KREIS DÜREN

Dieser Prüfbericht wird nach § 6 Abs. 3 der Rechnungsprüfungsordnung des Kreises Düren nach der Sitzung des Rechnungsprüfungsausschusses am 31.05.2022 veröffentlicht. Personen- oder unternehmensbezogene Daten wurden hierbei, soweit vorhanden, anonymisiert.

Prüfung – Beratung – Revision

RECHNUNGSPRÜFUNGSAMT

P R Ü F B E R I C H T

DES

RECHNUNGSPRÜFUNGSAMTES

Datenschutz und Datensicherheit in der Kreisverwaltung Düren

Drs. Nr. 103/22

Kreis Düren

Rechnungsprüfungsamt

P R Ü F B E R I C H T

Datenschutz und Datensicherheit in der Kreisverwaltung Düren

Verfasser: Guido Kämmerling, Leiter der örtlichen Rechnungsprüfung

Bismarckstraße 16

52351 Düren, Haus A, Zimmer 192

Tel. 02421 – 22 1014001, Fax. 02421 - 22 182258

www.kreis-dueren.de

E-Mail: amt14@kreis-dueren.de

Inhaltsverzeichnis

1. Einleitung und Prüfauftrag

Das Rechnungsprüfungsamt ist neben der Prüfung des Jahresabschlusses auch für die Prüfung der der *Ordnungsmäßigkeit* und *Zweckmäßigkeit* des Verwaltungshandelns sowie die Wirksamkeit *interner Kontrollen* im Rahmen des internen Kontrollsystems zuständig (§ 104 GO).

Unter diesen umfassenden Prüfauftrag ist auch der **Datenschutz** zu subsumieren. Dieser ist in zahlreichen Rechtsnormen des Europäischen sowie des Bundes- und des Landesrechts normiert und enthält entsprechende Verpflichtungen für die Behörden, Kommunen und ihre jeweiligen Hauptverwaltungsbeamten. Die Pflicht zur Einrichtung besonderer Datenschutzbeauftragter unterstreicht die Bedeutung des Datenschutzes nachhaltig. Daneben muss die **Datensicherheit** unter zahlreichen (rechtlichen, technischen) Aspekten ebenfalls Gegenstand der Rechnungsprüfung sein. Hierbei geht es auch darum, technischen oder wirtschaftlichen Schaden vom Kreis Düren abzuwenden.

Mit Aspekten des Datenschutzes hat sich die Rechnungsprüfung in der Vergangenheit bereits mehrfach befasst.[1]

Anlass zur erneuten Betrachtung der Aspekte **Datenschutz** und **Datensicherheit** gab aber eine seit dem Verwaltungsprüfbericht 2009/2010 existierende Prüfbemerkung, die bis heute *nicht* abgearbeitet und ausgeräumt worden ist. Hinzu treten die zahlreichen rechtlichen Änderungen und technischen Weiterentwicklungen, die bisher erkennbar *nicht* Eingang in verwaltungsinterne Regularien gefunden haben.

Aspekte von Datenschutz und Datensicherheit wurden zudem im Prüfbericht „**IT-Management**“ (Drs. Nr. 236/20) aufgegriffen.

Letztlich waren die Belange des *Datenschutzes* und der *Datensicherheit* auch im Rahmen der verwaltungsseitig geplanten „**Digitalisierung der Verwaltung**“ in den Blick zu nehmen.

[1] Verwaltungsprüfberichte 2008/2009 (Drs. Nr. 267/09), VwPB 2009/2010 (Drs. Nr. 420/10), VwPB 2010/2011 (Drs. Nr. 351/11), VwPB 2011/2012 (Drs. Nr. 284/12).

2. Grundsätze des Datenschutzes

Das Datenschutzrecht offenbart sich als komplexe und auf verschiedenen Ebenen normierte Rechtsmaterie, die sowohl das *Europarecht* wie auch das *Bundes*- und *Landesrecht* umfasst. Gleichzeitig gilt insbesondere der Grundsatz *lex specialis* vor *lex generalis*. Dies wird besonders im Verhältnis vom Sozialdatenschutz zum "allgemeinen" Datenschutz deutlich.

Die obersten Landesbehörden, die Gemeinden und **Gemeindeverbände** sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform haben allerdings jeweils für ihren Bereich die Ausführung der Verordnung (EU) 2016/679, des Datenschutzgesetzes NRW sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen (§ 2 DSG NRW).

Die Datenschutz-Grundverordnung

Am 25. Mai 2016 ist die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4.5.2016, S. 1) in Kraft getreten. Gemäß Artikel 99 Absatz 2 der Verordnung (EU) 2016/679 gilt sie ab dem 25. Mai 2018.

Die Verordnung (EU) 2016/679 weist zum einen Öffnungsklauseln für den nationalen Gesetzgeber, zum anderen konkrete Regelungsaufträge auf.

Die Verordnung (EU) 2016/679 ist unmittelbar geltendes Datenschutzrecht, das gegenüber dem nationalen Recht - insbesondere im Fall von widersprechenden Regelungen - den Vorrang genießt.

Daneben ist die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L119 vom 4.5.2016,

S. 89) in Kraft getreten. Die Richtlinie (EU) 2016/680 ist von den Mitgliedstaaten in nationales Recht umzusetzen.[2]

Die Europäische Datenschutz-Grundverordnung (DS-GVO) ersetzte damit die aus dem Jahr 1995 stammende EU-Datenschutzrichtlinie und gab nach Auffassung des **BMWi** zeitgemäße Antworten auf die fortschreitende **Digitalisierung** von Wirtschaft und Gesellschaft. Mit einem modernen Datenschutz auf europäischer Ebene bot die DS-GVO Lösungen zu Fragen, die sich durch „Big Data" und neue Techniken oder Arten der Datenverarbeitung wie Profilbildung, Webtracking oder dem Cloud Computing für den Schutz der Privatsphäre stellen.

Das Europäische Parlament hatte die DS-GVO am **14. April 2016** mit breiter Mehrheit angenommen. Sie ist am 25. Mai 2018 nach einer Übergangsphase von zwei Jahren wirksam geworden und bildet den datenschutzrechtlichen Rahmen innerhalb der Europäischen Union. Unternehmen mussten ihre Geschäftsabläufe bis zum 25. Mai 2018 an die neue Rechtslage anpassen.[3]

Nach dem bedeutsamen **Art. 6 Abs. 1 DSGVO** eine Verarbeitung von Daten nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur *Erfüllung einer rechtlichen Verpflichtung* erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

[2] Quelle: https://**www.im.nrw**/themen/verwaltung/datenschutz/rechtsgrundlagen
[3] Quelle: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Nach Art. 6 Abs. 3 DSGVO wird die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c) und e) wiederum festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e) für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Datenschutzregelungen im DSG NRW und BDSG

Mit dem Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU - NRWDSAnpUG-EU) vom 17. Mai 2018 (GV. NRW. S. 244) wurden die datenschutzrechtlichen Regelungen zur Anpassung bzw. Umsetzung des europäischen Datenschutzrechts für den öffentlichen Bereich auf Landesebene vorgenommen. Hierbei wurde der am 1. März 2018 eingebrachte Gesetzesentwurf unter Berücksichtigung des zuvor angenommenen Änderungsantrags am 16. Mai 2018 verabschiedet.[4]

Das *Datenschutzgesetz NRW* trifft damit die zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher

[4] Quelle: https://**www.im.nrw**/themen/verwaltung/datenschutz/rechtsgrundlagen

Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (*Datenschutz-Grundverordnung*) notwendigen *ergänzenden* Regelungen. Innerhalb der Grenzen der Verordnung (EU) 2016/679 werden spezifische Anforderungen an die Verarbeitung personenbezogener Daten geregelt.

Nach § 5 DSG NRW gilt dessen Teil 2 für die Verarbeitung personenbezogener Daten durch die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die *Gemeinden* und *Gemeindeverbände* sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform (öffentliche Stellen). Soweit allerdings *besondere* Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften des Teils 2 des DSG NRW vor (vgl. § 5 Abs. 6 DSG NRW).

Nach § 9 Abs. 1 DSG NRW dürfen personenbezogene Daten durch öffentliche Stellen auch zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen verarbeitet werden.

In Teilbereichen der Kommunalverwaltung gelten (trotz des Landesdatenschutzgesetzes) zum Teil auch Vorschriften des *Bundesdatenschutzgesetzes*. Nach § 23 Abs. 1 Nr. 6 BDSG ist die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung zulässig, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient.

Sozialdatenschutz

Das Sozialgesetzbuch enthält an verschiedenen Stellen datenschutzrechtliche Vorgaben, die in der Kommunalverwaltung im Sozialamt, Jugendamt oder auch in Job-Centern (z.B. bei Optionskommunen) Geltung erlangen.

Nach der **Grundsatznorm** des § 35 SGB I hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 2 SGB X) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Nach Maßgabe des § 35 Abs. 2 SGB I regeln die Vorschriften des *Zweiten Kapitels des Zehnten Buches* und der *übrigen* Bücher des Sozialgesetzbuches die

Verarbeitung von Sozialdaten abschließend, soweit nicht die *Datenschutz-Grundverordnung* in der jeweils geltenden Fassung unmittelbar gilt.

Zur Datenverarbeitung und datenschutzrechtlichen Verantwortung enthalten die §§ 50 ff. SGB II besondere Regelungen (**Job-Com**).

Nach § 61 SGB VIII gelten wiederum für den **Jugendamtsbereich** grundsätzlich die Regelungen der §§ 35 SGB I bzw. 67 ff. SGB X. Daneben gibt es spezielle Regelungen z.B. für Amtspfleger, Amtsvormünder, Beistände und Gegenvormünder oder im Rahmen persönlicher oder erzieherischer Hilfen (vgl. auch §§ 65, 68 SGB VIII).

Das Neunte Sozialgesetzbuch regelt die **Rehabilitation** und **Teilhabe** von Menschen mit Behinderungen. Nach dem AG SGB IX NRW sind *Landschaftsverbände* bzw. *Kreise* Träger für bestimmte Aufgaben in der Eingliederungshilfe bzw. dem Schwerbehindertenwesen (vgl. §§ 1 und 9 AG SGB IX NRW). Mangels eigener spezieller Regelungen zum Datenschutz (einschließlich Bezügen zur Rechnungsprüfung) gelten für diesen Bereich somit die allgemeinen Bestimmungen des I. und X. Sozialgesetzbuches.

Für das **Sozialamt** enthält das SGB XII im Vergleich zu anderen Sozialgesetzbüchern keine spezifische(re)n Regelungen und verweist insoweit auf die allgemeinen Regelungen von SGB I und SGB X.

Weitere Fachbereiche

Entsprechend den zahlreichen Aufgabenstellungen und gesetzlichen Zuständigkeiten im kommunalen Bereich sind für die unterschiedlichen Fachbereiche stets die spezialgesetzlichen Regelungen zu beachten, die entweder eigene datenschutzrechtliche (Sonder)bestimmungen enthalten oder aber auf bestehende Regelungen (des DSG NRW, des BDSG oder der Sozialgesetzbücher I oder X) verweisen. Die Bandbreite erfasst den gesamten kommunalen Aufgabenbereich, neben der Sozialverwaltung also z.B. das Rettungs-, Ausländer-, Vermessungs- und Katasterwesen, die Bauverwaltung, Ordnungsämter, Umweltverwaltung, Landschafts- und Wasserbehörden, Abfallwesen u.v.m. Für den Kreis Düren sind weiterhin u.a. der Bereich des **Gesundheitsdatenschutzes** oder des **Schulwesens** von Bedeutung. Selbstredend sind datenschutzrechtliche Vorgaben auch im Bereich der **Personalverwaltung** und des Personalaktenrechts zu beachten (z.B. §§ 83 LBG, 50 BeamtStG, 18 DSG NRW).

Datenschutz und Rechnungsprüfung

Neben den besonderen Prüfungsbefugnissen aus der Gemeindeordnung (§§ 101 ff. GO) enthalten die vielfältigen datenschutzrechtlichen Bestimmungen zahlreiche Regelungen, die eine Erhebung, Kenntnisnahme oder Weiterverarbeitung von Daten durch die Rechnungsprüfung ausdrücklich erlauben.[5]

3. Datensicherheit

Unter dem Begriff „Datensicherheit" versteht man den generellen Schutz aller Daten eines Unternehmens (oder einer Kommune). Es geht also darum, dass geeignete Maßnahmen eingeführt werden, um diesen Schutz gewährleisten zu können. Datensicherheit ist also weniger ein Prozess, sondern vielmehr ein Zustand, der erreicht werden soll.

Dabei handelt es sich sowohl um Daten mit Personenbezug als auch um Daten, die keinen Bezug zu einer Person herstellen. Solche Daten können beispielsweise Konstruktionspläne oder Unternehmensstrategien sein. Bei den Daten ist es unerheblich, ob diese in analoger oder digitaler Form vorliegen.

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)**[6] ist eine in Bonn ansässige zivile obere Bundesbehörde für Fragen rund um die IT-Sicherheit. Der Aufgabenbereich des BSI wird durch das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" (BSI-Gesetz) festgelegt. Ziel des BSI ist es, die Informationssicherheit und Cybersicherheit zu fördern und voranzutreiben. Dies erfolgt beispielsweise durch ausgearbeitete Handlungsempfehlungen zur IT-Sicherheit, um Risiken zu minimieren oder gar verhindern zu können.

Das BSI gibt außerdem die **IT-Grundschutz-Kataloge** heraus, die Empfehlungen für Standardmaßnahmen für typische IT-Systeme enthalten. Das kann vor allem bei der Sicherung von digitalen Daten für Unternehmen von Nutzen sein.

[5] Hierzu *Kämmerling*: Prüfungsrechte und Datenschutz in der kommunalen Rechnungsprüfung, in: der gemeindehaushalt 2021, S. 148 ff. *Oebbecke/Desens:* Die Rechtsstellung der Leitungen der örtlichen Rechnungsprüfung in Nordrhein-Westfalen, Wiesbaden 2012, S. 39 ff.
[6] www.bsi.bund.de

Durch die Datensicherheit sollen alle Daten eines Unternehmens (oder einer Kommune) in jeglicher Hinsicht geschützt werden. Damit ist ein Schutz vor Verlust, Verfälschung, Beschädigung oder auch Löschung gemeint. Die Ziele der Datensicherheit sind somit Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Unter Vertraulichkeit ist gemeint, dass die Daten nur von berechtigten Personen eingesehen werden dürfen. Geschützt wird also, dass unbefugte Personen keinen Zugriff auf Daten und deren Informationen erhalten. Bei der Integrität geht es darum, dass Daten nicht unbemerkt verändert oder verfälscht werden dürfen. Durch die Verfügbarkeit soll gewährleistet werden, dass der Zugriff auf Daten jederzeit gewährleistet werden kann. Das bedeutet, dass sich ein Unternehmen beispielsweise vor Systemausfällen schützen sollte. Durch den Absturz eines Systems können Daten nicht eingesehen werden, wodurch die Verfügbarkeit von Daten nicht vorhanden ist. Durch die Authentizität sollen die Echtheit und Vertrauenswürdigkeit von Daten gewährleistet werden. Datensicherheit ist somit der Prozess zum Erreichen des Zustandes von Sicherheit und die dazugehörigen Maßnahmen.[7]

Regelungen zur Datensicherheit wurden aber auch in das (aufgrund der DSGVO) neu zufassende Datenschutzgesetz NRW aufgenommen.

Nach § 58 DSG NRW haben die Verantwortlichen[8] und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

Die vorgenannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit ihr Aufwand in einem

[7] Quelle: https://www.haufe.de/compliance/management-praxis/datensicherheit/was-ist-datensicherheit_230130_483950.html
[8] Vgl. Legaldefinition in Art. 4 Nr. 7 DSGVO

angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Maßnahmen sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und

2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Im Fall einer Verarbeitung personenbezogener Daten haben der Verantwortliche und der Auftragsverarbeiter auf Grundlage einer **Risikobewertung** Maßnahmen zu ergreifen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (**Vertraulichkeit**),

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**) und

5. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).

Zu dieser Umsetzung sind insbesondere

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (**Zugangskontrolle**),

2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Datenträgerkontrolle**),

3. die unbefugte Eingabe sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (**Speicherkontrolle**),

4. zu verhindern, dass automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (**Benutzerkontrolle**),

5. zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (**Zugriffskontrolle**),

6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**),

7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**),

8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (**Auftragskontrolle**),

9. zu verhindern, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**),

10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (**Organisationskontrolle**),

11. zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

12. zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellung**),

13. zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**),

14.zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**) und

15. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (**Trennbarkeit**).

Prüfbemerkung

Nach Erkenntnissen der örtlichen Rechnungsprüfung liegen zu den vorgenannten Anforderungen verwaltungsseitig **keine** grundlegenden und umfassenden Regelungen, Verfügungen, Anweisungen oder sonstige verwaltungsweit geltenden schriftlichen Vorgaben vor.

Zwar wurde auch zum Prüfbericht „*IT-Management*“ (Drs. Nr. 236/20) verwaltungsseitig die Erarbeitung von Richtlinien und Hinweise zur Gewährleistung der Datensicherheit durch den IT-Sicherheitsbeauftragten angekündigt, eine Fertigstellung oder verwaltungsinterne Bekanntmachung solcher Richtlinien konnte aber ebenfalls noch **nicht** festgestellt werden.

4. Datenschutzbeauftragter

Bereits nach altem Recht des Datenschutzgesetzes NRW (vom 09.06.2000) hatten öffentliche Stellen einen internen Datenschutzbeauftragten sowie einen Vertreter zu bestellen (§ 32a DSG NRW a.F.).

Nach überarbeitetem Recht ist die Bestellung eines Datenschutzbeauftragten nunmehr in Art. 37 DSGVO geregelt.

Der Datenschutzbeauftragte hat eine wichtige Funktion innerhalb der Kommunalverwaltung. Dieser kann er allerdings nur nachkommen, wenn dem Datenschutz die erforderliche Bedeutung beigemessen wird und verbindliche und aktuelle Regularien vorliegen.

Der Blickwinkel der behördlichen Datenschutzbeauftragten geht nach Auffassung des zuständigen Landesministeriums NRW in zwei Richtungen: Zum einen sollen sie die Mitarbeiterinnen und Mitarbeiter auf allen Ebenen motivieren, sensibel mit den ihnen anvertrauten Daten umzugehen und zum anderen die Behördenspitze veranlassen, die Leitungsverantwortung auf dem Gebiet des Datenschutzes problembewusst und informiert wahrzunehmen.

Die Aufgaben werden abschließend in Artikel 39 der Datenschutz-Grundverordnung beschrieben. Es sind Tätigkeiten in den drei Bereichen: Unterstützung, Beratung und Kontrolle.

Im Gesetz genannt werden (in der Reihenfolge der Aufzählung):

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten hinsichtlich der Datenschutzvorschriften
- Überwachung der Einhaltung der Datenschutzvorschriften
- Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeitern
- Beratung im Zusammenhang mit der Datenschutz-Folgeabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für Bediensteten in Angelegenheiten des Datenschutzes

Die Aufzählung zeigt, dass der Aufgabenschwerpunkt bei den unterstützenden und beratenden Tätigkeiten liegt. Der bzw. die behördliche Datenschutzbeauftragte versteht sich in erster Linie als Partner/in aller Behördenbediensteten.

Erst in zweiter Linie kommt die Kontroll- und Überwachungsfunktion zum Tragen. Diese ist für eine umfassende Sicherstellung des Datenschutzes zwar unumgänglich, kann aber bei entsprechend guter und vertrauensvoller Zusammenarbeit bei der Planung und Realisierung der Vorhaben flexibel gehandhabt werden ("so viel Unterstützung und Beratung wie möglich und so viel Kontrolle wie nötig").[9]

Nach der Bestellung des jetzigen Datenschutzbeauftragten im Jahre 2014 erfolgte mit Verfügung vom 10.05.2016 auch dessen Bestellung zum **IT-Sicherheitsbeauftragten**. Grundlegende und umfassende schriftliche Regularien zur **IT-Sicherheit**, die verwaltungsweit bekanntgegeben worden wären, waren hiernach für die Rechnungsprüfung allerdings nicht erkennbar.[10] Gleichwohl liegen Informationen zum Datenschutz auf der Webseite des Kreises Düren unter www.kreis-dueren.de/datenschutz und im Intranet des Kreises zum Abruf bereit.[11]

[9] Quelle: https://**www.im.nrw**/themen/verwaltung/datenschutz/behoerdlicher-datenschutz/aufgaben-der-behoerdlichen
[10] Hierzu ebenfalls Prüfbericht „*IT-Management*“ (Drs. Nr. 236/20)
[11] Auch interne Verfügungen thematisieren z.T. datenschutzrechtliche Aspekte, z.B. „*Einführung der sog. Link-Lösung*“ (vom 17.08.2018) oder „*Datenschutz bei dienstlichen E-Mails*“ (vom 30.06.2021). Gleichzeitig liegen *Informationsblätter* gemäß Art. 13 DSGVO, u.a. auch über die „*3G“ Kontrollen im Zuge der Corona Maßnahmen* (vom 25.11.2021) oder Hinweise zu *Pishing Mails* (Verweis auf Bundesamt für

5. Digitalisierung der Verwaltung

Nach der Hausverfügung der Verwaltung vom 21.12.2020 hat sich der Kreis Düren zum Ziel gesetzt, ab dem Jahr 2025 *medienbruchfrei* und *papierlos* zu arbeiten.

Unter Einbeziehung externer Beratung wurde zur Umsetzung dieses Konzepts eine **Digitalisierungsstrategie** erarbeitet. Diese sehe vor, dass diese Aufgabe im Hauptamt verortet ist. Das Programm werde aktuell konzeptioniert und in Kürze initiiert. Die Digitalisierung werde dezernats- und amtsweise erfolgen. Hierfür würden künftig Digitalisierungsmanager/-innen eingesetzt, die das große Ziel im Jahre 2025 sicherstellen sollen.

Im Rechnungsprüfungsausschuss am 06.09.2021 wurde im Rahmen der Prüfung der (veralteten) Aktenplanverwaltung (vgl. Drs. Nr. 246/21) zudem angekündigt, zukünftig jährlich einen **Digitalisierungsbericht** vorzulegen.[12]

Prüfbemerkung

Im Rahmen einer künftigen (vollständigen) Digitalisierung der Verwaltung sind grundlegende Aspekte des *Datenschutzes*, aber auch der *Datensicherheit* (s.o.) umfassend zu berücksichtigen. Diese Berücksichtigung muss parallel mit der Erarbeitung von *Digitalisierungsstrategien* vollzogen werden.

6. Prüfhistorie und Verfügungslage

Zum Stand der hiesigen Prüfung hat in der Kreisverwaltung nach wie vor die *Dienstanweisung und über den Datenschutz und die Datensicherheit* vom **05.11.2002** Gültigkeit.

Das Rechnungsprüfungsamt hatte datenschutzrechtliche Aspekte u.a. bereits im **Verwaltungsprüfbericht 2009/2010** aufgegriffen. Im Rahmen dieser Prüfung wurden

Verfassungsschutz vom 23.09.2021). Mustererklärungen *Informationspflicht bei Datenerhebung* oder *Mustervertrag Auftragsverarbeitung* liegen im Intranet der Kreisverwaltung ebenfalls vor. Zusätzlich zur Dienstanweisung (DA) zu Datenschutz und Datensicherheit beim Kreis Düren von 2002 existieren noch die DA für die Kommunikation in *sozialen Netzwerken* der Mitarbeiter/innen der Kreisverwaltung Düren, die Dienstvereinbarung (DV) *Telearbeit* oder die DV über die Nutzung und den Umgang mit dem *Internet* und dem Intranet in der Kreisverwaltung Düren

[12] Niederschrift Rechnungsprüfungsausschuss vom 06.09.2021 (Drs. Nr. 309/21, TOP 12).

Unschärfen in der internen Verfügungslage aufgezeigt und in einer Prüfbemerkung (Beanstandung) aufgegriffen.[13]

Seit diesem Verwaltungsprüfbericht steht eine Überarbeitung der entsprechenden Dienstanweisung aus. Zudem wurden angekündigte Richtlinien (vgl. Prüfbericht **IT-Management**, Drs. 246/20) ebenfalls noch *nicht* erarbeitet.

Damit *blieben* und *bleiben* insgesamt zentrale Angelegenheiten der öffentlichen Verwaltung, z.B. veraltete Aktenplanverwaltung und Aufgabengliederungsplan (Drs. 246/21), Datenschutz und Datensicherheit, Korruptionsgefährdete Bereiche (Drs. 287/07, 131/21), Rotationsprinzip (Drs. 267/09, 131/21, 306/21), veraltete Vergaberichtlinien (Drs. 320/20, 131/21), Zuwendungswesen (Drs. 284/12, 88/14, 136/14), Zentrales Vertragsmanagement (Drs. 181/09, 131/21) oder Internes Kontrollsystem (Drs. 53/14, 131/21) hinter den zeitlichen und tatsächlichen Erfordernissen unmittelbarer Bearbeitung zurück.

Prüfbemerkung B 1

1.) Die *Dienstanweisung über den Datenschutz und die Datensicherheit* aus dem **Jahre 2002** ist signifikant veraltet und berücksichtigt weder die Rechtsentwicklungen im Datenschutz oder die Neuregelungen der Datenschutzgrundverordnung noch die sich fortentwickelnden Möglichkeiten und Gefahren, die sich im Rahmen zunehmender Digitalisierung für die Datensicherheit einer Verwaltung (und im Allgemeinen) ergeben. Damit ist auch *keine* rechtssichere Handlungsgrundlage für die Tätigkeit der Organisationseinheiten im Hause, des behördlichen **Datenschutzbeauftragten** oder des **IT-Sicherheitsmanagements** existent.

2.) Die technischen Entwicklungen der vergangenen 20 Jahre (**Digitalisierung**), die daraus resultierenden Risiken und die erforderlichen Vorkehrungen der Verwaltung werden von der vg. Dienstanweisung ebenfalls *nicht* im Ansatz erfasst. Dies tangiert nicht nur den **Datenschutz** selbst, sondern auch die **Sicherheit** der Daten und damit letztlich das **Interne Kontrollsystem**, zu dessen Aufbau die Verwaltung verpflichtet und dessen Wirksamkeit von der örtlichen Rechnungsprüfung zu überprüfen ist (§ 104 Abs. 1 Nr. 6 GO).

3.) Für die Rechnungsprüfung ist derzeit kein Grund erkennbar, warum die Prüfbemerkung aus dem Jahre 2009/2010 bzw. die Überarbeitung der Dienstanweisung aus dem Jahre 2002

[13] Verwaltungsprüfbericht 2009/2010 (Drs. Nr. 420/10)

auch **nach zwölf Jahren** immer noch nicht vollzogen wurde bzw. die Aufarbeitung dieser Thematik seit Jahren lediglich in den „*Übersichten über den aktuellen Stand der noch abzuarbeitenden Hinweise, Anmerkungen und Feststellungen zu Beratungsergebnissen aus den Sitzungen des Rechnungsprüfungsausschusses*“ (vgl. zuletzt Drs. Nr. 444/21) zwar aufgeführt aber nicht abgearbeitet wird.

4.) Für den Bereich der **Datensicherheit** gibt es neben der veralteten Dienstanweisung aus dem Jahre 2002 ebenfalls keine erkennbare oder verwaltungsweit geltende und aktuelle Verfügungslage, die diese Thematik umfassend aufgreifen oder fortlaufend darstellen würde. Die zum Prüfbericht „*IT-Management*“ (Drs. 236/20) angekündigten Richtlinien fehlen bisher ebenfalls.

5.) In diesem Sinne ist unabdingbar, dass die Aspekte von Datenschutz und Datensicherheit verwaltungsseitig eine höhere Aufmerksamkeit erfordern und nachhaltiger aufgegriffen werden müssen. Dies gilt insbesondere im Rahmen der erklärten Absicht, eine umfassende **Digitalisierung der Verwaltung** entwickeln und etablieren zu wollen.

6.) Die Rechnungsprüfung empfiehlt vorliegend dringend eine zeitnahe Überarbeitung und Aktualisierung der grundlegenden Regularien zum *Datenschutz* und zur *Datensicherheit* auf den neuesten Rechtsstand und den Stand der Technik und eine anschließende verbindliche Vorgabe für die Tätigkeit aller Organisationseinheiten im Hause.

7. Ausräumverfahren und Stellungnahme der Verwaltung

Der Prüfberichtsentwurf wurde der Verwaltung am **15.12.2021** zugeleitet. Die Verwaltungsstellungnahme hierzu ging am **01.03.2022** ein. Darin führt die Verwaltung aus:

> *Für die Übersendung des o. g. Prüfberichts danke ich und nehme nachfolgend wie folgt Stellung:*
>
> *Die Prüfbemerkung(en) werden vollumfänglich akzeptiert. Die Verwaltung dankt der Rechnungsprüfung für die abermalige Sensibilisierung für die Thematik. Die Erarbeitung der angesprochenen Regelwerke wurde auch nach dem personellen Wechsel in der Leitung des Hauptamtes bereits im vergangenen Jahr priorisiert, konnte aber insbesondere pandemiebedingt und angesichts der großen Tragweite und Komplexität der Thematik noch nicht abgeschlossen werden. Die Verwaltung ist fest entschlossen, hier so schnell wie möglich die erforderlichen Resultate zu erzielen.*
>
> *Der Vollständigkeit halber möchte die Verwaltung sich den Hinweis erlauben, dass in der Praxis auch in enger Zusammenarbeit mit dem Datenschutz- und IT-Sicherheitsbeauftragten trotz der noch ausstehenden Aktualisierung / Erarbeitung der Regelwerke den Belangen des Datenschutzes und der Datensicherheit stets bestmöglich Rechnung getragen wird.*

8. Abschließende Bewertung der Rechnungsprüfung

Die Rechnungsprüfung nimmt die Stellungnahme der Verwaltung zur Kenntnis. Die Prüfbemerkungen wurden verwaltungsseitig akzeptiert. Das entsprechende Problembewusstsein für *nicht vorhandene* oder *veraltete* Regularien und für die Bedeutung dieser Prüfungsthematik für die Gesamtverwaltung wurde dokumentiert. Über den Fortgang der Angelegenheit und die Erarbeitung aktueller Regelungen sollte die Verwaltung im Rahmen des *Prüfcontrollings* zeitnah berichten. Hiernach kann die Prüfbemerkung als ausgeräumt angesehen werden.

9. Veröffentlichung des Prüfberichts

Dieser Prüfbericht wird zunächst in **nichtöffentlicher** Sitzung des Rechnungsprüfungsausschusses beraten. Er enthält gleichwohl keine Sachverhalte oder Ausführungen, die im Sinne des Kommunalverfassungsrechts einer Nichtöffentlichkeit oder besonderen Schutzwürdigkeit unterliegen würden.

Die Einzelprüfberichte können sodann **nach** ihrer Beratung im Rechnungsprüfungsausschuss vom Rechnungsprüfungsamt der Öffentlichkeit zugänglich gemacht werden.

Hierbei sind personen- oder unternehmensbezogene Daten, soweit vorhanden, zu anonymisieren (§ 6 Abs. 3 RPO).