Datenschutzbelehrung elektronische Kommunikation „RIS“

(Stand: November 2019)

1. Regelungsgegenstand

Die Verbandsgemeindeverwaltung Simmern-Rheinböllen und die Städte Simmern und Rheinböllen stellen ihren Ratsmitgliedern, Beigeordneten und Ausschussmitgliedern über das Ratsinformationssystem (RIS) https://simmern.more-rubin1.de oder über die Applikation für Tablets „Dipolis“ Zugriff auf Tagesordnungen der Sitzungen der Gremien, Sitzungsunterlagen, Sitzungsniederschriften 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 Verbandsgemeindeverwaltung Simmern-Rheinböllen und der Städte Simmern und Rheinböllen. Somit insbesondere für alle Mitglieder des Verbandsgemeinderates und der Stadträte und deren Ausschüsse, die diesen Service wahrnehmen und sich mit den nachfolgenden Benutzungsbedingungen einverstanden erklären.

3. Verschwiegenheitspflicht

Die Ratsmitglieder/Ausschussmitglieder 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 Ratsinformationssystem 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.

4. Zugangsdaten Ratsinformationssystem (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. 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).

Bei Personalangelegenheiten handelt es sich um solche personenbezogenen Daten, die nach dem Datenschutzgesetz einem besonderen Schutz unterliegen. Für diese scheidet eine Verarbeitung und Speicherung auf privaten Geräten aus.

Mobile Endgeräte müssen mittels PIN oder Sperrmuster gesichert sein, es muss eine Trennung der privaten Anwendungen und Ratsunterlagen (z.B. über „Containerlösungen“ in Form von Kapselungen) erfolgen und für die Ratsunterlagen eine verschlüsselte Speicherung vorhanden sein. 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).
- Das Passwort muss mindestens ein Sonderzeichen oder eine Zahl enthalten.
- Das Passwort muss mindestens acht Zeichen lang sein.
- 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, 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 Kollegen/innen, ist nicht zulässig und untersagt.

7. Zugriff

Der Zugriff auf das Ratsinformationssystem von Privatgeräten aus muss über eine gesicherte Leitung erfolgen. Es ist darauf zu achten, dass keine unbefugten Dritten 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 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 8.). Das Ausdrucken von Dokumenten aus dem Ratsinformationssystem ist erlaubt. Die erstellten Ausdrucke sind gegen den unbefugten Zugriff Dritter zu schützen.

9. Grundsatz der Datensparsamkeit

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 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 Ratsinformationssystem erfolgen soll, ist ein Virenscanner zu installieren.
Weiterhin wird – soweit möglich – 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 *„Erklärung über den elektronischen Zugang von Einladungen zu Sitzungen und Ausschüssen des Verbandsgemeinderates und seiner Ausschüsse“* 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).

Information nach Art. 13, 14 und 21 der Datenschutz-Grundverordnung (DSGVO)

Mit diesen Datenschutzhinweisen informieren wir Sie gemäß der ab dem 25. Mai 2018 geltenden Datenschutz-Grundverordnung (DSGVO) über die Verarbeitung Ihrer personenbezogenen Daten durch uns sowie über die Ihnen zustehenden Rechte.

Diese Hinweise werden, soweit erforderlich, aktualisiert und auf den Homepages der *Verbandsgemeinde Simmern-Rheinböllen und den Städten Simmern und Rheinböllen* veröffentlicht. Dort finden Sie auch die Datenschutzhinweise für Besucher unserer Homepages.

1. Verantwortlicher (Art. 13 Abs. 1 lit. a DS-GVO)

Verbandsgemeindeverwaltung Simmern-Rheinböllen
Brühlstr. 2
55469 Simmern/Hunsrück
Telefon: +49 (0) 6761-8370
E-Mail: info@sim-rhb.de
www.sim-rhb.de

2. Beauftragte oder Beauftragter für den Datenschutz (Art. 13 Abs. 1 lit. b DS-GVO)

Verbandsgemeinde Simmern-Rheinböllen
Datenschutzbeauftragte/r
Brühlstr. 2
55469 Simmern/Hunsrück
Telefon: +49 (0) 6761-8370
E-Mail: datenschutz@sim-rhb.de

3. Zwecke und Rechtsgrundlage der Verarbeitung personenbezogener Daten (Art. 13 Abs. 1 lit. c DS-GVO)

Ihre personenbezogenen Daten werden zur Erfüllung der in der Zuständigkeit der Gemeinde liegenden Aufgabe, insb. nach §§ 33, 34 und 41 GemO, die Ratsmitglieder/Beigeordneten/-Ausschussmitglieder zu unterrichten, Einladung und Tagesordnung sowie ggf. Niederschriften zu übermitteln, erforderlich, damit die Ratsmitglieder/Beigeordneten/Ausschussmitglieder ihre Aufgaben insb. nach §§ 32, 50 GemO wahrnehmen können.
Erfolgt die Verarbeitung der Daten nicht aufgrund einer speziellen Rechtsvorschrift oder regelt diese den Datenschutz nicht abschließend, wird das Landesdatenschutzgesetz Rheinland-Pfalz (LDSG) angewendet.

Datenschutzrechtliche Grundlagen sind Art. 6 DSGVO und § 3 LDSG bzw. Art. 9 DSGVO und § 19 LDSG für besondere Kategorien personenbezogener Daten. Die Rechtsgrundlage für die Einholung von Einwilligungen ist Art. 6 Abs. 1 lit. a und Art. 7 DSGVO, die Rechtsgrundlage für die Verarbeitung zur Erfüllung unserer Leistungen und Durchführung vertraglicher Maßnahmen sowie Beantwortung von Anfragen ist Art. 6 Abs. 1 lit. b DSGVO, die Rechtsgrundlage für die Verarbeitung zur Erfüllung unserer rechtlichen Verpflichtungen ist Art. 6 Abs. 1 lit. c DSGVO, und die Rechtsgrundlage für die Verarbeitung zur Wahrung unserer berechtigten Interessen ist Art. 6 Abs. 1 lit. f DSGVO. Für den Fall, dass lebenswichtige Interessen der betroffenen Person oder

einer anderen natürlichen Person eine Verarbeitung personenbezogener Daten erforderlich machen, dient Art. 6 Abs. 1 lit. d DSGVO als Rechtsgrundlage.

Hinweis zum Widerruf von Einwilligungen:
Haben Sie der Verarbeitung Ihrer personenbezogenen Daten zugestimmt, können Sie diese Einwilligung bei Bedarf jederzeit widerrufen. Dies gilt jedoch nur für die Zukunft. Die bis zum Widerruf erfolgte Verarbeitung bleibt also rechtmäßig.

4. Empfänger oder Kategorien von Empfängern (Art. 13 Abs. 1 lit. e DS-GVO)

Eine Weitergabe Ihrer Daten erfolgt nur, soweit eine Rechtsgrundlage dies gestattet.

Darüber hinaus können folgende Stellen Ihre Daten erhalten:

- von der Verbandsgemeinde Simmern-Rheinböllen oder den Städten Simmern und Rheinböllen eingesetzte Auftragsverarbeiter (Art. 28 DSGVO) insbesondere im Bereich IT-Dienstleistungen, Logistik- und Druckdienstleistungen, die Ihre Daten weisungsgebunden für uns verarbeiten
- Dritte bei Vorliegen einer gesetzlichen, vertraglichen oder behördlichen Verpflichtung

5. Übermittlung an Drittland (Art. 13 Abs. 1 lit. f DS-GVO)

Wir übermitteln Ihre Daten in Staaten außerhalb des Europäischen Wirtschaftsraums - EWR (Drittländer) nur, soweit dies zur Ausführung des gesetzlichen Verwaltungshandelns erforderlich ist.

6. Dauer der Speicherung (Art. 13 Abs. 2 lit. a DS-GVO)

Soweit erforderlich, verarbeiten wir Ihre personenbezogenen Daten nur für die Dauer der Bearbeitung. Es gelten unterschiedliche Löschfristen.

Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus der Abgabenordnung (AO), SGB I und X usw. ergeben Fristen zur Aufbewahrung bzw. Dokumentation können bis zu 30 Jahre betragen

7. Betroffenenrechte (Art. 13 Abs. 2 lit. c bis d DS-GVO)
Jede von einer Datenverarbeitung betroffene Person hat nach der Datenschutzgrundverordnung insbesondere folgende Rechte:

- Recht auf **Auskunft** über die zu ihrer Person gespeicherten personenbezogenen Daten und deren Verarbeitung (Art. 15 DS-GVO). In dem Auskunftsantrag sollten das Anliegen präzisiert werden, um das Zusammenstellen der erforderlichen Daten zu erleichtern. Daher sollten in dem Antrag möglichst Angaben zum konkreten Verwaltungsverfahren (z.B. Steuerart und

Jahr) und zum Verfahrensabschnitt (z.B. Festsetzung, Zahlungsabwicklung, Vollstreckung) gemacht werden.

- Recht auf **Berichtigung**, soweit sie betreffende Daten unrichtig oder unvollständig sind (Art. 16 DS-GVO).

- Recht auf **Löschung** der zu ihrer Person gespeicherten Daten, soweit eine der Voraussetzungen nach Art. 17 DS-GVO zutrifft. Der Anspruch auf Löschung hängt unter anderem davon ab, ob die betreffenden Daten von der öffentlichen Stelle zur Erfüllung ihrer gesetzlichen Aufgaben noch benötigt wird.

  Ausnahmen vom Recht auf Löschung bestehen zur Ausübung der Meinungs- und Informationsfreiheit, zur Erfüllung rechtlicher Speicherpflichten, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für öffentliche Archivzwecke, wissenschaftliche, historische und statistische Zwecke sowie zur Durchsetzung von Rechtsansprüchen.

- Recht auf **Einschränkung der Verarbeitung**,
  - insbesondere soweit die Richtigkeit der Daten bestritten wird,
  - für die Dauer der Überprüfung der Richtigkeit, wenn die Daten unrechtmäßig verarbeitet werden, die betroffene Person aber statt der Löschung die Einschränkung der Verarbeitung verlangt,
  - wenn die betroffene Person die Daten zur Geltendmachung oder Ausübung von Rechtsansprüchen oder zur Verteidigung gegen solche benötigt werden und deshalb nicht gelöscht werden können,
  - oder wenn bei einem Widerspruch nach Art. 21 noch nicht feststeht, ob die berechtigten Interessen des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

  Die Einschränkung steht einer Verarbeitung nicht entgegen, soweit an der Verarbeitung ein wichtiges öffentliches Interesse besteht.

- Recht auf **Widerspruch** gegen die Verarbeitung personenbezogener Daten aus persönlichen Gründen, soweit kein zwingendes öffentliches Interesse an der Verarbeitung besteht das die Interessen, Rechte und Freiheiten der betroffenen Person überwiegt, oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 DS-GVO) dient.

Die verantwortliche Stelle kann dem jedoch nicht nachkommen, wenn an der Verarbeitung ein überwiegendes öffentliches Interesse besteht oder eine Rechtsvorschrift sie zur Verarbeitung verpflichtet (z.B. Durchführung des Besteuerungsverfahrens, Führung des Gewerberegisters).

- **Beschwerderecht (Art. 13 Abs. 1 lit. e DS-GVO)**

Jede betroffene Person hat das Recht auf Beschwerde beim **Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz**, wenn sie der Ansicht ist, dass ihre personenbezogenen Daten rechtswidrig verarbeitet werden:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz,
Hintere Bleiche 34,
55116 Mainz,
Tel.-Nr.: 06131/208-2449,
Fax: 06131/208-2497,
E-Mail: poststelledatenschutz.rlp.de