

24 Leitlinie zu IT-Sicherheit und Datenschutz der Landeshauptstadt Düsseldorf

01
10/1

16.02.2004

Präambel

Der Erfolg unserer täglichen Arbeit hängt unmittelbar von genauen Informationen und einer zuverlässigen IT-Infrastruktur ab. Informationen und die für Informationsverarbeitung und Kommunikation benutzten Einrichtungen sind daher wertvoll und schützenswert.

Von größter Wichtigkeit ist neben der Genauigkeit und Verfügbarkeit auch die Vertraulichkeit der Informationen. Alle Mitarbeiterinnen und Mitarbeiter müssen sich daher der Notwendigkeit von IT-Sicherheit und Datenschutz bewusst sein und entsprechend handeln. Die in dieser Leitlinie genannten Grundsätze sind gesetzlich verankert. Die Leitlinie ist somit nicht nur eine verbindliche Erklärung zu IT-Sicherheit und Datenschutz, sondern auch eine Verpflichtung gegenüber den Bürgerinnen und Bürgern, Behörden, Unternehmen und Partnern.

1 Einleitung

Die vorliegende Leitlinie zu IT-Sicherheit und Datenschutz erläutert die Bedeutung von Informationen für unsere Verwaltung und bildet den Rahmen für Standards und Richtlinien. Jede Mitarbeiterin und jeder Mitarbeiter hat daher diese Leitlinie und die daraus abgeleiteten Regelungen zu beachten.

Die nachfolgenden Leitsätze umfassen Sicherheitsanforderungen zur Planung, zum Betrieb von IT-Systemen und Anwendungen sowie zur Gestaltung der gesamten IT-Infrastruktur.

Bei der Vorbereitung und Umsetzung von Maßnahmen zu IT-Sicherheit und Datenschutz trägt jede Führungskraft für ihren Geschäftsbereich die Verantwortung. Dabei hat IT-Sicherheit zum Ziel, Systeme der Informationstechnik und Telekommunikation, Netze und Anwendungen vor möglichen Bedrohungen zu schützen, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen zu gewährleisten.

Vertraulichkeit

Es ist sicherzustellen, dass nur Befugte Informationen zur Kenntnis nehmen können.

Integrität

Es ist sicherzustellen, dass Informationen während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

Verfügbarkeit

Es ist sicherzustellen, dass Informationen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Bei der Verarbeitung personenbezogener Daten stellen zusätzlich technische und organisatorische Maßnahmen im Sinne eines effektiven Datenschutzes sicher, dass Authentizität, Revisionsfähigkeit und Transparenz der Datenverarbeitung gewährleistet werden.

Authentizität

Personenbezogene Daten sollen jederzeit ihrem Ursprung zugeordnet werden können.

Revisionsfähigkeit

Es soll festgestellt werden können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Transparenz

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

2 Leitsätze

Zu den Grundsätzen von IT-Sicherheit und Datenschutz werden fünf Leitsätze aufgestellt, die in den folgenden Abschnitten erläutert werden.

Leitsatz 1:

Im Rahmen der Erfüllung unserer Aufgaben verarbeiten wir nur die personenbezogenen oder sonstigen vertraulich zu behandelnden Daten unserer
– *Bürgerinnen und Bürger,*
– *Mitarbeiterinnen und Mitarbeiter,*
die erforderlich sind.

Sicherheitsmaßnahmen erstrecken sich auf den Schutz der personenbezogenen Daten nicht nur der Bürgerinnen und Bürger, sondern auch der Mitarbeiterinnen und Mitarbeiter.

Zu berücksichtigen ist außerdem, dass weitere Informationen, wie zum Beispiel Finanz- oder Planungsdaten, schutzbedürftig sind.

Leitsatz 2:

Wir schützen vertrauliche Informationen vor dem Zugriff Unbefugter und stellen sicher, dass autorisierte Nutzer jederzeit auf die benötigten Informationen zugreifen können.

Durch geeignete Maßnahmen muss gewährleistet sein, dass Zugriffsrechte auf schutzbedürftige Informationen restriktiv vergeben werden können. Sofern sich Nutzer für den Zugriff auf die von ihnen benötigten Informationen authentifiziert haben, ist sicherzustellen, dass die Informationen im Sinne der definierten Ziele zur Verfügung stehen.

Leitsatz 3:

IT-Sicherheit und Datenschutz sind integrale Bestandteile unseres Handelns.

IT-Sicherheit und Datenschutz sind zunehmend wichtige Faktoren geworden, damit unsere Dienstleistungen bürgerorientiert erbracht werden können. Nach Maßgabe dieser Leitlinie trägt jede Organisationseinheit in ihrem Geschäftsbereich dafür die Verantwortung. Wert und Bedeutung der Informationen bestimmen dabei die Maßnahmen, die zu treffen sind, um die genannten Ziele zu erreichen.

Leitsatz 4:

Wir gehen verantwortungsvoll mit Informationstechnologie um.

Alle Mitarbeiterinnen und Mitarbeiter sind verpflichtet, die Sicherheit der Informationen und Informationssysteme, auf die sie Zugriff haben, zu wahren und aktiv zu unterstützen. Informationssysteme dienen der Aufgabenerfüllung. Mit ihnen ist angemessen im Rahmen der geltenden Regelungen umzugehen.

Leitsatz 5:

Wir sind alle dafür verantwortlich, die Rahmenbedingungen für einen angemessenen Sicherheitsstandard zu schaffen.

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

3 Verantwortlichkeit

Für alle Informationen, die in der Stadtverwaltung verarbeitet werden, trägt eine Organisationseinheit als „Herr der Daten“ die Verantwortung. Dies ergibt sich aus der Aufgabenstellung des Fachbereiches.

3.1 „Herr der Daten“¹⁾

Jede Organisationseinheit ist für die Maßnahmen zum Schutz ihrer Informationen verantwortlich. Hierbei sind die geltenden Regelungen zu beachten. Sie legt den Zugriff auf ihre Informationen fest und definiert hierzu Art und Umfang der Nutzung. Der Zugriff auf die Informationen hat sich an der Aufgabenerfüllung zu orientieren. Informationen können auch treuhänderisch verarbeitet werden.

3.2 Nutzer

Die Nutzer von Systemen sind bei der Verarbeitung von Informationen verpflichtet, diese Grundsätze und die daraus abgeleiteten Standards und Richtlinien zu beachten.

Wem Regelverletzungen oder Sicherheitslücken auffallen, hat dies unverzüglich der Führungskraft mitzuteilen.

1) Mit diesem in der Informationstechnik üblichen Eigenbegriff soll zum Ausdruck gebracht werden, wer die Verantwortung für die ordnungsgemäße Verarbeitung der Daten trägt.

3.3 Treuhänder

Der Treuhänder verarbeitet Informationen im Auftrag des „Herrn der Daten“ und kann sowohl interner (Amt 10) als auch externer Dienstleister sein. Er ist für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen in dem vom „Herrn der Daten“ festgelegten Umfang nach Maßgabe dieser Grundsätze verantwortlich. Der Treuhänder ist verpflichtet, den „Herrn der Daten“ bei erkennbaren Mängeln der Sicherheitsvorgaben zu informieren.

4 Umsetzungsempfehlungen

4.1 Sicherheitsmanagement

Es wird ein Sicherheitsmanagement aufgebaut, das diese Leitlinie fortschreibt, die daraus abgeleiteten Standards und Richtlinien erstellt, sie veröffentlicht und permanent auf ihre Wirksamkeit hin überprüft.

4.2 Unabhängige Prüfung

In besonders sicherheitskritischen Bereichen wird eine unabhängige Prüfung angestrebt, damit die Verarbeitung von Informationen und die Anwendung der Sicherheitsstandards von unabhängiger Seite beurteilt werden.

4.3 IT-Sicherheitsrichtlinien

Die aus dieser Leitlinie abgeleiteten Standards und Richtlinien werden vom Amt für Informationstechnik und Organisationsentwicklung unter Beteiligung des Datenschutzbeauftragten erlassen.

5 Verletzung der Sicherheit

Die an der Verarbeitung von Informationen Beteiligten können für schuldhafte Verstöße gegen die aus dieser Leitlinie abgeleiteten Standards und Richtlinien nach den geltenden Rechtsvorschriften zur Verantwortung gezogen werden. Dies gilt insbesondere, wenn

- der Landeshauptstadt Düsseldorf 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 werden oder
- der gute Ruf der Landeshauptstadt Düsseldorf beeinträchtigt wird.

Nähere Regelungen werden in den IT-Sicherheitsrichtlinien getroffen.

MittBl. 3/2004

Joachim Erwin
Oberbürgermeister