# Datenschutzrichtlinie des Rings evangelischer Gemeindepfadfinder e.V. (REGP)

## Einleitung

Der Ring evangelischer Gemeindepfadfinder e.V. (im Folgenden „REGP“) ist gesetzlich verpflichtet, personenbezogene Daten unter Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften zu verarbeiten. Einschlägige Rechtsvorschriften sind dabei insbes. das EKD-Datenschutzgesetz (DSG-EKD), die ergänzenden Datenschutzvorschriften der EKD und der Ev.-Luth. Kirche in Norddeutschland (Nordkirche) sowie ggf. staatliche oder bereichsspezifische Rechtsvorschriften.

Um eine rechtskonforme Verarbeitung von personenbezogenen Daten zu gewährleisten, sind grundsätzliche Verhaltensanweisungen und Vorgaben erforderlich. In dieser Richtlinie sind solche von dem Vereinsvorstand verabschiedeten grundsätzlichen Verhaltensanweisungen und Vorgaben zum Datenschutz und zur Informationssicherheit wiedergegeben. Datenschutz und Informationssicherheit sind angesichts der Vielzahl an Pfadfindern und angesichts der Vielzahl an verarbeiteten personenbezogenen Daten unerlässlich für den REGP. Die Einhaltung der nachfolgenden Regelungen ist daher besonders wichtig.

## 1. Geltungsbereich

Diese Richtlinie gilt für den Ring evangelischer Gemeindepfadfinder e.V. (REGP). Sie gilt für alle Standorte und ist von allen Personen, die personenbezogene Daten für den REGP verarbeiten, einzuhalten.

## 2. Ziele

Ziel dieser Datenschutzrichtlinie ist es, Datenschutz und Informationssicherheit im REGP zu stärken und zur Einhaltung der datenschutzrechtlichen Vorschriften beizutragen.

## 3. Verantwortlichkeiten

a) Die Gesamtverantwortung für Datenschutz und Informationssicherheit liegt beim Vereinsvorstand. Jede Person, die Daten für den REGP verarbeitet, trägt durch ihr Verhalten zur Gewährleistung von Datenschutz und Informationssicherheit bei. Alle Beschäftigten sowie alle sonstigen Personen, die personenbezogene Daten für den REGP verarbeiten, sind verpflichtet, diese Datenschutzrichtlinie und sonstige Richtlinien und Anweisungen zu Datenschutz und Informationssicherheit einzuhalten.

b) Um Datenschutz und Informationssicherheit im REGP zu gewährleisten, sind die datenverarbeitenden Personen verpflichtet, Störungen, Sicherheitsvorfälle und Notfälle im Bereich des Datenschutzes und der Informationssicherheit unverzüglich zu melden. Hierbei ist insbesondere das Dokument „Prozessbeschreibung im Falle einer möglichen Datenschutzverletzung“ zu beachten, das dieser Datenschutzrichtlinie als **Anlage** beigefügt ist.

c) Jeder Prozess, der im Verein mit einer Verarbeitung personenbezogener Daten einhergeht, ist vom REGP auf die Einhaltung der datenschutzrechtlichen Vorgaben zu prüfen. Sollten hierbei offene Frage- oder Problemstellungen bestehen, sind der Vorstand und/oder der Datenschutzbeauftragte zu beteiligen.

## 4. Datengeheimnis

Hauptamtlich wie ehrenamtlich Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie sind vor der Aufnahme ihrer Tätigkeit gemäß § 26 DSG-EKD auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch den Vorstand oder eine durch diesen beauftragte Person unter Verwendung des hierzu vorgesehenen kirchenamtlichen Formulars.

**5. Dienstliche Nutzung der IT-Systeme**

a) Unter IT-Systemen sind alle Geräte oder Anwendungen (Hard- und Software) zu verstehen, mitdenen Informationen elektronisch verarbeitet oder übertragen werden können. Dazu gehören insbesondere PCs, Notebooks/Laptops, Tablet-PCs, Telefone, Mobiltelefone, Server, Speichermedien, Netzwerktechnologie, Softwareprodukte oder Drucker.

b) Die Nutzung der vom REGP bereitgestellten IT-Systeme ist ausschließlich zu dienstlichen Zwecken und zur dienstlichen Aufgabenerledigung zulässig.

**6. Vorgaben zur Gestaltung des Arbeitsplatzes**

a) Der Arbeitsplatz ist von den Beschäftigten so zu gestalten, dass Besucher oder sonstige Drittekeine Einsicht in personenbezogene Daten nehmen können. Insbesondere in Bereichen mit Publikumsverkehr sind die Bildschirme der IT-Systeme so auszurichten, dass das Risiko der Kenntnisnahme durch Besucher oder Dritte nach Möglichkeit ausgeschlossen wird. Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

b) Beim Verlassen des Arbeitsplatzes muss der jeweilige Mitarbeiter sein IT-Gerät ausschalten oder(manuell) sperren, sodass vor der erneuten Nutzung des IT-Systems eine Authentifizierung erforderlich wird.

**7. Vorgaben für den Passwort-Gebrauch**

Soweit dies technisch möglich ist, sind alle dienstlichen IT-Systeme durch die Verwendung von Passwörtern zu schützen. Zudem sind, soweit dies technisch möglich ist, auf dienstlichen Geräten Bildschirmsperren zu verwenden, die automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne (von etwa 10 bis 15 Minuten) keine Aktion durch den Benutzer durchgeführt wurde. Die Bildschirmsperre darf nur durch eine erfolgreiche Benutzerauthentifizierung deaktiviert werden können. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Soweit möglich oder angeordnet, werden Zwei-Faktor-Authentifizierungs-Systeme verwendet. Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist komplex zu gestalten und muss mindestens 3 der nachfolgenden 4 Kategorien enthalten:

1. Großbuchstaben,
2. Kleinbuchstaben,
3. Sonderzeichen,
4. Ziffern.

Soweit technisch möglich ist jeder Beschäftigte verpflichtet, sein Initial-Passwort unverzüglich zu ändern. Die Passwörter sind so zu wählen, dass sie nicht durch Dritte leicht zu erraten sind. Vor und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Passwörter dürfen nicht mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden. Passwörter müssen geheim gehalten werden und dürfen nur unbeobachtet eingegeben werden. Passwörter dürfen nicht auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden. Auch dürfen Passwörter nicht notiert und die Notiz dann in der Nähe des Geräts bzw. des Bildschirms aufbewahrt werden. Bei Passwort-Managern mit Funktionen oder Plug-Ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, müssen diese Funktionen und Plug-Ins deaktiviert werden. Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.

**8. Schutz vor Schad-Inhalten**

a) Zum Schutz vor Schad-Inhalten sind auf dienstlichen Geräten des REGP Virenschutzprogrammeeinzusetzen. Zudem kommen Systeme zum Einsatz, mit denen aus den dienstlichen E-Mail-Accounts E-Mails mit unverlangter Werbung (Spam) herausgefiltert werden. Die Einstellungen der Spam- und Virenschutzprogramme dürfen durch die Beschäftigten nicht eigenmächtig verändert werden.

b) Die Nutzung privater und/oder nicht freigegebener Hard- oder Software auf dienstlichen Geräten ist nicht gestattet.

**9. Vorgaben zur Nutzung von dienstlichen E-Mail Accounts**

Beschäftigte erhalten, sofern dies für ihre Tätigkeit erforderlich ist, einen dienstlichen E-Mail Account. Der dienstliche E-Mail Account darf ausschließlich für dienstliche Zwecke genutzt werden.

**10. Vorgaben zur Verschlüsselung von E-Mail**

a) Ausgehende E-Mails werden grundsätzlich durch das E-Mail-Programm mittels TLS auf dem Transportweg verschlüsselt (einfache E-Mail). Für E-Mails, die sensible Daten oder Informationen enthalten, ist dieser Schutz jedoch nicht ausreichend. Derartige Informationen dürfen nicht per einfacher E-Mail versendet werden. Hier müssen die Beschäftigten im Rahmen der E-Mail-Kommunikation weitere Schutzmaßnahmen (bspw. Einsatz einer Ende-zu-Ende-Verschlüsselung oder Generierung passwortgeschützter und verschlüsselter Dokumenten-Anhänge) ergreifen oder sie müssen sich auf alternative Kommunikationswege (bspw. Brief oder Telefon) zurückziehen.

b) Die Beschäftigten haben daher vor dem Versand einer E-Mail zu prüfen, ob die Versendung von Inhalten per einfacher E-Mail oder als unverschlüsselter E-Mail-Anhang zulässig ist. Unzulässig ist die Versendung, wenn durch die Offenlegung sensibler Inhalte ein nicht unerhebliches Risiko für die betroffene Person entstehen kann.

c) Neben der Versendung der in § 4 Nr. 2 EKD-Datenschutzgesetz benannten Kategorien personenbezogener Daten (dies sind: alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft; alle Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit einer natürlichen Person hervorgehen; genetische Daten; biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person; Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person) ist beispielsweise die Versendung folgender Inhalte, Angaben oder Dokumente unzulässig: die Versendung von Arbeitsverträgen, Bewerbungsunterlagen oder dienstlichen Beurteilungen, von Abmahnungen oder Angaben hierzu, von Konto- oder Kreditkartendaten von natürlichen Personen, von Gehaltsabrechnungen oder von sonstigen Lohn- und Gehaltsdaten, von Angaben zu Lohnpfändungen oder zur Zahlungsunfähigkeit, von Sozialversicherungsdaten, von Daten, die dem Sozialgeheimnis oder einem Berufsgeheimnis unterliegen, von Gesundheitsdaten (bspw. von Arbeitsunfähigkeitsbescheinigungen, Angaben zu Krankheitstagen oder das Betriebliche Eingliederungsmanagement betreffende Daten) sowie von Daten zu Vorstrafen.

**11. Grundsätze der Nutzung von mobilen Datenträgern**

Mobile Datenträger sind alle leicht transportablen Geräte, auf denen Daten gespeichert werden können. Dazu gehören insbesondere Laptops, Tablet-PCs, USB-Sticks, externe Festplatten, Speicherkarten, CD-ROMs und DVDs. Mobile Datenträger bergen aufgrund einer erhöhten Verlust- bzw. Diebstahlanfälligkeit das Risiko in sich, dass unbefugte Dritte in den Besitz von Informationen

oder von personenbezogenen Daten gelangen können. Daher sind mobile Datenträger grundsätzlich nur von den Beschäftigten einzusetzen, die aufgrund ihrer Tätigkeit beim REGP auf die Nutzung von mobilen Datenträgern angewiesen sind.

Informationen sind auf den mobilen Datenträgern grundsätzlich verschlüsselt zu speichern, wenn es sich um personenbezogene Daten und/oder vertrauliche Informationen handelt. Daten auf mobilen Datenträgern sind, sofern diese für die dauerhafte Speicherung beim REGP vorgesehen sind, unverzüglich auf die hierfür vorgesehenen Laufwerke, Server oder sonstigen Speicherorte des REGP zu übertragen, sofern sie dort noch nicht vorhanden sind. Bei der Übertragung der Daten ist in besonderer Weise darauf zu achten, dass eine Prüfung der Inhalte des Datenträgers im Hinblick auf Schadsoftware erfolgt.

**12. Grundsätze für die Inanspruchnahme von Dritten / Auftragnehmern**

Beim REGP werden auch Auftragnehmer (bspw. Drittunternehmen) mit der Durchführung von Leistungen beauftragt. Wenn Auftragnehmer im Zusammenhang mit ihrer Tätigkeit für den REGP Zugriff auf Informationen oder personenbezogene Daten erhalten können, ist die Beauftragung vorher vom Vorstand zu genehmigen. Der Vorstand wird sich bei Bedarf mit dem Datenschutzbeauftragten in Verbindung setzen, um die datenschutzrechtliche Zulässigkeit und rechtliche Absicherung der Inanspruchnahme des Auftragnehmers zu prüfen und zu klären.

Alle Beschäftigten des REGP sollten beachten, dass für den Fall, dass der Auftragnehmer personenbezogene Daten im Auftrag verarbeitet und/oder eine Wartung oder Pflege von IT-Systemen durchgeführt wird, bei der eine Kenntnisnahme von personenbezogenen Daten theoretisch möglich ist, zwingend ein sog. Auftragsverarbeitungsvertrag abzuschließen ist. Vor dem Abschluss des Auftragsverarbeitungsvertrags hat eine Überprüfung des Auftragnehmers und des Auftragsverarbeitungsvertrags zu erfolgen. Diesbezüglich soll der Datenschutzbeauftragte frühzeitig beteiligt werden.

**13. Betroffenenrechte**

Jede Person kann ihre Betroffenenrechte nach den §§ 16-25 DSG-EKD gegenüber dem REG geltend machen. Dies beinhaltet insbesondere das Recht auf Auskunft, Berichtigung und Löschung von personenbezogenen Daten sowie das Recht auf Einschränkung der Verarbeitung und das Recht auf Widerspruch gegen eine Verarbeitung von Daten. Alle Personen, die Daten für den REGP verarbeiten, sind verpflichtet, einen von einer betroffenen Person geltend gemachten datenschutzrechtlichen Anspruch (etwa auf Auskunft, Berichtigung, Löschung oder einen Widerspruch) unverzüglich nach Eingang der Mitteilung an den Vorstand und den Datenschutzbeauftragten weiterzuleiten. Das weitere Vorgehen ist sodann zwischen Vorstand, meldender Person und dem Datenschutzbeauftragten abzustimmen.

**14. Informationspflichten**

Werden personenbezogene Daten bei einer Person durch den REGP erhoben, so hat der REGP der betroffenen Person auf ihr Verlangen hin in geeigneter und angemessener Weise die in § 17 DSGEKD genannten Informationen zur Verfügung zu stellen.

**15. Datenschutzbeauftragter**

a) Der REGP hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte ist Ansprechpartner für das Thema Datenschutz und berät und unterstützt den Vorstand und die Beschäftigten hinsichtlich der Verarbeitung von personenbezogenen Daten. Seine weiteren Aufgaben ergeben sich vor allem aus § 38 EKD-Datenschutzgesetz (DSG-EKD).

b) Die Kontaktdaten des Datenschutzbeauftragten finden sich auf der Homepage des REGP.

c) Im Bereich der Verarbeitung von personenbezogenen Daten ist Sorge dafür zu tragen, dass eine frühe Einbindung des Datenschutzbeauftragten bei der Planung und Einführung von neuen Prozessen, in deren Zusammenhang auch personenbezogenen Daten verarbeitet werden, erfolgt. Gleiches gilt für Änderungen an bestehenden Prozessen.

d) Die vom REGP umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sind in regelmäßigen zeitlichen Abständen (mindestens einmal pro Jahr) unter Hinzuziehung des Datenschutzbeauftragten zu evaluieren.

**16. Datenschutz-Folgenabschätzung**

Hat eine Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge, so muss im REGP vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt werden, § 34 Absatz 1 DSG-EKD. Informationen zur Durchführung der Datenschutz-Folgenabschätzung können beim Datenschutzbeauftragten angefordert werden. Der Datenschutzbeauftragte ist hinsichtlich der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen, vgl. § 34 Absatz 2 DSG-EKD.

**17. Sanktionen**

Ein Verstoß gegen diese Richtlinie kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

**Neumünster, 4 März 2024**

**Der Vorstand**