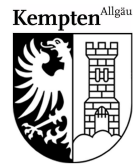


Anlage 1

zur Geschäftsordnung des Stadtrates der Stadt Kempten (Allgäu)



Datenschutzbelehrung Ratsinformationssystem (RIS) **(Stand 07.05.2020)**

1. Regelungsgegenstand

Die Stadt Kempten (Allgäu) stellt ihren Stadtratsmitgliedern über eine Webapplikation oder App (Ratsinformationssystem – „RIS“) einen gesicherten Zugriff auf Tagesordnungen der Sitzungen der städtischen Gremien, Sitzungsunterlagen, Sitzungsniederschriften (für den öffentlichen Teil der Sitzungen) sowie weitere Informationen wie z. B. Pläne etc. zur Verfügung.

Mit der vorliegenden Datenschutzbelehrung werden einheitliche Regelungen und Voraussetzungen für die Benutzung des Ratsinformationssystems geschaffen. Diese Regelungen sollen die Einhaltung datenschutzrechtlicher Vorschriften gewährleisten und verhindern, dass die gespeicherten Informationen in unbefugte Hände gelangen.

2. Geltungsbereich

Die Datenschutzbelehrung gilt für alle Benutzer des Ratsinformationssystems der Stadt Kempten (Allgäu) und somit insbesondere für alle Mitglieder des Stadtrates, die diesen Service wahrnehmen möchten und sich mit den nachfolgenden Benutzungsbedingungen einverstanden erklären.

3. Verschwiegenheitspflicht

Die Stadtratsmitglieder haben als ehrenamtlich tätige Gemeindeglieder über die ihnen bei ihrer ehrenamtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren (Art. 20 Bayer. Gemeindeordnung – GO). Dies gilt selbstverständlich auch für alle im Ratsinformationssystem enthaltenen Informationen.

Da die dort hinterlegten Dokumente eine Vielzahl von verschiedenen personenbezogenen Daten enthalten, sind insbesondere auch die allgemeinen Datenschutzvorschriften einzuhalten.

4. Zugangsdaten (Benutzername und Passwort)

Jeder Benutzer erhält für den Zugang zum Ratsinformationssystem eine persönliche Benutzerkennung. Hierzu legt sich jeder Benutzer ein eigenes Passwort fest, das nur ihm persönlich bekannt ist. Benutzername und Passwort müssen geheim gehalten werden und dürfen nicht an Dritte weitergegeben werden. Auch ein Speichern der Zugangsdaten auf dem PC oder im Browser (Programm zum Betrachten von Internetseiten) ist nicht zulässig.

Das Ausprobieren, Ausforschen und die Benutzung fremder Benutzerkennungen und Passwörter sind nicht zulässig. Sollte ein Missbrauch von Benutzerkennungen festgestellt werden, werden diese Benutzerkonten gesperrt.

5. Passwortschutz

Für den korrekten Gebrauch von Kennwörtern gelten folgende Grundsätze:

- Das Passwort darf nicht leicht zu erraten sein (z. B. keine Namen, keine Geburtsdaten, keine Kfz-Kennzeichen).
- Das Passwort muss mindestens acht Zeichen lang sein. Innerhalb des Passwortes muss mindestens ein Buchstabe, ein Sonderzeichen und eine Zahl verwendet werden.
- Initialpasswörter und voreingestellte Passwörter (z. B. bei der erstmaligen Anmeldung) müssen umgehend durch individuelle Passwörter ersetzt werden.
- Das Passwort muss geheim gehalten werden und darf nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte nicht schriftlich fixiert werden. Falls ein Passwort vergessen wird, kann ein neues Passwort über das RIS angefordert werden (*Alternativ: besteht die Möglichkeit, dies der Verwaltung mitzuteilen. Diese wird das Passwort wieder zurücksetzen*).
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Ein Passwort ist unverzüglich zu wechseln, wenn es unautorisierten Personen bekannt geworden ist.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.
- Die Weitergabe des eigenen Passworts an andere, auch an andere Ratsmitglieder, ist nicht zulässig und untersagt.

6. Zugriff

Sitzungsvorlagen der Verwaltung sind interne Ausarbeitungen für die Ratsmitglieder. Eine Bereitstellung der Sitzungsvorlagen und weiterer Sitzungsunterlagen zum Abruf durch Ratsmitglieder setzt voraus, dass Dritte weder lesend noch schreibend auf die Unterlagen zugreifen können. Es ist daher darauf zu achten, dass unbefugte Dritte keinen Zugriff auf die Daten des Ratsinformationssystems erlangen. Zu beachten ist in diesem Zusammenhang, dass sich nach dem Aufrufen von Internetseiten auf dem Privatgerät (beispielsweise im Cache) noch Teile dieser Daten bzw. einzelne Dateien befinden können. Es ist deshalb empfehlenswert, vor dem Schließen des Browsers die temporären Internetdateien zu löschen.

Der Zugang zum verwendeten Privatgerät ist mit einem Kennwort zu schützen (über Betriebssystem, BIOS o. ä.).

Sofern mehrere Personen das Privatgerät benutzen, darf der Zugriff auf das Ratsinformationssystem nur unter einer eigenen, individuellen Benutzerkennung erfolgen, die mit einem Passwort, Fingerabdrucksensor oder einer Gesichtserkennung abgesichert ist. Der Zugriff anderer Benutzer muss dadurch ausgeschlossen sein.

7. Verarbeitung

Soweit Dokumente auf privaten Geräten gespeichert werden, sind sie gegen den unbefugten Zugriff Dritter zu schützen. In diesem Fall muss der Zugang zum Privatgerät mit einem individuellen und geheimen Passwort geschützt sein. Bei mehreren Nutzern sind verschiedene individuelle Benutzerkennungen mit Passwort je Nutzer und getrennten Dateizugriffsrechten einzurichten (vgl. dazu auch Ziffern 5. und 6.; Virenschutz entsprechend Ziffer 8.).

Die aus dem Ratsinformationssystem heruntergeladenen Dateien sind zu löschen, sobald sie für die Mandatsausübung nicht mehr benötigt werden.

Das Ausdrucken von Dokumenten aus dem Ratsinformationssystem ist erlaubt. Die erstellten Ausdrucke sind gegen den unbefugten Zugriff Dritter zu schützen und, sobald sie für die Mandatsausübung nicht mehr benötigt werden, zu vernichten.

8. Virenschutz

Auf den privaten Geräten, über die der Zugriff auf das Ratsinformationssystem erfolgen soll, ist ein Virens Scanner von einem Anbieter zu installieren, der einen regelmäßigen (möglichst täglichen) Update-Service gewährleistet.

Weiterhin ist die Verwendung einer Firewall oder einer Security Suite (Programm, das mehrere Schutzprogramme vereinigt, und mindestens ein Antivirenprogramm und eine Firewall enthält, ergänzt durch Funktionen wie Anti-Spam, Anti-Phishing, Anti-Spyware oder eine Kindersicherung) oder vergleichbarer Programme erforderlich.

9. Verbindlichkeit

Durch die Unterzeichnung der Empfangsbestätigung und des Kenntnisnahmevermerkes wird diese Datenschutzbelehrung als verbindlich anerkannt.

10. Folgen der Nichtbeachtung

Für die Gewährleistung der Erfordernisse des Datenschutzes ist das Beachten und Einhalten der o. g. Regelungen unbedingt erforderlich. Für Schäden, die aus der Nichtbeachtung entstehen, können die Benutzer ggf. in Haftung genommen werden bzw. es können sich strafrechtliche Konsequenzen (z. B. § 203 Abs. 2 des Strafgesetzbuchs – StGB; Art. 23 Abs. 2 des Bayer. Datenschutzgesetzes – BayDSG) bzw. solche des Ordnungswidrigkeitenrechts (z. B. Art. 23 Abs. 1 Nr. 1 BayDSG) ergeben. Auf die Möglichkeit der Verhängung von Ordnungsgeldern bei Verletzung der Verschwiegenheitspflichten wird hingewiesen (Art. 20 Abs. 4 GO).

Datenschutzbelehrung Ratsinformationssystem (RIS)

Name, Vorname

Empfangsbestätigung und Kenntnisnahmevermerk

Hiermit bestätige ich, dass ich die Datenschutzbelehrung gelesen und in schriftlicher Form erhalten habe. Die Inhalte der Datenschutzbelehrung (Stand: 07.05.2020) erkenne ich für mich als verbindlich an.

Auf die rechtlichen Folgen einer Nichtbeachtung wurde ich hingewiesen.

Ort und Datum

Unterschrift Stadtratsmitglied