sperrung und Löschung nach § 19 Abs. 2 und Abs. 3,
10. eine beabsichtigte Datenübermittlung an Drittstaaten nach § 17 Abs. 2 u. 3,
11. die begründeten Ergebnisse der Vorabkontrollen nach § 10 Abs. 3 Satz 1.

Für jedes Verfahren ist dessen Zweck zu beschreiben, welche Personengruppen davon betroffen sind – also wessen Daten verarbeitet werden – sowie die genutzten Datenkategorien (z.B. Namen, Anschriften, Telefonnummern, Prüfungsergebnisse). Aufzuführen sind alle Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können (z.B. Jugendamt, Versicherungen, Behörden), die Fristen für die Löschung der Daten und ob Daten in Staaten außerhalb des europäischen Wirtschaftsraumes übermittelt werden sollen. Diese Angaben sind für jedes Verfahren individuell aufzulisten. Abschließend sind alle technisch-organisatorischen Maßnahmen zum Schutz der Daten für einen möglichen Missbrauch durch Dritte vollständig aufzulisten, für öffentliche Stellen in NRW zusätzlich eine Beschreibung der Technik, die verwendete Hard- und Software und das begründete Ergebnis der Vorabkontrolle der Verfahren durch die Datenschutzbeauftragten der jeweiligen Behörde (weitere Hinweise siehe: www.ldi.nrw.de/Datenschutz/Datenschutzbeauftragte/Behoerdliche_Datenschutzbeauftragte). Damit ist die Verfahrensbeschreibung der Dreh- und Angelpunkt jeder datenschutzrechtlichen Zulässigkeitsprüfung.

TIPP *Jede neue Befragung oder Statistik sollte in dieser Weise dokumentiert werden und den zuständigen Datenschutzbeauftragten zur Kontrolle übergeben werden. Diese entscheiden dann über die Aufnahme in das Verfahrensverzeichnis.*

Das Verfahrensverzeichnis dient aber nicht nur der Selbstkontrolle, sondern kann jederzeit – so verlangen es die Datenschutzgesetze – durch die Aufsichtsbehörde angefordert werden. Dieses Verfahrensverzeichnis kann ohne den Teil mit den Sicherheitsmaßnahmen aber auch von jedermann zur Einsicht verlangt werden – es ist also ein öffentliches Verzeichnis.

Dabei kommt es nicht darauf an, ob die Daten der Anfragenden tatsächlich gespeichert werden. „Jedermann" meint tatsächlich jeden Menschen, ohne irgendein Interesse nachweisen oder dafür bezahlen zu müssen. Deshalb empfiehlt sich oft eine Veröffentlichung mit den Datenschutzhinweisen auf der eigenen Webseite, wenn vorhanden.

Gewährt die verantwortliche Stelle keinen Einblick in das Verfahrensverzeichnis oder hat sie gar keins, kann das bei nicht-öffentlichen Stellen als Ordnungswidrigkeit, bei öffentlichen Stellen mit einer Beanstandung der Landesdatenschutzbeauftragten geahndet werden.

TIPP *Die erstmalige Erhebung von Verfahren kann niemand „mal so nebenbei" erledigen. Diese sollte vielmehr in einen Qualitätssicherungsprozess einbezogen werden, fachkundig moderiert, gut strukturiert und von entsprechenden Fortbildungsmaßnahmen aller Mitarbeitenden begleitet sein. Hier sind die Träger in ihrer Verantwortung gefordert!*

3.3 Technisch-organisatorische Maßnahmen

Das Datenschutzrecht verlangt von jeder verantwortlichen Stelle die Einrichtung und Dokumentation von sogenannten technisch-organisatorischen Maßnahmen (TOM) zum Schutz der Daten vor Missbrauch.

Welche dies sein müssen, konkretisiert die jeweilige gesetzliche Vorschrift meistens nur als Zieldefinition (z.B. § 10 DSG NRW: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz). Welche konkreten Maßnahmen geeignet und erforderlich sind, kann und muss die verantwortliche Stelle selbst definieren.

Diese Festlegungen werden in dem sogenannten „nicht-öffentlichen Teil" des Verfahrensverzeichnisses, das nicht an jedermann herausgegeben werden darf, dokumentiert. Einige Landesdatenschutzgesetze verlangen von öffentlichen Stellen die Erstellung eines Sicherheitskonzeptes, so auch § 10 Abs. 3 DSG NRW.

Es ist grundsätzlich zu protokollieren, an wen Daten übermittelt wurden (Weitergabekontrolle), die Eingabe und Änderung von Daten ist ebenso zu protokollieren (Eingabekontrolle), bei der Beauftragung von Dienstleistern sind diese zu überwachen (Auftragskontrolle), Sicherheitskopien sind anzufertigen (Verfügbarkeitskontrolle) und die Daten voneinander getrennt aufzubewahren (Trennungskontrolle).

TIPP *Das Versenden personenbezogener Daten per E-Mail oder Fax sollte sich von selbst verbieten – es gibt keine unsicherere Transportmöglichkeit. Dagegen ist das Übermitteln auf eine Online-Plattform unbedenklich und sicher, wenn dies ssl-verschlüsselt erfolgt (https:\). Lassen Sie sich nicht von der Einfachheit der E-Mail verführen! Die meisten Standardprogramme bieten heute einen Schutz für die zu versendenden Dateien an, zum Beispiel die Kennwortvergabe. Nutzen Sie wenigstens diese Möglichkeit und teilen Sie dem Empfänger das Passwort dann zum Beispiel telefonisch mit.*

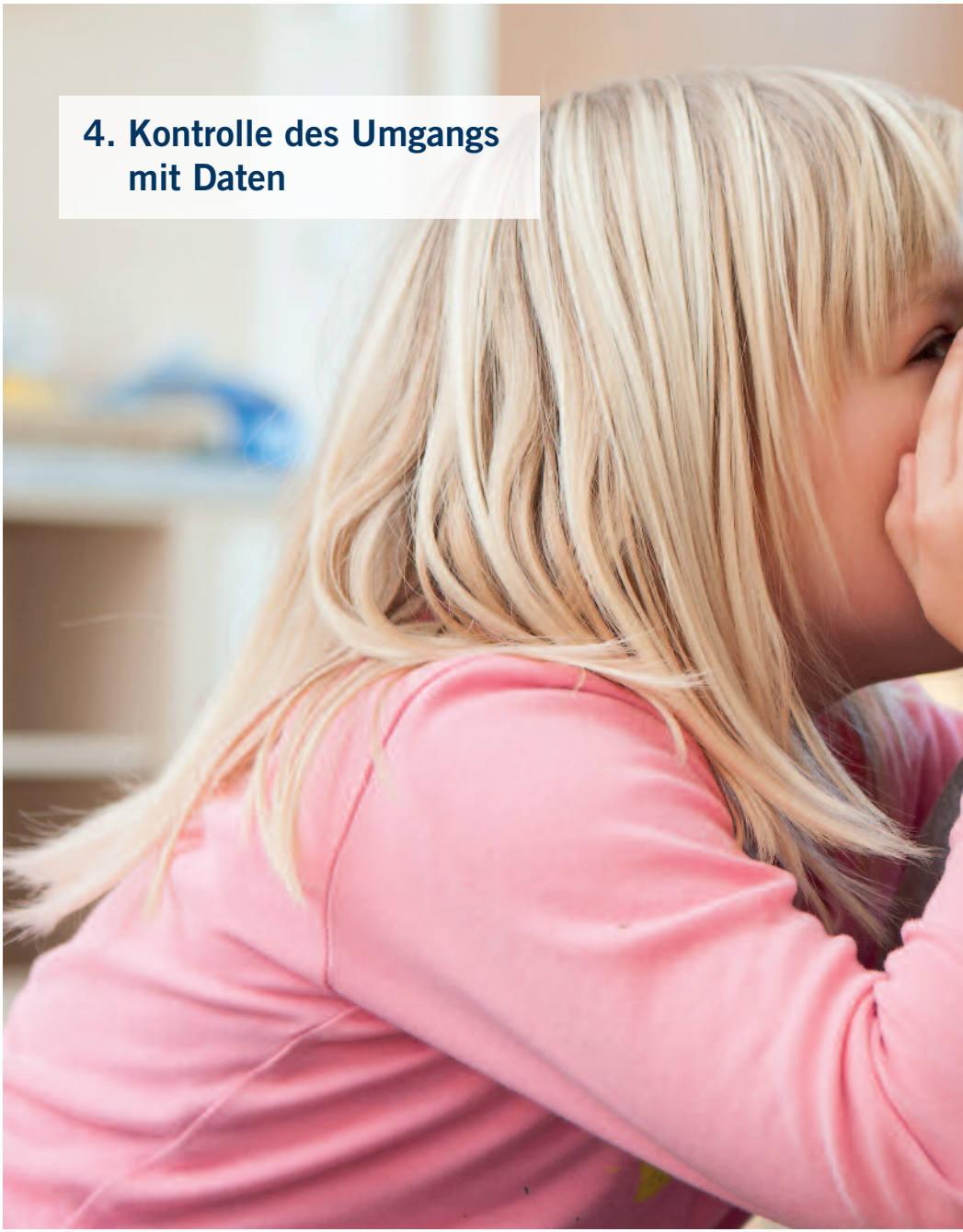
Stellt eine verantwortliche Stelle fest, dass bei ihr gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sein könnten (z.B. Diebstahl von Rechnern, Verlust von Laptops oder USB-Sticks), hat sie dies unverzüglich der zuständigen Aufsichtsbehörde, der zuständigen Datenschutzaufsichtsbehörde sowie den Betroffenen mitzuteilen.

TIPP *Beziehen Sie im Fall des Verlustes von Datenträgern immer den Datenschutzbeauftragten ein, damit dieser das Vorliegen der Anforderungen für eine Meldepflicht sofort prüfen kann.*

Diese Anforderungen klingen sehr umfassend und kompliziert – im Kern geht es aber einfach um den verantwortungsvollen Umgang mit Informationen: Wenn die Bildungsdokumentation in einem offenen Schrank im Flur steht, könnten alle Vorbeikommenden die Dokumentationen einsehen, mitnehmen oder zerstören. Deshalb sind diese zu verschließen oder dort zu lagern, wo nicht jeder unbeobachtet Zugang hat.

TIPP *Welche dieser Maßnahmen erforderlich sind, darf und muss die Leitung selbst einschätzen – unter fachlichen Gesichtspunkten. Die Maßnahmen sollten nach Rücksprache mit Ihren Datenschutzbeauftragten festgelegt werden und im Verfahrensverzeichnis dokumentiert werden. Das schafft Handlungssicherheit für die Mitarbeitenden und Rechtssicherheit für die Leitungen.*

4. Kontrolle des Umgangs mit Daten



4. Kontrolle des Umgangs mit Daten

4.1 Betroffene haben Rechte

Betroffene sind immer diejenigen, deren Daten verarbeitet wurden oder werden sollen. Alle, die Grund zu der Annahme haben, dass ihre Daten durch eine Einrichtung verarbeitet werden, haben zusätzlich zur Einsicht in das Verfahrensverzeichnis

- das Recht auf Anrufung der zuständigen Aufsichtsbehörde,
- bei Verletzungen eines Persönlichkeitsrechts Anspruch auf Schadensersatz,
- das Recht auf die Korrektur falscher und die Löschung unzulässig gespeicherter Daten,
- das Recht auf kostenfreie schriftliche Auskunft durch die verantwortliche Stelle

  > über die zur Person gespeicherten Daten, auch bezogen auf die Herkunft dieser Daten,

  > über die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und

  > über den Zweck der Speicherung.

4.2 Schutz vor Missbrauch – nicht vor Gebrauch!

Das Datenschutzrecht soll die Einzelnen vor einem möglichen Missbrauch der eigenen Daten schützen, vor einem unzulässigen Eingriff in die Rechte und Freiheiten. Aber auch diese sind nicht grenzenlos gewährleistet, wie es dem Datenschutz gern vorgeworfen wird. Wenn Leben und Gesundheit eines Menschen in Gefahr sind, stehen diese Rechte höher als das Recht auf informationelle Selbstbestimmung. Aber die Planung der Essensausgabe sollte keine Rechtfertigung für die ungeschützte und jahrelange Erhebung der Daten von tausenden Kindern sein. Die Effektivität der Verwaltung sollte nicht höher stehen als das Recht auf Privatsphäre. Beispielfälle finden sich unter www.projekt-datenschutz.de.

4.3 Was, wenn die Aufsichtsbehörde kommt?

Auch die Datenschutzaufsichtsbehörde hat in erster Linie beratende Funktion: Sie kann und soll vor allem Empfehlungen geben, Mängel feststellen und dem Landtag berichten. Dies macht sie in einem geregelten Verfahren von Anhörung der verantwortlichen Stelle, Prüfung und Stellungnahme. Der bzw. die Landesbeauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen, wenn es sich um unerhebliche Mängel handelt oder wenn deren Behebung sichergestellt ist.

Wenn sich also eine Entscheidung trotz einer gründlichen Prüfung, der Einbeziehung der betrieblichen bzw. behördlichen Datenschutzbeauftragten und trotz einer Verfahrensbeschreibung mit technisch-organisatorischen Sicherheitsmaßnahmen als falsch herausstellen sollte, muss der Landesdatenschutzbeauftragte keine Beanstandung aussprechen, wenn im Ergebnis der Prüfung durch ihn das beanstandete Verfahren eingestellt wird.

4.4 Keine Rechtsgrundlage, keine Einwilligung – was nun?

Eine Datenerhebung, -verarbeitung oder -übermittlung personenbezogener Daten ohne Rechtsgrundlage ist unzulässig. Das Bundesdatenschutzgesetz sieht dann einen Bußgeldrahmen von bis zu 300.000 € pro Fall (Datensatz einer betroffenen Person) vor. Wenn vorsätzlich und mit Bereicherungsabsicht gehandelt wurde, kann dies auch als Straftat mit bis zu zwei Jahren Haft geahndet werden.

Aber auch ohne eine solche Androhung ist die Wirkung einer öffentlichen Debatte über eine Beanstandung durch die Landesbeauftragten für Datenschutz oder einer Schlagzeile in der örtlichen Presse in ihrer Wirkung für das Bildungsmonitoring einer Kommune mit einem Bußgeld vergleichbar. Unzulässig erhobene Daten sind zu löschen, auch wenn diese nur deshalb unzulässig sind, weil die Einwilligungserklärung „im Kleingedruckten versteckt“ wurde. Wenn die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt wird, ist sie besonders hervorzuheben, § 4a Abs. 1 Satz 4 BDSG.

5. Und zum Schluss: Geht nicht – gibt's nicht!


511
of love...

5. Und zum Schluss: Geht nicht – gibt's nicht!

Probleme frühzeitig erkennen und lösen
Oft werden die Datenschutzbeauftragten erst gefragt, wenn alles „zu spät" ist. Wenn sich beispielsweise eine betroffene Lehrerin beschwert oder wenn die Eltern eines Schülers die Einwilligung zurückziehen. Dann können auch die besten Datenschutzbeauftragten keine Lösung mehr finden – eine unzulässige Datenerhebung muss gestoppt oder deren Ergebnisse gelöscht werden.

Viele Probleme lassen sich erkennen, wenn man den gesamten Prozess der geplanten Datenverarbeitung mit allen Beteiligten frühzeitig genau besprochen und durchdacht hat und dabei den roten Faden – „die 4 W" – nicht aus der Hand lässt:
1. Wer verarbeitet
2. welche Daten
3. zu welchem Zweck
4. auf welcher Rechtsgrundlage?

Die entscheidenden Weichen für die Zulässigkeit oder Unzulässigkeit werden bereits bei der Konzeption einer Maßnahme zur Datenerhebung durch die verantwortliche Stelle selbst gestellt.

Beim Umgang mit personenbezogenen Daten gibt es in der Praxis selten ein klares „Ja" oder „Nein". In der Regel wird die Antwort lauten: „Es kommt darauf an …", und der Datenschutzbeauftragte weiß, worauf es ankommt. Anhand einer detaillierten Analyse, welche Daten konkret erforderlich sind, zu welchem Zweck diese erhoben und verarbeitet werden sollen und unter wessen Verantwortung dies erfolgt, können die Bedingungen konkret formuliert werden.

Wenn dann noch alle Anforderungen an die Datenschutzorganisation einer Behörde (Datenschutzbeauftragte, Schulung der Mitarbeiterinnen und Mitarbeiter, Datenschutzanweisung, Verfahrensverzeichnis etc.) und an die Wirksamkeit der technisch-organisatorischen Maßnahmen erfüllt sind, steht dem Vorhaben in der Regel nichts entgegen.

In der Zusammenarbeit zwischen verschiedenen Akteuren sollten sich auch die beteiligten Datenschutzbeauftragten frühzeitig über die sich aus ihren jeweilig unterschiedlichen datenschutzrechtlichen Anforderungen ergebenden Bedingungen austauschen. Dann können gemeinsam akzeptable und rechtlich zulässige Lösungen gefunden werden.

Gute Datenschützerinnen und Datenschützer „machen" keine Probleme: Sie erkennen und lösen diese.

Über den Autor

Karsten Neumann
ehem. Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Als Jurist war der 1966 geborene Autor Koordinierungsreferent für Landtags- und Kabinettsangelegenheiten im Sozialministerium, Mitglied des Landtages und stellv. Mitglied im europäischen Ausschuss der Regionen. Seit dem Ausscheiden aus dem Amt als Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern berät er Unternehmen und Verbände in Datenschutzfragen, unter anderem als (externer) Datenschutzbeauftragter der Deutschen Kinderhilfe e.V., der Stiftung Mercator und RuhrFutur gGmbH.

Danksagung

Dafür, dass wir in der Person von Herrn Neumann einen so starken Partner für diese Zielsetzung gewinnen konnten, sind wir dankbar. Karsten Neumann ist als ehemaliger Landesdatenschutzbeauftragter des Landes Mecklenburg-Vorpommern ein ausgewiesener Datenschutz-Experte.

Karsten Neumann hatte bereits auf der Veranstaltung „Bildung zählt!“, bei der RuhrFutur gemeinsam mit dem Regionalverband Ruhr das Thema Bildungsmonitoring in seinen zahlreichen Facetten präsentiert hat, unter Beweis gestellt, dass er die schwierige und komplexe Thematik nicht nur außerordentlich versiert, sondern auch sehr anschaulich zu präsentieren versteht.

Auf seine Anregung hin durchlief die Entstehung dieses Textes mehrere Proof-of-Concept-Phasen, bei denen wir durch unterschiedliche Experten für Bildungsmonitoring aus der Region unterstützt wurden. An dieser Stelle möchten wir uns besonders für die Unterstützung von Prof. Hans Döbert, David Gehne (und seinem Team), Thomas Groos, Klaus Hermann, Volker Kersting sowie Martin Zilkens bedanken.

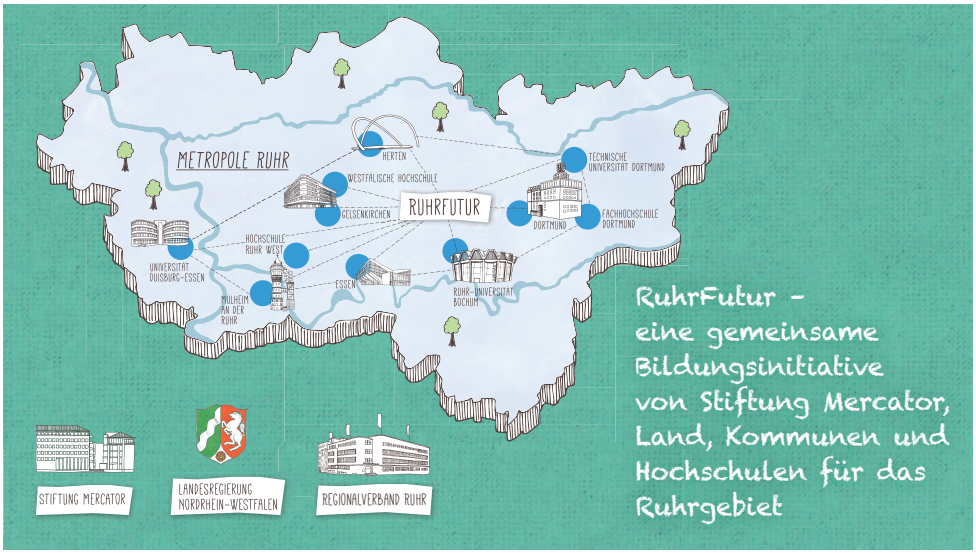
Dr. Markus Küpker und Julia Balke, RuhrFutur

Herausgeber

RuhrFutur gGmbH
Huyssenallee 52, 45128 Essen

Redaktion: Karsten Neumann,
Julia Balke/RuhrFutur, Dr. Markus Küpker/RuhrFutur, Daniel Laprell/RuhrFutur
Fotos: RuhrFutur gGmbH
Lektorat, Design und Realisation: brand.m GmbH, Gelsenkirchen

Essen, August 2017



RuhrFutur gGmbH
Huyssenallee 52
45128 Essen
Tel. +49 (0)201-177878-0
info@ruhrfutur.de
www.ruhrfutur.de