Der Digital-Dialog

Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zum Dialog-Papier

Der Digital-Dialog verfolgt das Ziel, eine Digitalstrategie „Rheinland-Pfalz digital" zu entwickeln. Der Datenschutz, aber auch die Informationsfreiheit und die Transparenz – wie die Einführung eines Transparenzgesetzes in der jüngsten Vergangenheit zeigt –, können wesentliche Beiträge auf dem Weg zu diesem Ziel leisten.

Da Digitalisierung immer den Umgang mit Daten betrifft, sind die Berührungspunkte und Querschnittsmengen zum Datenschutz erheblich. Dies zeigt bereits das seit einiger Zeit laufende Projekt „Digitale Dörfer" zur Belebung ländlicher Regionen. Insbesondere bei den Schwerpunkten Nahversorgung, Living Labs vor Ort in den Gemeinden und Dienste zur Vernetzung der Gemeinde spielt auch der Datenschutz eine wesentliche Rolle. Die datenschutzrechtlichen Grundsätze der Datenvermeidung und Datensparsamkeit bedürfen in diesem Kontext besonderer Berücksichtigung.

In der Folge sollen daher ausgewählte Themenbereiche erörtert werden, die aus Sicht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) im Zusammenhang einer rheinland-pfälzischen Digitalstrategie zukünftig eine besondere Rolle spielen könnten. Dies schließt nicht aus, dass in der weiteren Entwicklung dieser Strategie dann auch weitere Gesichtspunkte von Seiten des LfDI eingebracht werden.

Wirtschaft und Verwaltung in Rheinland-Pfalz sollen die Chancen der Digitalisierung nutzen, ohne ihre Risiken aus den Augen zu verlieren. Der LfDI verfolgt einen konstruktiven Ansatz, in dem aktuelle Entwicklungen aufgegriffen, bewertet und konstruktive Lösungen für rechtliche und praktische Probleme gesucht werden. Dies betrifft den Datenschutz, aber auch die Datensicherheit, die ein zentrales Element der übergreifenden IT-Sicherheit ist. Im Kern geht es darum, den Schutz des Rechts auf informationelle Selbstbestimmung und der Persönlichkeitsrechte effektiv zu gewährleisten und in einen schonenden und angemessenen Ausgleich mit anderen Rechtspositionen zu bringen, die im Prozess der Digitalisierung eine Rolle spielen. Das zugrundeliegende Problem, Privatheit in Zeiten der Digitalisierung neu zu bestimmen, kann hier nicht weiter angesprochen werden. Im Vordergrund sollen konkrete Rahmenbedingungen stehen, die aus Sicht des Datenschutzes die Digitalisierung anleiten.

Der rechtliche Rahmen ist in Bewegung. Das Bundesdatenschutzgesetz wird gerade neu gefasst, die Europäische Datenschutz-Grundverordnung ist verabschiedet und wird im Mai 2018 wirksam. Das Landesdatenschutzgesetz bedarf der Anpassung an diese geänderten Vorgaben. Aus diesem Grund werden im Folgenden allgemeine Grundlagen des Datenschutzrechts als Ausgangspunkt gewählt und weniger die einzelnen Rechtsvorschriften. Dabei ist zu berücksichtigen, dass zukunftsorientierte Lösungen mit der nach dem Wirksamwerden der Datenschutz-Grundverordnung geltenden Rechtslage vereinbar sein müssen. Eine wachsende Rolle werden dabei generelle Vorabprüfungsszenarien im Zusammenhang von Zertifizierung, Akkreditierung oder anderen Instrumenten für die Digitalisierung spielen. Sie betreffen sowohl die Wirtschaft wie die Verwaltung.

Ein weiterer Schwerpunkt wird auf den Datenschutz in der rheinland-pfälzischen Wirtschaft gelegt, wobei die positive Bedeutung des Datenschutzes besonders herausgehoben wird. In Rheinland-Pfalz gibt es zahlreiche Unternehmen, die im Gesundheitswesen aktiv sind. Da Gesundheitsdaten nicht nur gesammelt, sondern immer intensiver genutzt werden und es sich bei dem Gesundheitswesen nicht

zuletzt aufgrund des demografischen Wandels zugleich um ein gesellschaftlich wesentliches Feld handelt, soll dieses daher näher erörtert werden.

Digitalisierung in der Bildung betrifft eine Vielzahl von Menschen, kann vom Landesgesetzgeber wesentlich geregelt werden und soll daher ebenfalls besonders dargestellt werden.

Schließlich soll den technischen Aspekten, wie z.B. Verschlüsselung und Pseudonymisierung, besonderes Augenmerk geschenkt werden.

Diese vorgenannten ausgewählten Aspekte werden aus der Perspektive von Datenschutz und Datensicherheit beleuchtet und im Hinblick auf ihre Ausgestaltung und Entwicklung vor dem Hintergrund des Schutzes der Rechte der Bürgerinnen und Bürger befragt.

1. Datenschutzgrundverordnung und Instrumente zur Wahrung der Rechtsstellung des Einzelnen in der digitalen Welt

Die Verantwortung für den Datenschutz trägt derjenige, der die Daten erhebt und verarbeitet. Der Verantwortliche hat die rechtlichen Regelungen einzuhalten. Verantwortlich kann sowohl der Unternehmer wie die Behörde sein, die daher mit betrieblichen bzw. behördlichen Datenschutzbeauftragten ihre konkreten Verantwortlichkeiten prüfen und wahrnehmen. Angesichts der Komplexität von Digitalisierung sind die Herausforderungen oft nur kooperativ zu bewältigen. Die Instrumente, die dafür sorgen sollen, dass Datenschutzverletzungen gar nicht erst vorkommen, sind daher oft auf Kooperation angelegt. Die Vermeidung von Verstößen bedarf eigener Konzepte. Proaktiver Datenschutz unterstützt den Verantwortlichen bei seiner Pflicht zur Wahrung des Rechts.

Aus datenschutzrechtlicher Sicht sollte die Digitalisierung wesentlich von den Grundsätzen des Privacy by Design und der Nutzung von Instrumenten proaktiven Datenschutzes geprägt sein. Bereits im Entstehungs- oder Entwicklungsprozess neuer Technologien sollen datenschutzrechtliche Aspekte betrachtet werden, um Probleme zu erkennen und in die Gesamtkonzeption einzubeziehen. Im Mittelpunkt steht dabei die Datensparsamkeit. Der Datenschutz wird also ins Vorfeld verlagert, statt im Nachhinein an die möglichen Datenschutzverletzungen anzuknüpfen. Datensicherheit hat hierzu einen engen Bezug.

Schon nach der aktuellen Rechtslage gibt es Pflichten der Vorabkontrolle, bevor Systeme und Programme der Datenverarbeitung in Betrieb gehen. Der LfDI berät und unterstützt die betrieblichen Beauftragten für den Datenschutz und die Verantwortlichen (§ 38 Abs. 1 Satz 2 BDSG).

Diese bereits vorhandenen Instrumente des proaktiven Datenschutzes, der Datenschutzverletzungen verhindern soll, werden aber durch die Datenschutz-Grundverordnung noch ausgebaut und ausdifferenziert.

Verantwortliche können Verhaltensregeln ausarbeiten, die insbesondere auch den Bedürfnissen von Kleinstunternehmen sowie Klein- und mittleren Unternehmen Rechnung tragen sollen (Art. 40 DS-GVO). Aufgerufen sind hier Verbände und andere Vereinigungen, die durch derartige Verhaltensregeln (Codes of Conduct) ihre Beteiligten oder Mitglieder darin unterstützen sollen, sich datenschutzgerecht zu verhalten. Die Überwachung der genehmigten Verhaltensregeln obliegt einer zertifizierten Stelle, die dazu auch akkreditiert werden kann.

Akkreditierung, Zertifizierung und die Verleihung von Gütesiegeln sind weitere Instrumente proaktiven Datenschutzes. Zusammenfassend geht es darum, Konzepte für effektiven Datenschutz zu

erstellen und entsprechend prüfen zu lassen. Datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und Datenschutzprüfzeichen sollen von Mitgliedstaaten, Aufsichtsbehörden und den europäischen Gremien besonders gefördert werden (Art. 42 Abs. 1 DS-GVO). Zertifizierungsstellen sind zu akkreditieren. Zu Akkreditierung berechtigt ist die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle.

Eng im Zusammenhang mit Privacy by Design steht auch der Grundsatz Privacy by Default, d.h. der Datenschutz durch datenschutzfreundliche Voreinstellungen. Letztlich geht um die Verwirklichung des Grundsatzes der Datensparsamkeit. Der Verantwortliche soll geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, wobei die Verpflichtung für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit gilt (Art. 25 Abs. 2 DS-GVO). Dies wendet sich an eine Vielzahl von Herstellern aller Arten von Produkten.

Dem Grunde nach geht es um die datenschutzrechtliche Selbstorganisation der Wirtschaft, die von den zuständigen Datenschutzaufsichtsbehörden angeleitet und kontrolliert werden muss. Neue Herausforderungen an die Unternehmen auch in Rheinland-Pfalz stellen die Umsetzungen der einschlägigen Gedanken. Zwar ist der technisch-organisatorische Datenschutz bereits im Bundesdatenschutzrecht verankert. Jedoch sind Neuausformungen und eine grundsätzliche Stärkung der Idee proaktiven Datenschutzes durch die Datenschutz-Grundverordnung festzustellen.

Während sich Zertifizierung, Akkreditierung oder Gütesiegel tendenziell eher an die private Wirtschaft wenden, ist das Konzept der Datenschutz-Folgenabschätzung übergreifend. Es betrifft auch die Verwaltung. In Anknüpfung an Regelungen zur Vorabkontrolle geht es bei der Datenschutz-Folgenabschätzung darum, im Fall von Datenverarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheit natürlicher Personen zur Folge haben, vorab die Folgen der vorgesehenen Verarbeitungsvorgänge abzuschätzen. Der Verantwortliche kann seinen betrieblichen oder behördlichen Datenschutzbeauftragten heranziehen und wird dies regelmäßig tun. Trifft der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos, ist vor der Datenverarbeitung die Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO). Eine Datenschutz-Folgenabschätzung umfasst durchaus weitreichende Prüfungen (Art. 35 DS-GVO). Für die öffentliche Verwaltung gilt eine Sonderregel dann, wenn bereits bei Erlass des Gesetzes eine entsprechende Folgenabschätzung durchgeführt wurde. Dann ist eine weitere Datenschutz-Folgenabschätzung nur nach Ermessen im Einzelfall erforderlich (Art. 35 Abs. 10 DS-GVO).

Diese Instrumente dienen zur Anleitung der Digitalisierung und stellen sich als Maßnahmen der datenschutzrechtlichen Selbstorganisation und Selbstregulierung der Verantwortlichen dar. In der komplexen digitalen Welt ist eine effektive Sicherung der Grundrechte und der Persönlichkeit des Einzelnen nur durch eine umfangreiche Systematik von Schutzregelungen möglich. Diese Systematik umfasst staatliche Kontrolle und gesetzgeberisches Tun, sie nimmt aber auch die Verantwortlichen im Sinne des Datenschutzrechts in die Verantwortung für die Gestaltung einer datenschutzfreundlichen digitalen Zukunft.

2. Datenschutz und Wirtschaft

Digitalisierung bedeutet gleichzeitig auch Registrierung. Nahezu alles, was wir tun und erleben, wird technisch erfasst, gespeichert und regelmäßig auch ausgewertet. Die Daten der Bürgerinnen und Bürger werden damit immer mehr zum Produktionsfaktor, zum Antriebsmittel der Wirtschaft. Dabei begegnet die wirtschaftliche Nutzung von Daten keinen grundsätzlichen Einwänden. Wie jedes wirtschaftliche Tätigwerden unterliegt aber auch die Verarbeitung von Daten allgemeinen Regeln.

Denn der Umgang mit personenbezogenen Daten betrifft den Grundrechtsschutz der Einzelnen und kann daher nicht rein wirtschaftlich verstanden werden. Das Internet ist kein rechtsfreier Raum, aber auch kein ökonomiefreier Tummelplatz des Altruismus. Hier wird mindestens ebenso hart um die Verwirklichung von Geschäftsmodellen und um Marktanteile gekämpft wie in der analogen Welt.

Im Zeitalter von Big Data stellen personenbezogene Daten ein spezifisch geschütztes Gut dar, bei dem die gegenläufigen Interessen immer wieder zu einem Ausgleich gebracht werden müssen. Daten sind ein Gut mit wirtschaftlichen Bezügen, zuvörderst aber ein öffentliches Gut, das grundrechtlich geschützt ist. Die Betroffenen – seien es Kunden, Beschäftigte oder Geschäftspartner – sind vor der Verletzung dieses Grundrechts zu bewahren.

Der Datenschutz ist kein Wettbewerbshindernis. Ein angemessen verwirklichter Datenschutz ist eine Voraussetzung dafür, dass ein fairer Wettbewerb funktioniert. Datenschutz kann zudem Wettbewerbsvorteile bringen. Hier liegen auch ökonomische Chancen für dynamische Unternehmen in Rheinland-Pfalz. Im Unternehmen selbst sind die befriedenden und motivierenden Wirkungen eines funktionierenden Arbeitnehmerdatenschutzes nicht zu verkennen. Glaubwürdigkeit und Vertrauen sind im lokalen wie im globalen Wettbewerb die Münze, in der der Datenschutz die Investitionen zurückzahlt, die zuvor in ihn getätigt wurden.

Aus Angst vor Reputationsverlust wagt kaum ein Unternehmen öffentlich über Sicherheitsprobleme zu sprechen. Derartige Attacken bedrohen aber nicht nur große Unternehmen, sondern auch den Mittelstand. Das Sicherheitsbewusstsein scheint mit dem Digitalisierungszuwachs nicht Schritt zu halten. Der Schutz der IT-Infrastruktur und der Kommunikation müssen als unternehmenskritische Faktoren gesehen werden, deren mangelnde Berücksichtigung Risiken für den Bestand eines Unternehmens oder seine Position im Markt bergen. Die Sensibilisierung und die Aufklärung der Unternehmensleitungen und Beschäftigten sind ebenso notwendig wie angemessene Sicherheits- und Datenschutzkonzepte. Hier kommen Zertifizierung, Akkreditierung, Gütesiegel oder Datenschutz-Folgenabschätzung erneut ins Spiel. Sie betreffen übergreifende Konzepte der Datenverarbeitung, die auch Elemente der IT-Sicherheit umfassen.

3. Gesundheitsdatenschutz

Elektronische Patientenakten, Videosprechstunde, intelligente Assistenzsysteme oder medizinische Versorgungs-Apps – die Digitalisierung ist mittlerweile auch im Gesundheitswesen angekommen und beginnt, über lange Zeit etablierte Verhaltensmuster und Verantwortlichkeiten einschließlich der darauf gestützten Arbeitsprozesse in Frage zu stellen. Es herrscht Goldgräberstimmung. Mit der Digitalisierung sollen sich alle Akteure des Gesundheitswesens einschließlich der Pflege so umfassend und transparent wie möglich vernetzen. Dies stellt einen Paradigmenwechsel dar, von dem sich Kostenträger, Leistungserbringer, Patienten und die politischen Entscheidungsträger enorme Vorteile für die Allgemeinheit versprechen: Medizinische und pflegerische Behandlung und Versorgung sollen besser, schneller, kostengünstiger und nachhaltiger werden. Die anfallenden Daten sollen so weit wie möglich der Forschung dienen, um neue, noch effektivere Behandlungsmethoden zu entwickeln. Und schließlich hofft man, dass die digitale Gesundheitswirtschaft als Zukunftsmarkt dazu beiträgt, den Wirtschaftsstandort Deutschland langfristig abzusichern.

Bei all den berechtigten Chancen und Erwartungen gilt es, die mit der Digitalisierung einhergehenden Risiken für den Einzelnen und die Solidargemeinschaft nicht aus dem Blick zu verlieren. Wo liegen die roten Linien, die bei der künftigen flächendeckenden Nutzung digitaler Technik im Gesundheitsbereich eingehalten werden müssen? Neben allgemein einzuhaltenden Kriterien, wie z.B. festgelegter Qualitätsstandards oder angemessener Bedienbarkeit, muss aus der Sicht des Datenschutzes der Wesensgehalt des Grundrechts gerade im Kontext der Gesundheitsversorgung gewahrt bleiben:

hierzu gehören ein wirksamer Schutz der Patientenautonomie und des Vertrauensverhältnisses zwischen Behandler und Patienten, eine nach dem aktuellen Stand der Technik garantierte Manipulationssicherheit der eingesetzten Verfahren sowie die Einhaltung ethischer Schranken.

Was ist zu tun?

Für einen verantwortungsvollen Umgang mit digitaler Gesundheitstechnologie müssen alle Betroffenen – d.h. die Akteure im Gesundheits- und Pflegebereich genauso wie die Patienten – sensibilisiert und vorbereitet sein. Der Vermittlung von Medienkompetenz und einem datenschutzrechtlichen Basiswissen kommt dabei ebenso eine wichtige Bedeutung zu wie der Fähigkeit, die jeweiligen Informationen richtig und rollengemäß einordnen zu können.

Die verschiedenen Einsatzfelder digitaler Technik im Kontext Gesundheit sollten präzisiert (z.B. Gesundheitsversorgung; Prävention, Lifestyle/Wellness) und die jeweils dazu gehörenden Rahmenbedingungen verbindlich festgelegt werden. So sollten Patienten davon ausgehen können, dass die in einem professionellen Umfeld verwendeten Technologien datenschutzrechtliche Belange der Betroffenen bereits von sich aus so weit wie möglich sicherstellen, ohne dass es einer ausdrücklichen Einforderung durch sie bedarf. Auch in diesem Zusammenhang können wieder Zertifizierungen oder Auditierungen dabei helfen. Auf der anderen Seite muss geklärt werden, inwieweit bei rein privater Nutzung digitaler Gesundheitsangebote staatliche Vorkehrungen geboten sind, um datenschutzrechtliche Mindeststandards zu garantieren, und wo es in der Verantwortung des Einzelnen liegen muss, sich selbstverantwortlich um den Schutz seiner Daten zu kümmern.

Es bedarf einer öffentlichen Diskussion, wie die Veränderungen, die sich aus der Digitalisierung im Gesundheitswesen ergeben, so genutzt werden können, dass das Vertrauensverhältnis zwischen Arzt und Patienten nicht gefährdet wird. Welche Vorteile bieten sich für Behandlung und Therapie, und welche Risiken bestehen? An der Meinungsbildung sollten alle Akteure, die von der Digitalisierung im Gesundheitsbereich betroffen sind, beteiligt werden.

Um der Gefahr einer Technisierung der Gesundheitsversorgung und der Entsolidarisierung der Versichertengemeinschaft entgegenzuwirken sollten geeignete rechtliche Rahmenbedingungen festgelegt werden, die dies verhindern. Dabei sollte geklärt werden, ob und in welchem Maße die Einwilligung, also die Übertragung der Verantwortung für einen zulässigen Umgang mit den Gesundheitsdaten von den datenverarbeitenden Stellen auf die Betroffenen, in diesem Zusammenhang für die Menschen überhaupt noch zumutbar ist.

Das Potential datenschutzfreundlicher technischer Voreinstellungen (Privacy by Default) und Funktionalitäten (Privacy by Design) muss ausgeschöpft werden. Hierbei gilt es, angesichts der regelmäßig europaweit oder sogar global agierenden Softwarehersteller und Anbieter zu internationalen verbindlichen Standardisierungen zu kommen. Es ist klärungsbedürftig, auf welchem Wege (Selbstverpflichtung oder Regulierung) dies effektiv erreicht werden kann.

Schließlich müssen die ethischen Schranken des Umgangs mit digital verarbeiteten Gesundheitsdaten allgemeinverträglich justiert werden. Wie können die neuen digitalen Möglichkeiten im Hinblick auf Big Data so gestaltet werden, dass auch zukünftig zentrale Werte der Menschenwürde in der Gesundheitsversorgung erhalten bleiben? Welche staatlichen und nichtstaatlichen Institutionen tragen hierbei Verantwortung? In diesem Zusammenhang bedarf es einer breiten öffentlichen Meinungsbildung, an der alle gesamtgesellschaftlich relevanten Akteure beteiligt werden sollten.

4. Digitale Bildung

Der Ansatz, dass alle Lehrenden und Lernenden entlang der Bildungskette beim Erwerb und der Fortentwicklung digitaler Kompetenzen zu unterstützen seien, ist uneingeschränkt zu befürworten. Gerade weil die digitale Bildung Voraussetzung für eine souveräne Teilhabe in einer digitalisierten Lebenswelt ist, bedarf es allerdings noch weiteren Handelns.

In jüngster Zeit haben die Nachfragen zu Fortbildungsangeboten zum Datenschutz in Kitas stark zugenommen. Die allgegenwärtige Nutzung von Smartphones hat auch im Bereich der Kitas Rechtsfragen zu den Persönlichkeitsrechten von Kindern, Eltern und Erzieherinnen und Erziehern aufgeworfen. Daher sollten Erzieherinnen und Erzieher schon in ihrer Ausbildung darin geschult werden, beim Medieneinsatz in Kitas auf die Persönlichkeitsrechte der Kinder und Eltern zu achten. Dies gilt insbesondere bei der Speicherung von Bildungs- und Lerndokumentationen auf Tablets und deren Synchronisation über Clouddienste, bei der Nutzung von Messengerdiensten als Kommunikationsmittel mit Eltern oder Kollegen, bei der Gestaltung einer Kita-Homepage und bei der Sensibilisierung der Eltern, wenn diese Fotos und Videos ihrer Kinder fertigen und online stellen.

Im schulischen Kontext kommt den Lehrkräften bei der Vermittlung digitaler Bildungsinhalte als Lehrende und Multiplikatoren eine maßgebliche Rolle zu. Digitale Bildung sollte in ihren Grundlagen daher bereits im Studium prüfungsrelevant vermittelt und im Bereich der Fort- und Weiterbildung stetig an die aktuellen Entwicklungen angepasst werden. Angesichts der vielfältigen Fortbildungsmöglichkeiten sollten für Lehrkräfte besondere Anreize für die Wahrnehmung von Fortbildungen mit Datenschutz- und Medienkompetenzinhalten geschaffen werden. Hier wäre zu überlegen, mit einem Punktesystem zu arbeiten, wie dies im Bereich der Ärztefortbildungen derzeit gehandhabt wird. Entsprechende Fortbildungsangebote könnten über Webinare kostengünstig und mit überschaubarem Aufwand angeboten werden.

Auch wenn man den Ansatz eines eigenständigen Schulfachs „Digitale Bildung" nicht für unterstützungswürdig hält, sollte das Thema in den Lehrplänen fächerübergreifend und prüfungsrelevant verankert werden. Hier gilt es, den Beschluss der Konferenz der Kultusminister aus dem Jahr 2012 zur „Medienbildung in der Schule" und die im Dezember 2016 verabschiedete Strategie „Bildung in der digitalen Welt" in der Praxis umzusetzen. Aus Sicht des LfDI ist die Erhöhung der Verbindlichkeit dabei maßgeblich für die Vermittlung von Medien- und Datenschutzkompetenzinhalten im Schulunterricht.

Der Ausbau des Schulfachs „Sozialkunde" bietet sich gut als Ansatzpunkt zur Vermittlung einer „mündigen Kritikfähigkeit" an, wie es Professor Daschmann im Jahr 2015 in der Expertenrunde „Weiterentwicklung des Landesprogramms 'Medienkompetenz macht Schule'" gegenüber dem Bildungsministerium formulierte. Die aktuelle Diskussion um „Fake-News" bestätigt die Richtigkeit dieses Ansatzes. Die Vermittlung des dem Datenschutz zugrunde liegenden Wertekanons und der Funktionsbedingungen des digitalen Zeitalters sind hierbei ebenso zentral, wie die Sensibilisierung für die Risiken, die mit diesen Funktionsbedingungen verbunden sind sowie für die Möglichkeiten, sich im Netz selbst helfen zu können.

Des Weiteren sollten den Lehrkräften niedrigschwellige Angebote für die Vermittlung von Medienkompetenzfragen im Schulunterricht angeboten werden. Hierbei können e-learning-Szenarien eine wichtige Rolle spielen. Auf für Lehrkräfte zugänglichen Plattformen, wie beispielsweise dem Omega-Server oder der Moodle-Plattform, sollten entsprechende Module vorgehalten werden, die es einer Lehrkraft ohne aufwändige Eigenfortbildung ermöglichen, beispielsweise in einer Vertretungsstunde, eine Unterrichtseinheit zu Datenschutzthemen zu gestalten.

Außerdem sollte über die systematische Anbindung von Medienpädagogen an die Schulgemeinschaft nachgedacht werden. Hierdurch könnten bedarfsgerecht interne Seminare für Lehrkräfte und Schüler angeboten, Unterrichtsbegleitungen durchgeführt, Methoden und Unterrichtsmodule entwickelt und die konzeptionelle Ausrichtung der Schulen von innen mitgestaltet werden. Um Synergieeffekte zu erzielen, wäre außerdem zu überlegen, das Amt des/der schulischen Datenschutzbeauftragten mit der Funktion eines Jugendmedienschutzberaters zusammenzulegen.

Die Schaffung einer digitalen Lernumgebung für Schülerinnen und Schüler darf nicht auf eine zeitgemäße Hardwareausstattung und das Vorhandensein von WLAN in den Schulen reduziert werden. Denn bereits bei der Planung und Anschaffung der IT-Infrastruktur einer Schule sollten in Abstimmung mit dem Schulträger Fragen der technisch-organisatorischen Datensicherheit mit einbezogen werden. Darüber hinaus ist auch die Nutzung von Online-Wettbewerben, elektronischen Klassenbüchern, Lernplattformen, Messenger- und Clouddiensten oder des Unterrichtskonzepts „Bring your own device" mit rechtlichen und technischen Datenschutzfragen verbunden, die von den Schulaufsichtsbehörden beantwortet werden müssen.

5. Sicherheit der Verarbeitung und datenschutzkonforme Gestaltung von IT-Verfahren

Eine angemessene Sicherheit bei der automatisierten Verarbeitung ist ein datenschutzrechtliches Gebot, sie liegt jedoch auch im Interesse der datenverarbeitenden Stellen. Geschäftsprozesse werden zunehmend ins Internet verlagert und IT-Strukturen durch den Einsatz mobiler Geräte und die Nutzung von Cloud-Lösungen auf Bereiche außerhalb der eigenen Organisation ausgedehnt. Die Einbindung von Geschäftspartnern, Dienstleistern und Lieferanten in Wertschöpfungsketten, E-Commerce- und E-Government-Lösungen sowie die elektronische Anbindung von Kundinnen und Kunden bzw. Bürgerinnen und Bürgern eröffnen zunehmend Zugriffsmöglichkeiten durch externe Stellen. Mit dieser fortschreitenden Digitalisierung nehmen Angriffe auf IT-Strukturen von Verwaltungen und Unternehmen zu. Informationen über Wettbewerber und Märkte, Technologien, Kundinnen und Kunden, aktuelles Know-how oder staatliche Kommunikation wecken vielfältige Begehrlichkeiten. Rheinland-Pfalz mit einer Wirtschaftsstruktur in Feldern, in denen technologische Kompetenz und Know-how von essentieller Bedeutung sind (Chemie, Fahrzeugbau, Maschinenbau etc.) und mit einer Exportquote von über 50 Prozent im verarbeitenden Gewerbe ist hier besonders exponiert.

Die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft spricht allein in Deutschland von jährlich 50 Milliarden Euro Schaden durch solche Wirtschaftsspionage. Andere Schätzungen gehen von bis zu 100 Milliarden Euro aus. Dies sind fast zwei bzw. vier Prozent des Bruttoinlandsprodukts Deutschlands. Bei einem rheinland-pfälzischen BIP-Anteil von ca. vier Prozent ergibt sich ein Schadensvolumen zwischen zwei und vier Milliarden allein in Rheinland-Pfalz.

Die Datensicherheit ist, vor allem bei kleinen und mittleren Unternehmen und Verwaltungen, oftmals jedoch noch ausbaufähig (vgl. Ausführungen unter Ziff. 2). Nach einer Untersuchung des Branchenverbandes BITKOM verfügt weniger als die Hälfte der Unternehmen über einen Notfallplan für IT-Sicherheitsvorfälle und lediglich ein Viertel über eine Sicherheitsstrategie, um sich gegen Angriffe zu schützen (https://www.bitkom.org/Presse/Presseinformation/Unternehmen-muessen-bei-IT-Sicherheit-nachbessern.html). Die Roadmap der Landesregierung zum Digitaldialog nimmt daher folgerichtig die Sicherheit der Datenverarbeitung und den Aufbau sicherer IT-Strukturen in den Blick.

Die kommende Datenschutz-Grundverordnung sieht in diesem Zusammenhang sowohl eine standardmäßige Analyse und Bewertung der mit der automatisierten Verarbeitung verbundenen Risiken vor (Art. 25 Abs. 1, Art, 32 Abs. 1 DS-GVO), als auch die Einführung eines Verfahrens mit dem die

getroffenen Sicherheitsmaßnahmen und ihre Wirksamkeit regelmäßig überprüft werden (Art 32 Abs. 1 lit. d) DS-GVO.

Risikoanalyse und IT-Sicherheits- und Datenschutzmanagement sind daher Anforderungen, die Unternehmen und Verwaltungen gleichermaßen treffen und als integraler Bestandteil von Digitalisierungsprojekten vorgesehen werden müssen.

Die datenschutzkonforme Gestaltung von IT-Verfahren spielt eine zentrale und zugleich alle Bereiche der Wirtschaft und Verwaltung betreffende Rolle. Sie ist bei jeder automatisierten Verarbeitung personenbezogener Daten neben den Zulässigkeitsvoraussetzungen (z.B. Rechtsgrundlage, Unterrichtung/Einwilligung, Zweckbindung) in den Blick zu nehmen. Von besonderer Bedeutung ist hierbei die Einhaltung der Grundätze nach Art. 5 Abs. 1 lit. c) DS-GVO (Datenminimierung), Art. 5 Abs. 1 lit. f) DS-GVO (Integrität und Vertraulichkeit), Art. 25 DS-GVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) sowie die Wahrung der Betroffenenrechte (Art. 13 ff. DS-GVO). Hier setzt das im Auftrag der Datenschutzkonferenz entwickelte Standard-Datenschutzmodell (http://s.rlp.de/sdm) an. Es fußt auf dem Eckpunktepapier "Ein modernes Datenschutzrecht für das 21. Jahrhundert" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. März 2010 und ergänzt die Ziele der IT-Sicherheit um datenschutzbezogene Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit, Datensparsamkeit, Transparenz, Wahrung der Betroffenenrechte (Intervenierbarkeit) und Sicherstellung der Zweckbindung.

Das Standard-Datenschutzmodell berücksichtigt damit grundlegende Datenschutzprinzipien und ermöglicht die datenschutzgerechte Gestaltung von informationstechnischen Verfahren. Es sollte daher bei der Gestaltung von IT-Verfahren einbezogen werden.

Zentrale Aspekte einer datenschutzfreundlichen Technikgestaltung (Privacy by Design, vgl. Art. 25 DS-GVO und Ausführungen unter Ziff. 1) sind weiterhin Verschlüsselung und Pseudonymisierung. Diese ermöglichen es, oftmals datenschutzkritische Technologien wie Big Data und Data Mining datenschutzgerecht abzufedern (vgl. Ausführungen unter Ziff. 3). Sie eröffnen Auswertungs- und Verarbeitungsmöglichkeiten, mit denen deren Potenziale erschlossen werden können und die datenschutzrechtlichen Anforderungen dabei angemessen entsprechen.

Verschlüsselung und Pseudonymisierung sollten bei der Gestaltung von IT-Verfahren als grundsätzliche Datenschutzmechanismen berücksichtigt werden.