Datenschutzbelehrung elektronische Kommunikation
(Stand: 25.07.2019)

1. Regelungsgegenstand

Die Verbandsgemeinde Edenkoben und die ihr zugehörigen Ortsgemeinden stellen ihren Ratsmitgliedern, Ausschussmitgliedern und Beigeordneten (nachfolgend: Ratsmitglieder) Zugriff

- auf elektronischem Wege (per E-Mail) für die Tagesordnung
- über eine Webapplikation (Ratsinformationssystem – „RIS“) auf die Unterlagen, Niederschriften und weitere Informationen wie z.B. Pläne

der Sitzungen der kommunalen Gremien (für den öffentlichen und den nichtöffentlichen Teil) zur Verfügung. Mit der vorliegenden Datenschutzbelehrung werden einheitliche Regelungen und Voraussetzungen für die Benutzung der elektronischen Kommunikation/ des Ratsinformationssystems geschaffen. Diese Regelungen sollen die Datensicherheit gewährleisten und verhindern, dass die gespeicherten Informationen in unbefugte Hände gelangen.

2. Geltungsbereich

Die Datenschutzbelehrung gilt bei Zugangseröffnung für die elektronische Kommunikation (E-Mail und RIS – Nutzung) und damit insbesondere für Ratsmitglieder, die diesen Service wahrnehmen möchten und sich mit den nachfolgenden Benutzungsbedingungen einverstanden erklären.

3. Verschwiegenheitspflicht

Die Ratsmitglieder haben als ehrenamtlich tätige Gemeindebürger über die ihnen bei ihrer ehrenamtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren (§ 20 Gemeindeordnung). Dies gilt auch für alle im RIS enthaltenen Informationen oder solche, die digital an ein Postfach übermittelt wurden.
Da die Dokumente eine Vielzahl von verschiedenen personenbezogenen Daten enthalten, sind insbesondere auch die allgemeinen Datenschutzvorschriften einzuhalten.
Auf die Verpflichtung bei Amtsantritt wird hingewiesen.

4. Zugangsdaten RIS (Benutzername und Passwort)

Jeder Benutzer erhält für den Zugang zum RIS 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. Einsatz privater Endgeräte

Das Sicherheitsniveau der eingesetzten Privatgeräte muss grundsätzlich dem entsprechender dienstlicher Geräte vergleichbar sein. Neben einem ausreichenden Schutz vor Schadsoftware bedarf es hierzu technischer Zugriffsregelungen, die eine unbefugte Kenntnisnahme wirksam verhindern (z.B. getrennte Nutzerkennungen, Differenzierung von Zugriffsrechten auf Dokumente und Verzeichnisse oder die Verschlüsselung der auf Privatgeräten gespeicherten Daten).

Personalangelegenheiten unterliegen einem besonderen Schutzniveau und sollen nur über das RIS eingesehen werden. Sofern erforderlich, sollen die Daten nur für die Sitzung lokal gespeichert und anschließend umgehend gelöscht werden.

Mobile Endgeräte müssen Mittels PIN oder Sperrmuster gesichert sein. Eine Trennung der privaten Anwendungen und Ratsunterlagen (z.B. über „Containerlösungen“ in Form von Kapselungen) sowie eine verschlüsselte Speicherung der Sitzungsunterlagen ist zu empfehlen. Die Betriebssysteme der Geräte müssen auf einem aktuellen Stand sein. Die Eigentümerinnen und Eigentümer des Geräts verpflichten sich, die erforderlichen Sicherheitsmaßnahmen auf ihrem Gerät umzusetzen.

6. 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).
- Innerhalb des Passwortes muss mindestens ein Sonderzeichen *(.,:;+-*#§$%&=@!"/()?)*,eine Zahl, ein Groß- sowie Kleinbuchstabe verwendet werden.
- Das Passwort muss mindestens sechs Zeichen lang sein.
- Initialpasswörter und voreingestellte Passwörter (z. B. bei der erstmaligen Anmeldung) müssen umgehend durch individuelle Passwörter ersetzt werden. Beim erstmaligen Anmelden ist ein individuelles Passwort binnen 7 Tagen zu vergeben.
- 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, besteht die Möglichkeit, dies der Verwaltung mitzuteilen. Diese wird ein neues Initialpasswort vergeben.
- 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 Kollegen, ist nicht zulässig und untersagt.

7. Zugriff

Der Zugriff auf das RIS von Privatgeräten aus muss über eine gesicherte Leitung erfolgen. Es ist darauf zu achten, dass keine unbefugten Dritte Zugriff auf die Daten des RIS 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 RIS nur unter einer eigenen Benutzerkennung erfolgen, die zumindest mit einem Passwort abgesichert ist. Der Zugriff anderer Benutzer muss dadurch ausgeschlossen sein.

8. Verarbeitung

Soweit Dokumente auf privaten Geräten gespeichert werden, sind sie gegen den unbefugten Zugriff Dritter zu schützen (z.B. Schutz des Zugangs zum Privatgerät mit einem individuellen und geheimen Passwort, bei mehreren Nutzern Verwendung verschiedener Benutzerkennungen mit getrennten Dateizugriffsrechten, vgl. dazu auch Ziffern 5. und 6.; Virenschutz entsprechend Ziffer 10.). Das Ausdrucken von Dokumenten aus dem RIS ist erlaubt. Die erstellten Ausdrucke sind gegen den unbefugten Zugriff Dritter zu schützen.

9. Grundsatz der Datensparsamkeit

Sitzungsunterlagen und Niederschriften stehen im RIS zum Abruf bereit. Aus diesem Grund ist das lokale Speichern grundsätzlich nicht erforderlich. Entsprechend dem Grundsatz der Datensparsamkeit sind Vorlagen zu löschen bzw. datenschutzgerecht zu vernichten, wenn sie nicht mehr benötigt werden – i.d.R nach Beendigung der Sitzung. Eine weitere lokale Speicherung bzw. Aufbewahrung ist nur zulässig, wenn dies zu einer weiterhin andauernden Aufgabenerfüllung notwendig ist.

10. Virenschutz

Auf den privaten Geräten, über die der Zugriff auf das RIS erfolgen soll, ist ein Virenscanner zu installieren.
Weiterhin wird die Verwendung einer Firewall oder einer Security Suite (Programm, das mehrere Schutzprogramme vereinigt, und mindestens ein Antivirenprogramm und eine Firewall enthält, ggf. ergänzt durch Funktionen wie Anti-Spam, Anti-Phishing, Anti-Spyware oder eine Kindersicherung) oder vergleichbarer Programme dringend angeraten.

11. Verbindlichkeit

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

12. 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 ergeben (z. B. § 203 Abs. 2 StGB). Auf die Möglichkeit der Verhängung von Ordnungsgeldern bei Verletzung der Verschwiegenheitspflichten wird hingewiesen (§ 20 Abs. 2 i.V.m. 19 Abs. 3 GemO).

Datenschutzbelehrung Ratsinformationssystem

Name, Vorname

Einwilligung, Empfangsbestätigung und Kenntnisnahmevermerk

Hiermit bestätige ich, dass ich die Datenschutzbelehrung gelesen und in schriftlicher Form erhalten habe. Hiermit sind die Inhalte der Datenschutzbelehrung (Stand: 25.07.2019) für mich verbindlich.

Ich bin zudem mit der Verarbeitung meiner Daten zwecks elektronischer Kommunikation, insbesondere den Versand von Einladung, Tagesordnung und weiteren Unterlagen in Zusammenhang mit Gremiensitzungen zur Erfüllung meines kommunalpolitischen Mandats einverstanden.

Die Einwilligung kann jederzeit für die Zukunft widerrufen werden mit der Folge, dass die Übermittlung von Einladung und Tagesordnung ab diesen Zeitpunkt wieder schriftlich erfolgt.

Die Information nach Art. 13, 14 und 21 der Datenschutz-Grundverordnung (DSGVO) wurden bzw. werden mir über die Homepage der Verbandsgemeinde (www.vg-edenkoben.de/datenschutz/) zur Kenntnis gegeben.

Auf die rechtlichen Folgen einer Nichtbeachtung wurde ich hingewiesen.

Ort und Datum Unterschrift Mandatsträger