Stadt Leipzig

Leitlinie für Informationssicherheit und Datenschutz

Inhaltsverzeichnis

1. Vorbemerkung

Diese Leitlinie beschreibt die strategischen Grundlagen zur Gewährleistung der Informationssicherheit und des Datenschutzes in der Stadt Leipzig.

Die Leitlinie für Informationssicherheit und Datenschutz

- beschreibt den Stellenwert der Informationssicherheit und des Datenschutzes,
- enthält das Bekenntnis der Behördenleitung zu ihrer Verantwortung für die Informationssicherheit und den Datenschutz,
- legt die Sicherheitsstrategie fest,
- formuliert die allgemeinen Sicherheitsziele,
- definiert die Sicherheitsorganisation,
- verpflichtet zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit und des Datenschutzes,

Diese Leitlinie bezieht sich auf:

- BSI-Standard 200-2 (IT-Grundschutz-Methodik)
- EU-Datenschutz-Grundverordnung (EU-DSGVO)
- Standard-Datenschutzmodell (SDM)

2. Geltungsbereich

Die Leitlinie für Informationssicherheit und Datenschutz gilt für alle Organisationseinheiten der Stadtverwaltung Leipzig. Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Bediensteten der Stadtverwaltung Leipzig zu beachten und einzuhalten.
Den Eigenbetrieben der Stadt Leipzig wird die Anwendung und Umsetzung dieser Leitlinie empfohlen.

3. Leitbild und Selbstverpflichtung

Die Behördenleitung und die Bediensteten der Stadt Leipzig sind sich ihrer Verantwortung bei der Verarbeitung von personenbezogenen und anderen Daten und im Umgang mit den dafür eingesetzten informationstechnischen Infrastrukturen bewusst. Die Umsetzung von In-

formationssicherheit und Datenschutz hat einen hohen Stellenwert. Es werden alle notwendigen geeigneten und angemessenen Maßnahmen getroffen, um negative materielle und immaterielle Folgen für Betroffene und die Stadt Leipzig auszuschließen.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit für die Fachaufgaben / Geschäftsprozesse zu organisieren, welches gleichzeitig den Anforderungen des Datenschutzes gerecht wird.

4. Verantwortlichkeiten und Rollen

4.1. Gesamtverantwortung

Der Oberbürgermeister trägt die Gesamtverantwortung für die Informationssicherheit und die Einhaltung des Datenschutzes.

Die Verantwortung umfasst:

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit und Datenschutz,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits- und Datenschutz-Managements,
- die Bereitstellung der erforderlichen Ressourcen, für die Planung und Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen,
- das Einbetten der Informationssicherheit und des Datenschutzes in die Strukturen, und Arbeitsabläufe der Stadtverwaltung.

4.2. Zentrales Datenschutz- und Informationssicherheitsmanagement

4.2.1 Informationssicherheitsbeauftragter

Die Stadt Leipzig hat als zentrale Sicherheitsinstanz einen Informationssicherheitsbeauftragten (ISB) ernannt. Der ISB ist dem Oberbürgermeister direkt unterstellt, arbeitet fachlich weisungsfrei und ist gegenüber allen Bediensteten weisungsbefugt, soweit Belange der Informationssicherheit betroffen sind.
Der Informationssicherheitsbeauftragte hat Zutrittsrecht zu allen Räumen der Stadtverwaltung.
Er hat ein direktes Vortragsrecht bei allen Amtsleitern, Beigeordneten und dem Oberbürgermeister.

4.2.2 Datenschutzbeauftragter

Für die Wahrnehmung der Aufgaben gem. Art. 39 DSGVO hat die Stadtverwaltung einen behördlichen Datenschutzbeauftragten (bDSB) benannt. Der bDSB ist dem Oberbürgermeister

direkt unterstellt, arbeitet fachlich weisungsfrei und ist nicht weisungsbefugt.
Er hat ein direktes Vortragsrecht bei allen Amtsleitern, Beigeordneten und dem Oberbürgermeister.

4.2.3 Informationssicherheitsmanagementteam

Zur Unterstützung des ISB und bDSB wird ein Informationssicherheitsmanagement-Team (ISM-Team) gebildet, um bei strategischen Entscheidungen, bei der Bewältigung von Sicherheitsvorfällen oder Einzelmaßnahmen (z.B. bei Projekten entsprechender Größenordnung) die Informationssicherheits- und Datenschutzbelange ausreichend zu berücksichtigen.

4.3. Dezentrale Gewährleistung von Datenschutz und Informationssicherheit
4.3.1 Informationseigentümer

Die Gewährleistung von Informationssicherheit und Datenschutz ist integraler Bestandteil jeder Fachaufgabe. Für jede Fachaufgabe / jeden Geschäftsprozess gibt es einen Informationseigentümer, der für alle Fragen der Informationsverarbeitung verantwortlich ist. Die Zuständigkeit der Informationseigentümer umfasst daher auch Maßnahmen zur Umsetzung und Aufrechterhaltung von Datenschutz und Informationssicherheit.

Im Rahmen der Aufgabenzuständigkeit der Dezernate, Ämter und Referate obliegt diese Funktion der jeweiligen Leitung, die hierzu mit dem zentralen Informationssicherheits- und Datenschutzmanagement zusammenarbeitet.

4.3.2 Die Verantwortung der Bediensteten

Alle Bedienstete gewährleisten die Informationssicherheit und den Datenschutz durch verantwortungsbewusstes Handeln und halten die für die Aufgabenerfüllung relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

5. Sicherheitsziele

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für die Stadtverwaltung die nachstehenden Sicherheitsziele festgelegt, für die geeignete Sicherheitsniveaus definiert werden:

- **Vertraulichkeit**
  Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.

- **Integrität**
  Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten

muss jederzeit gewahrt sein. Dieses umfasst auch die unberechtigte Erstellung oder Änderung von Informationen.

- **Verfügbarkeit**
  Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zur Verfügung stehen.

Bei der Verarbeitung personenbezogener Daten sind zusätzlich folgende Sicherheitsziele zu gewährleisten:

- **Nichtverkettung**
  Datenverarbeitung ist auf den Erhebungszweck und rechtmäßige Zweckänderung beschränkt.

- **Transparenz**
  Information und Auskunft der betroffenen Personen, welche Daten wofür verarbeitet werden, sind gewährleistet. Sämtliche Verarbeitungstätigkeiten sind vordefiniert und nachvollziehbar dokumentiert.

- **Intervenierbarkeit**
  Wahrnehmung der Betroffenenrechten ist gewährleistet.

6. Sicherheitsstrategie

Die Sicherheitsstrategie der Stadtverwaltung Leipzig ist es, mit wirtschaftlichem Ressourceneinsatz ein Risiko-angemessenes Sicherheitsniveau zu erreichen und aufrechtzuerhalten. Dazu wird ein Informationssicherheitsmanagementprozess eingeführt, der sich an der IT-Grundschutzvorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert und als kontinuierlicher Prozess unter besonderer Berücksichtigung des Datenschutzes gestaltet wird.

Der Prozess umfasst die Schritte

- **Planung:** Festlegung der Vorgaben für den Sicherheitsprozess und das ISMS

- **Umsetzung:** Aufbau eines ISMS, Erstellung und Umsetzung eines Sicherheitskonzeptes sowie Etablierung des Sicherheitsprozesses

- **Überprüfung:** Erfolgskontrolle der Erreichung der Sicherheitsziele

- **Aufrechterhaltung:** Durchführung von Korrekturen zur Optimierung des Sicherheitsprozesses und der Sicherheitsorganisation

Die Sicherheitsstrategie umfasst die gesamte Informationsverarbeitung in der Stadtverwaltung.

Das ISMS soll dem jeweiligen Schutzzweck angemessene Sicherheitsmaßnahmen definieren und für deren wirtschaftliche Umsetzung sorgen. Bei der Auswahl der Umsetzung von

Sicherheitsmaßnahmen ist darauf zu achten, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Geschäftsprozessen / Fachaufgaben unnötig zu beeinträchtigen.

Die Sicherheitsstrategie wird von den folgenden Grundsätzen geprägt:

- **Zentrale Rolle der Informationssicherheit / Datenschutz:** Die Informationssicherheit und der Datenschutz wird bei Änderungen und Neuerungen von Beginn an mitberücksichtigt.

- **Verhältnismäßigkeit der Sicherheitsmaßnahmen:** Aufwand und Ergebnis der eingesetzten Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinanderstehen.

- **Sicherheit für nachhaltige Verfügbarkeit:** Um eine langfristige Verfügbarkeit zu erreichen, ist eine kurzfristige Einschränkung bei Funktionalität und Komfort vertretbar.

- **Prinzip des Schutzbedarfs:** Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse und Fachaufgaben, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung Sicherheitsziele entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden sowie Risiken für die Rechte und Freiheiten natürlicher Personen realistisch einzuschätzen.

- **Minimalprinzip des Zugriffs:** Der Zugriff auf IT-Systeme und Daten wird auf die notwendigen Personen und Systeme beschränkt.

- **Restriktives Nutzungsprinzip:** Es werden nur Berechtigungen erteilt, die zur Erfüllung der jeweiligen Aufgabe tatsächlich benötigt werden.

- **Bereitstellung von ausreichenden Ressourcen**: Um ein angemessenen Sicherheitsniveaus zu erreichen und aufrecht zu erhalten, werden ausreichende finanzielle und personelle Ressourcen und letzteren der notwendige zeitliche Freiraum bereitgestellt.

- **Einbindung aller Bedienstete:** Alle Bedienstete werden in den Sicherheitsmanagementprozess zur Unterstützung der Sicherheitsstrategie eingebunden und hinsichtlich der Informationssicherheit sensibilisiert.

7. Umsetzung der Sicherheitsstrategie

Auf der Grundlage dieser Leitlinie werden eine Dienstanweisung zur Informationssicherheit und Datenschutz sowie weitere, auch fachspezifischer Richtlinien und Informationssicherheitskonzepte zur Umsetzung der Sicherheitsstrategie erstellt.

Die für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen notwendigen Ressourcen sind bereitzustellen. Diese Maßnahmen müssen in einem angemessenen Verhältnis zu den mit der Datenverarbeitung verbundenen Risiken für die betroffenen Personen, Dritter und der Stadt Leipzig stehen.

8. Verpflichtung zur kontinuierlichen Verbesserung

Die Verwaltungsleitung unterstützt den Prozess zur Optimierung der Informationssicherheit und des Datenschutzes. Der Prozess muss regelmäßig auf seine Aktualität, Wirksamkeit und die Übereinstimmung mit den Informationssicherheitszielen überprüft werden. Die Sicherheitsmaßnahmen sind regelmäßig daraufhin zu untersuchen, ob sie den Bedienstete bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit und den Datenschutz zu verbessern und ständig auf dem aktuellen Stand zu halten.