Ergänzung zur Satzung des Freundeskreis Römerkanal e.V. - Datenschutzrichtlinie

(Stand April 2018)

1. Grundsätze

Der Schutz personenbezogener Daten ist dem Freundeskreis Römerkanal e.V. (Freundeskreis) ein wichtiges Anliegen. Deshalb verarbeitet der Freundeskreis die personenbezogenen Daten der Vereinsmitglieder sowie Spender in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten durch den Freundeskreis erhoben werden, wie diese Daten genutzt werden, an wen sie unter Umständen übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit der Verarbeitung der Daten haben. Außerdem wird beschrieben, mit welchen Maßnahmen die Sicherheit der Daten gewährleistet werden und wie betroffene Personen Kontakt mit dem Freundeskreis aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit beim Freundeskreis bestehenden Verantwortlichkeiten. Alle Vorstandsmitglieder sind zur Einhaltung der Richtlinie verpflichtet.

Sie richtet sich an

- die Personen oder Mitglieder, die über den Einsatz/die Bereitstellung von Verarbeitungsprozessen mit personenbezogenen Daten und eines entsprechenden Anwendungssystems entscheiden (Vorstand);
- die Personen oder Mitglieder, die über die Nutzung von personenbezogenen Daten für die Erfüllung ihrer Aufgaben entscheiden (Vorstand);
- ehrenamtliche Benutzer, d.h. diejenigen, die das zur Verfügung gestellte Verarbeitungssystem personenbezogener Daten für die Erledigung ihrer Aufgaben nutzen.

Dabei gelten folgende Grundsätze:

- Die DV-Hard- und Software sind für satzungsgemäße Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen

  Verlust und Manipulation zu sichern.
- Jeder Benutzer ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass die Benutzer über diese Richtlinie informiert werden.

2. Beschaffung/Hard- und Software

2.1 Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

2.2 Der Freundeskreis wird bezüglich der Nutzer von personenbezogenen Daten ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme führen.

2.3 Bei Verdacht des Diebstahls von Hard-und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. ist der Vorstand unverzüglich zu informieren.

3. Verpflichtung der Nutzer

3.1 Jeder Nutzer, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

3.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und Information über die einschlägigen gesetzlichen Bestimmungen.

4. Transparenz der Datenverarbeitung

4.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, wird der Vorstand ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO führen.

4.2 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den Vorstand des Freundeskreis.

4.3 Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

5. Erhebung/Verarbeitung von personenbezogenen Daten

5.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen und insbesondere im Rahmen der Satzung des Freundeskreis erfolgen. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

5.2 Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.

Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

5.3 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes

Interesse der Stelle besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Vorstand zu kontaktieren.

6. Datenhaltung/Versand/Löschung

6.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu von Seiten des Vorstandes genutzten Netz-/Serverlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch den Vorstand und der Registrierung durch die den Vorstand einsetzende Benutzer. Bei Netzwerken ist der Vorstand für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

6.2 Soweit technisch bedingt ein anderer Speicherort zwingend erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

6.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Der Vorstand ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

6.4 Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht oder entsprechend zertifizierte Dienstleister mit der Löschung beauftragt wurden.

7. Externe Dienstleister/Auftragsverarbeitung/Wartung

7.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnispersonenbezogener Daten bekommen, so ist der Vorstand vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO

genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

7.2 Entsprechendes gilt, falls der Freundeskreis entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

8. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

Anlage 1

Informationen zum Umgang mit personenbezogenen Daten beim Freundeskreis Römerkanal e.V.

Der Datenschutz soll vor Missbrauch und unbefugtem Zugriff bewahren. Die wesentliche Idee ist es, den sogenannten „gläsernen Menschen“ zu verhindern. Jeder Mensch soll grundsätzlich selbst entscheiden können, wem wann welche seiner persönlichen Daten zugänglich sein sollen.

Die entsprechenden Datenschutzbestimmungen finden sich in der europäischen Datenschutz-Grundverordnung (DS-GVO). Diese wird ab dem 25.05.2018 für alle EU-Mitgliedstaaten verbindlich.

Durch die DS-GVO werden personenbezogene Daten geschützt.

Grundsätzlich sind alle Daten, die sich einer bestimmten oder bestimmbaren natürlichen Person zuordnen lassen zu schützen. Natürliche Person ist ein jeder Mensch in seiner Funktion als Träger von bestimmten Rechten und Pflichten.

Die DSGVO erweitert diese allgemeine Definition noch ein wenig: Personenbezogene Daten sind hiernach Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke ermöglichen in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität (Artikel 4 Ziffer 1 DSGVO).

Welche personenbezogene Daten gibt es im Einzelnen?

Die Arten personenbezogener bzw. auf Personen beziehbarer Daten sind zahlreich. Eine abschließende Zusammenfassung lässt sich kaum bewältigen. Im Folgenden wird eine Liste mit den Daten aufgeführt, die für die Arbeit des Freundeskreis relevant ist:

- allgemeine Personendaten (Name, Anschrift, E-Mail-Adresse, Telefonnummer usw.)
- Bankdaten (Bank und Kontonummern)

Ansonsten dürfen diese besonderen personenbezogenen Daten nur mit Einwilligung der betroffenen Person verarbeitet werden.

Zudem müssen diese Daten besonders geschützt werden, da nach dem Gesetz die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bedeutet.

Deshalb bedarf es beim Umgang mit diesen personenbezogenen Daten einer erhöhten Sorgsamkeit. Es gilt insbesondere:

- Sie sind dem Datengeheimnis verpflichtet und dürfen weder außenstehenden Dritten noch Benutzern, die nicht direkt mit dem jeweiligen Vorgang befasst sind, personenbezogene Informationen geben oder diesen entsprechende Daten zugänglich machen oder weiterleiten.
- Personenbezogene Mitgliederdaten und Vereinsdaten müssen getrennt gespeichert und bearbeitet werden. Sie haben Sorge dafür zu tragen, dass es nicht zu einer Vermengung der unterschiedlichen Datenbestände kommt.
- Personenbezogene Daten sind gegen unautorisierte Zugriffe zu schützen. Speichern Sie personenbezogene Daten daher nur in kennwortgeschützten Bereichen und sorgen Sie dafür, dass Ihre Benutzerdaten keinem Dritten und auch keinem anderen Nutzer bekannt werden.
- Das Speichern und/oder Kopieren vertraulicher und/oder personenbezogener Daten ist nur auf den dafür vorgesehenen und entsprechend gesicherten Massenspeichern gestattet.
- Das Speichern und/oder Kopieren vertraulicher und/oder personenbezogener Daten auf Wechseldatenträgern ist ausdrücklich verboten.
- Beachten Sie, dass Sie personenbezogene Daten nur für aktuelle Vereinsvorgänge erheben, speichern, verarbeiten und nutzen dürfen, soweit es für Ihre Tätigkeit erforderlich ist.
- Beachten Sie, dass Sie ohne die Zustimmung der betroffenen Personen keine personenbezogenen Daten sammeln und speichern dürfen.
- Dokumentieren Sie den Umgang mit personenbezogenen Daten so, dass nachvollziehbar ist, wann und warum Sie mit bestimmten personenbezogenen Daten gearbeitet und wo Sie diese gespeichert haben.
- Beachten Sie, dass betroffene Personen einen Anspruch darauf haben, Auskunft der über sie gespeicherten Daten zu erhalten, und seien Sie darauf vorbereitet, derartige Auskünfte zu erteilen.
- Die Weitergabe personenbezogener Daten an Dritte ist regelmäßig – und ohne Zustimmung des Betroffenen – nicht zulässig. Ist es in Ausnahmefällen gestattet, muss die Übermittlung verschlüsselt sein und die Daten müssen abgetrennt voneinander übermittelt werden. So soll am Ende zunächst das unrechtmäßige Abgreifen verhindert, zum anderen aber auch unterbunden werden, dass Datensammlungen zu einer Person zu viele Informationen über den Betroffenen preisgeben.
- Die Speicherung personenbezogener Daten bedarf erhöhter Sicherheitsmaßnahmen. Das meint nicht nur passwortgeschützte

Arbeitsplätze und Datenbänke, sondern vor allem auch angemessene Verschlüsselungsprogramme und höchstwirksame Maßnahmen zur Unterbindung einer Infiltrierung durch Schadsoftware (Antivirenprogramme, Firewall usw.). Unter Umständen müssen personenbezogene Daten auch anonymisiert werden, d. h. der Bezug zu einer bestimmten oder bestimmbaren Person wird aufgehoben.

- Die Verarbeitung personenbezogener Daten muss immer zweckgebunden erfolgen. Ist der Zweck erfüllt, müssen die Angaben gelöscht oder vor einem weiteren Zugriff geschützt werden. Diesem Zweck muss der Betroffene zudem eindeutig zugestimmt haben.
- Die Pflicht zur Löschung personenbezogener Daten besteht regelmäßig, sobald die Daten nicht mehr benötigt werden bzw. die Zweckgebundenheit aufgelöst ist. Auch unrechtmäßig gespeicherte Daten müssen umgehend sicher gelöscht werden.

Rechte der Betroffenen

Da die personenbezogenen Daten als Eigentum der jeweils betroffenen Person anzusehen sind, haben die Betroffene, deren Daten gesammelt, gespeichert und verarbeitet werden, zahlreiche Rechte. Die wichtigsten Rechte betreffen das Recht auf Berichtigung, das Recht auf Löschung („Recht auf Vergessenwerden“), den Auskunftsanspruch, Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Recht auf Widerspruch.

Wenn eine betroffene Person von ihrem Auskunftsrecht Gebrauch macht, informieren Sie bitte unverzüglich den Vorstand. Der Vorstand übernimmt die zentrale Bearbeitung und stellt die zu erteilenden Informationen gemäß Art. 12 Abs. 3 DSGVO zur Verfügung. Das Gesetzt sieht vor, dass diese Auskunft innerhalb eines Monats nach Eingang des Antrags erfolgen muss. Diese Frist kann in komplexen Fällen um zwei Monate verlängert werden. Über Fristverlängerungen ist die betroffene Person unter Angabe der für die Verzögerung verantwortlichen Gründe innerhalb eines Monats nach Eingang ihres Antrags zu informieren. Deshalb unsere Bitte: Handeln Sie rasch!

Ein Betroffener kann bei einer Verletzung seiner Rechte Anspruch auf Schadensersatz geltend machen und jederzeit die zuständige Aufsichtsbehörde einschalten.

Anlage 2

Allgemeines Merkblatt zur E-Mail-Nutzung

Beim Empfang von E-Mails ist auf Folgendes zu achten:

- Im Microsoft Explorer sollte die Anzeige aller Dateitypen aktiviert sein.
- Der elektronische Briefkasten muss regelmäßig (zumindest mehrmals täglich) hinsichtlich des Eingangs elektronischer Post überprüft werden.
- Offensichtlich unsinnige E-Mails von unbekannten Absendern sollten ungeöffnet gelöscht werden. Gleiches gilt für die Anhänge von Mails aus nicht zuverlässigen oder unbekannten Quellen.
- E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sind hinsichtlich des Inhalts zu überprüfen (zweifelhafter Text, fehlender Bezug zu konkreten Vorgängen etc.).
- Bei mehreren E-Mails mit gleich lautendem Betreff ist Vorsicht geboten.
- Nur vertrauenswürdige Dateianhänge (Attachments) dürfen geöffnet werden.
- Kein Doppelklick bei ausführbaren Programmen (z. B. *.COM, *.EXE) oder Script-Sprachen (z. B. *.VBS, *.BAT) sowie Bildschirmschonern (*.SCR).
- Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT).
- Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.
- Die Weiterleitung von Nachrichten im Vertretungsfall ist zu gewährleisten.
- Personenbezogene und vertrauliche Nachrichten sind physikalisch zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist.
- Elektronische Irrläufer sind nach Möglichkeit an den richtigen Adressaten weiterzuleiten. Ist dieser nicht zu ermitteln, muss die E-Mail an den Absender zurückgeschickt werden.

Beim Versenden von E-Mails ist zu beachten:

- Sensible personenbezogene oder sonstige vertrauliche Informationen dürfen nur unter Einsatz geeigneter Verschlüsselungsverfahren elektronisch übertragen werden. Das Gleiche gilt für beigefügte Anlagen.
- Auch die E-Mail-Adressen sind personenbezogene Daten. Die Weitergabe – insbesondere bei unseren Mitgliedern – bedarf der Einwilligung der Betroffenen. Aus diesem Grunde dürfen die E-Mail-Adressen niemals Dritten übermittelt werden. Somit ist z. B. bei einem

Massenversand sicherzustellen, dass die Adressen für die Empfänger nicht sichtbar sind. Verwenden Sie daher die Funktion „bcc“.

- Soweit möglich sollte von der Digitalen Signatur Gebrauch gemacht werden.
- Unnötige E-Mails dürfen nicht versandt werden.
- Der Versand von Kettenbriefen und Mails, deren Inhalt Anstoß erregen könnte, ist verboten. Ebenso das Abonnieren von Mailinglisten.
- Ausführbare Programme dürfen grundsätzlich nicht übermittelt werden.
- E-Mails sollten nicht im HTML-Format versendet werden.
- Aktive Inhalte (ActiveX, Java, JavaScript) in E-Mails sind zu vermeiden.
- Ein elektronisch zu versendendes Dokument muss den internen Vorschriften und Regelungen hinsichtlich äußerer Form und Gestaltung entsprechen. Außerdem muss es die erforderlichen Angaben zum Absender enthalten und im Betreff der E-Mail eine möglichst aussagekräftige Beschreibung des Nachrichteninhaltes angegeben sein.
- Zur Vermeidung einer fehlerhaften Zustellung müssen E-Mails eindeutig adressiert werden.
- Alle Dateien sind vor dem Versand explizit auf Virenbefall zu überprüfen.
- Grundsätzlich darf keiner Aufforderung zur Weiterleitung von Mails oder Anhängen ohne strenge Prüfung gefolgt werden.
- Gelegentlich ist zu prüfen, ob sich E-Mails im Postausgangskorb befinden, die nicht vom Benutzer selbst verfasst wurden.