Leitlinie zur Umsetzung des Datenschutzes bei der Stadt Rees

I. Bedeutung des Datenschutzes und sein Stellenwert

Die Stadtverwaltung Rees versteht sich als bürgerfreundlicher Dienstleistungsbetrieb.

Ihr Handeln richtet sich u. a. nach folgenden Grundsätzen:

1. Datenschutz ist Schutz des Grundrechts auf informationelle Selbstbestimmung.

2. Datenschutz ist unverzichtbarer Bestandteil und Qualitätsmerkmal der Aufgabenerledigung.

Jede Verwaltungstätigkeit, bei der personenbezogene oder –beziehbare Daten verarbeitet werden, hat die rechtlichen, informationstechnischen und organisatorischen Anforderungen des Datenschutzes zu berücksichtigen.

II. Geltungsbereich

Diese Leitlinie gilt für alle städtischen Organisationseinheiten (Dezernate, Fachbereiche), für die städtischen Eigenbetriebe sowie für die eigenbetriebsähnlichen Einrichtungen.

III. Zielsetzungen

1. Hohe Verlässlichkeit der Datenverarbeitung, besonders hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Daten

2. Beachtung der datenschutzrechtlichen Rahmenbedingungen und Umsetzung geeigneter technischer und organisatorischer Maßnahmen

3. Wahrung des guten Rufs der Stadtverwaltung Rees in der Öffentlichkeit und des Vertrauens der Bürger in datenschutzgerechtes Verwaltungshandeln

IV. Leitsätze

In Abwägung der Sensibilität der zu schützenden Daten, der Risiken sowie des Aufwands wird in der Stadtverwaltung Rees ein angemessenes Datenschutzniveau gewährleistet.

Diese Leitsätze stellen eine verbindliche Erklärung und Verpflichtung gegenüber Bürgerinnen und Bürger, anderen Behörden, Unternehmen sowie den eigenen Mitarbeiterinnen und Mitarbeitern dar.

V. Umsetzung des Datenschutzes

1. Verantwortung

Die Behördenleitung trägt die Gesamtverantwortung für den Datenschutz und unterstützt die in dieser Leitlinie formulierten Ziele und die daraus abgeleiteten Konzepte und Maßnahmen.

Ungeachtet dieser Gesamtverantwortung trägt jede Führungskraft ausgehend von ihrer fachlichen Verantwortung auch die Verantwortung für den Datenschutz in ihrem Aufgabenbereich. Die Führungskräfte übernehmen hierbei eine Vorbildfunktion.

Die Mitarbeiterinnen und Mitarbeiter sind sich der Wichtigkeit des Datenschutzes bewusst und handeln entsprechend. Sie halten die für den Datenschutz relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen in ihrem Verantwortungsbereich ein.

2. Organisation

Die Organisation des Datenschutzes und der Datensicherheit wird in städtischen Dienstanweisungen geregelt.

3. Bestellung eines Datenschutzbeauftragten

Der Bürgermeister der Stadt Rees bestellt bzw. benennt eine(n Datenschutzbeauftragte(n) und eine (n) Stellvertreter(in).

Der/Die Datenschutzbeauftragte(r) hat die Aufgabe, auf die Einhaltung der Datenschutzvorschriften hinzuwirken und die Verantwortungsträger zu beraten. Seine/Ihre Aufgaben und Zuständigkeiten ergeben sich insbesondere aus Artikel 39 der Verordnung (EU) 2016/679 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 (Datenschutz-Grundverordnung) (DS-GVO).

4. Ressourcen

Die Behördenleitung sorgt dafür, dass ausreichende finanzielle, personelle und zeitliche Ressourcen zur Einhaltung eines angemessenen Datenschutzniveaus zur Verfügung stehen.

5. Beteiligung

Der Datenschutz ist Bestandteil aller Prozesse und Projekte der Stadtverwaltung Rees, bei denen personenbezogene Daten verarbeitet werden. Somit werden Datenschutzanforderungen beispielsweise nicht nur bei der Beschaffung von Hard- und Software, sondern auch bei der Gestaltung von Prozessen sowie bei der Aus- und Weiterbildung von Mitarbeiterinnen und Mitarbeitern mit berücksichtigt.

6. Kernaussagen der Datenschutz-Grundverordnung

Beim Umgang mit personenbezogenen Daten in der Stadt Rees müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen der DS-GVO sowie des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und -Anwendungen sind zentrale Zielsetzungen zur Gewährleistung des Rechts auf informationelle Selbstbestimmung.

Begriff der personenbezogenen Daten (Art. 4 Nr. 1 DS-GVO):

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (z. B. Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Personalnummer, PC-Benutzerkennung).

Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO):

Personenbezogene Daten müssen

- auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden

- dem Zweck angemessen und in der Sache erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)
- sachlich richtig und erforderlichenfalls auf einem aktuellen Stand sein
- in einer Form gespeichert werden, welche die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet (erhoben) werden, erforderlich ist
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit durch geeignete technische und organisatorische Maßnahmen gewährleistet („Integrität u. Vertraulichkeit“), einschließlich dem Schutz vor
  - unbefugter oder unrechtmäßiger Verarbeitung
  - unbeabsichtigtem Verlust
  - unbeabsichtigter Zerstörung oder
  - unbeabsichtigter Schädigung

Rechte der betroffenen Person

Jede betroffene Person hat in Bezug auf ihre personenbezogenen Daten im Umfang der Bestimmungen der DS-GVO und des DSG NRW bestimmte Rechte:

- Recht auf Auskunft über die Verarbeitung personenbezogener Daten
- Recht auf Berichtigung unrichtiger Daten
- Recht auf Löschung personenbezogener Daten
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch gegen die Verarbeitung personenbezogener Daten
- Recht auf Widerruf einer Einwilligungserklärung
- Recht auf Schadenersatz, wenn wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist
- Recht, sich an die Datenschutzaufsichtsbehörde zu wenden

Datensicherheit durch technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken sind geeignete technische und organisatorische Maßnahmen zu treffen. Diese umfassen u. a.

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Dazu gehören z. B.:

Zutritt zu den Rechneranlagen, Servern und PC, auf denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren. Art und Umfang der notwendigen Sicherungsmaßnahmen zur Zutrittskontrolle richten sich nach der Sensibilität und der Menge der gespeicherten Daten.

Zugriff auf Daten und Informationen in einem Netzwerk oder auf EDV-Anlagen darf nur berechtigten Personen ermöglicht werden. Durch Benutzerkennung und Passwort werden die Systeme durch den Arbeitgeber entsprechend geschützt. In der Verantwortung eines jeden Einzelnen liegt der vertrauliche und sorgfältige Umgang mit den Zugangsberechtigungsdaten (Passwort).

Es ist sicherzustellen, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.