Leitlinie zum Datenschutz und zur Datensicherheit der Stadt Essen

1. Rechtliche Grundlage, Begriffe, Ziele

Die Stadt Essen ist bei ihrer Aufgabenwahrnehmung von genauen Informationen und einer zuverlässigen Informationstechnik (IT) abhängig. Durch den zunehmenden IT-Einsatz ergeben sich Gefahren, die zu einer Gefährdung der Aufgabenerfüllung und zu einer Verletzung des verfassungsrechtlich geschützten Rechtes auf informationelle Selbstbestimmung der betroffenen Person führen können (Art. 4 Abs. 2 Verfassung für das Land NRW und § 1 Datenschutzgesetz NRW - DSG NRW). Informationen und die für die Informationsverarbeitung benutzten IT-Systeme sind daher wertvoll und schützenswert.

Als **IT-System** werden die Hard- und Software bezeichnet, die geeignet sind, Daten zu speichern, zu verarbeiten oder zu übermitteln.

Datenschutz bezeichnet den Schutz des Einzelnen davor, dass er durch die Verarbeitung seiner personenbezogenen Daten in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

Datensicherheit umfasst alle technischen und organisatorischen Maßnahmen im Sinne des § 10 DSG NRW oder vergleichbarer Vorschriften des Bundesdatenschutzgesetzes (BDSG), die die Funktions-Fähigkeit der IT-Systeme und den Schutz des informationellen Selbstbestimmungsrechtes der Betroffenen sicherstellen.

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (z.B. Name, Anschrift, Geburtsdatum, familiäre Situation, Personalnummer, Beurteilungen, Fotos, berufliche Position).

Folgende im § 10 DSG NRW beschriebenen Sicherheitsziele sind zu gewährleisten:

Vertraulichkeit

Nur Befugte dürfen Informationen zur Kenntnis nehmen können (Schutz vor unbefugtem Zugriff).

Integrität

Informationen müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Schutz vor unbefugten Veränderungen, Verlust, Zerstörung).

Verfügbarkeit

Informationen sollen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Authentizität

Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können. An der richtigen Herkunft der Daten dürfen keine Zweifel bestehen und die Urheber der Daten müssen korrekt identifiziert werden können.

Revisionsfähigkeit

Es muss nachprüfbar sein, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Transparenz

Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sollen vollständig, aktuell und in einer Weise dokumentiert sein, dass sie in zumutbarer Zeit nachvollzogen werden können.

Die zu treffenden technischen und organisatorischen Maßnahmen sind nach § 10 DSG NRW auf der Grundlage eines zu dokumentierenden Sicherheitskonzeptes zu ermitteln.

Ziel eines Sicherheitskonzeptes ist es, Risiken und Bedrohungen, die durch die Verarbeitung von Informationen entstehen, zu reduzieren und dabei ein angemessenes Sicherheitsniveau zu erreichen. Die vorliegende Leitlinie zum Datenschutz und zur Datensicherheit ist der grundlegende Baustein des IT-Sicherheitskonzeptes der Stadt Essen und bildet den Rahmen für Standards und Richtlinien.

2. Leitsätze

Die Gewährleistung von Datenschutz und Datensicherheit ist ein zunehmend wichtiger Faktor bei der Erbringung unserer Dienstleistungen und wird durch die folgenden Leitsätze festgeschrieben:

Leitsatz 1:

Die Stadt Essen schützt die personenbezogenen oder sonstigen vertraulich zu behandelnden Daten ihrer Bürgerinnen und Bürger, ihrer Kundinnen und Kunden sowie ihrer Beschäftigten.

Schutzbedarf besteht nicht nur für personenbezogene Daten, sondern auch für sonstige vertrauliche Informationen, wie z. B. Finanz- oder Planungsdaten.

Leitsatz 2:

Die Verarbeitung personenbezogener Daten ist ohne gesetzliche Grundlage oder ohne Einwilligung des Betroffenen verboten.

Es werden nur die Daten verarbeitet, die für die rechtmäßige Aufgabenerfüllung erforderlich sind. Die Daten werden nur für Zwecke verarbeitet, für die sie erhoben worden sind. Ausnahmetatbestände sind abschließend in § 13 Abs. 2 DSG geregelt.

Leitsatz 3:

Die Gewährleistung von Datenschutz und Datensicherheit ist Aufgabe und Verpflichtung für alle Beschäftigten.

Die Mitarbeiter/innen sind als Nutzer von IT-Systemen bei der Verarbeitung von Daten verpflichtet, diese Leitlinie und die daraus abgeleiteten Standards und Richtlinien zu beachten.

Leitsatz 4:

Die Führungskräfte sind für die Einhaltung eines angemessenen Sicherheitsstandards im Datenschutz und in der Datensicherheit verantwortlich.

Alle Führungskräfte sind dafür verantwortlich, die bestehenden Sicherheitsstandards in ihrem Fach- bzw. Geschäftsbereich umzusetzen und aufrecht zu erhalten. Hierfür sind die organisatorischen, personellen und technischen Voraussetzungen zu realisieren.

3. Verantwortlichkeiten

3.1 Geschäfts- und Fachbereiche als Informationseigentümer

Für alle Daten, die innerhalb der Stadt Essen verarbeitet werden, tragen die Geschäfts- und Fachbereiche als Informationseigentümer die Verantwortung für deren ordnungsgemäße Verarbeitung. Dies ergibt sich aus der Aufgabenstellung des Geschäfts- bzw. Fachbereiches. Hierbei sind die geltenden Regelungen zu beachten.
Wert und Bedeutung der Informationen bestimmen dabei die technischen und organisatorischen Maßnahmen, die von den Führungskräften zu treffen sind, um die genannten Sicherheitsziele zu erreichen. Jede Organisationseinheit legt den Zugriff auf ihre Daten fest und definiert hierzu Art und Umfang der Nutzung. Der Zugriff auf die Daten hat sich an der Aufgabenerfüllung zu orientieren.

3.2 Mitarbeiter/innen als Nutzer

- nutzen die ihnen zugänglichen technischen Anlagen, Verfahren und Dateien mit personenbezogenen Daten oder Geschäftsgeheimnissen im Rahmen der ihnen übertragenen Aufgaben,
- achten darauf, dass nur Berechtigte auf die von ihnen verwalteten personenbezogenen oder anderen vertraulichen Daten Zugriff haben,
- sind verpflichtet, sich die notwendigen Kenntnisse der gesetzlichen Grundlagen und behörden-internen Dienstanweisungen / Dienstvereinbarungen zum Datenschutz und zur Datensicherheit anzueignen (entsprechende Informationen und Schulungen werden angeboten) und
- sind verpflichtet, Regelverletzungen oder Sicherheitslücken unverzüglich der Führungskraft und/oder der Stabsstelle Datenschutz mitzuteilen.

3.3 Interne oder externe Dienstleister als Treuhänder

Der Treuhänder verarbeitet Daten im Auftrag des Informationseigentümers. Er ist für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten in dem vom Informationseigentümer festgelegten Umfang nach Maßgabe dieser Leitlinie verantwortlich und verpflichtet, den Informationseigentümer bei erkennbaren Mängeln der Sicherheitsvorgaben zu informieren. Interner Treuhänder ist grundsätzlich das Essener Systemhaus.

3.4 Verstöße

Die Nichteinhaltung oder bewusste Verletzung dieser Leitlinie oder der daraus abgeleiteten Regelungen kann dienst-, arbeits-, straf- und zivilrechtliche Folgen nach sich ziehen. Dies gilt insbesondere, wenn

- der Stadt Essen durch die Gefährdung der Sicherheit von Informationen ein finanzieller Verlust zugefügt wird,
- auf Informationen unberechtigt zugegriffen wird oder diese unberechtigt übermittelt oder verändert werden,
- die Sicherheit der Beschäftigten oder der städtischen Vertragspartner gefährdet wird oder
- der gute Ruf der Stadt Essen beeinträchtigt wird.

4. Umsetzungsempfehlungen

Detaillierte Zielsetzungen und Anforderungen für Kontrollen zur Einhaltung dieser Leitlinie werden in einem IT-Sicherheitskonzept dokumentiert. Das IT-Sicherheitskonzept wird gemeinsam von einer Arbeitsgruppe unter Federführung der Stabsstelle Datenschutz entwickelt und ständig fortgeschrieben.

Basis für die Umsetzung des Sicherheitskonzeptes ist das Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik). Das Grundschutzhandbuch des BSI geht von differenzierten Schutzanforderungen aus und klassifiziert Informationssysteme nach Schutzbedarfsstufen.
Durch geeignete Anwendung von infrastrukturellen, organisatorischen, personellen und technischen Standardsicherheitsmaßnahmen wird ein angemessenes Sicherheitsniveau für IT-Systeme erreicht.

5. Inkrafttreten

Die Leitlinie zum Datenschutz und zur Datensicherheit der Stadt Essen tritt mit sofortiger Wirkung in Kraft.

Essen, den 27.10.2004

Dr. Reiniger

Oberbürgermeister