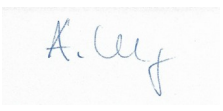
# Datenschutzkonzept

## erstellt am 30.12.2019

## für

## Evangelisch-Freikirchliche Gemeinde

## Hannover-Kronsberg



**Datum: 30.12.2019 Unterschrift Verantwortliche:**

**Gemeindeleiterin und Datenschutzbeauftragter**

# Inhaltsverzeichnis

# Maßnahmenkatalog und Handlungsempfehlungen

# zur Umsetzung der DSGVO

## erstellt am

## 30.12.2019 Anlagen

## Maßnahmenkatalog zur Umsetzung der DSGVO

Jede Organisation, die personenbezogene Daten verarbeitet, muss nach der DSGVO nachweisen können, dass Maßnahmen und Prozesse zum Schutz personenbezogener Daten getroffen und durchgeführt werden.

Anhand des Fragenkatalogs haben wir den aktuellen Stand der umzusetzenden Maßnahmen in unserer Organisation erfasst und in diesem Maßnahmenkatalog dokumentiert. So erkennen wir, in welchen Bereichen wir schon gut vorbereitet sind und in welchen Bereichen noch Handlungsbedarf besteht.

## Inhaltsverzeichnis

## 1. Leitlinie zum Datenschutz

Stand der Datenschutzpolitik und interne Richtlinie der Leitung für die Verarbeitung personenbezogener Daten in der Organisation sowie die Schaffung von organisatorischen und technischen Maßnahmen zur Umsetzung dieser Politik

| Datenschutzmanagement | **PLAN** (zu erledigen) | **DO** (wer / bis wann) | **CHECK** (erledigt und zu kontrollieren) | **ACT** (wer / wann) |
|---|---|---|---|---|
| **Datenschutzkonzept** | Ein Datenschutzkonzept wird als Bestandteil dieser Analyse erstellt. | 1 | Datenverarbeitung Gemeinderechner, churchtools<br>Personenenbezogene Daten werden auf getrennten Rechnern passwortgeschütz und autorisiert aufgehoben. | |
| **Einwilligungserklärungen** | Eine schriftliche Einwilligung der Betroffenen ist einzuholen. | 1 | | |
| **Datenschutzerklärung** | Eine Datenschutzwebseitenerklärung ist als Entwurf beigefügt. | 1 | | |
| **IT-Sicherheits- bzw. Benutzerrichtlinie** | Siehe Datenschutzkonzept | 1 | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 | | 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

## 2. Risikoabschätzung

Ermittlung des Schutzbedarfs und Definition konkreter Ziele; Ermittlung und Bewertung der einzelnen Datenverarbeitungsvorgänge iin der Organisation; Vorgaben für spezifische Datenverarbeitungen

| | **PLAN** (zu erledigen) | **DO** (wer / bis wann) | **CHECK** (erledigt und zu kontrollieren) | **ACT** (wer / wann) |
|---|---|---|---|---|
| **Risikobewertung je Verarbeitungstätigkeit** | Es ist eine Risikobewertung (Eintrittswahrscheinlichkeit, Auswirkung / Schaden) für jede im Verzeichnis der Verarbeitungstätigkeiten ausgewählten Verarbeitungstätigkeiten durchzuführen. (siehe Dokument 4. Risikoabschätzung) | 1 | | |
| **Einführung neuer Technologien bzw. Datenverarbeitungen** | Bei der Einführung neuer Technologien bzw. Datenverarbeitungen ist eine Risikobewertung (Eintrittswahrscheinlichkeit, Auswirkung / Schaden) durchzuführen. (siehe Dokument 4. Risikoabschätzung) | 1 | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 || 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

## 3. Technische und Organisatorische Maßnahmen für die Sicherheit der Verarbeitungen

Beschreibung und Dokumentation der technischen und organisatorischen Maßnahmen zum Schutz und zur Sicherheit der Verarbeitung von personenbezogenen Daten (Beispiele und Vorlagen siehe Anlage 1: Datensicherheitskonzept)

| | **PLAN** (zu erledigen) | **DO** (wer / bis wann) | **CHECK** (erledigt und zu kontrollieren) | **ACT** (wer / wann) |
|---|---|---|---|---|
| **Sicherheitsrichtlinie** | Es sind IT-Sicherheits- bzw. Benutzerrichtlinien zu erstellen. | 1 | | |
| **Einführung neuer Technologien bzw. Datenverarbeitungen** | Es sind Rollen und Verantwortlichkeiten für ITSicherheit zu definieren. | 1 | | |
| **Zutrittskontrolle** | | | Der Zutritt zum PC-Arbeitsplatz ist beschränkt. | 2 |
| | Der Daten-PC sollte sicher aufgestellt sein. | 1 | | |
| | Zugang zum PC haben nur Befugte. | 1 | | |
| | Zutritt zu Räumen, in denen Datenmaterial verwahrt wird (Akten, Datenträger) ist zu beschränken. | 1 | | |
| **Zugangskontrolle** | | | Es sind Bildschirmsperren eingerichtet. | 2 |
| | | | Eine Firewall wurde installiert, aktiviert und aktualisiert. | 2 |
| | | | Eine Software zum Schutz vor Schadsoftware wurde installiert, aktiviert und aktualisiert. | 2 |
| | | | Eine Benutzeridentifikation/Authentifizierung wurde eingerichtet. | 2 |
| | Protokollierungs- und Überwachungsmechanismen (z.B. Logins) sind einzuführen. | 1 | | |

| | | | | |
|---|---|---|---|---|
| | Es sind sichere Passwörter zu verwenden bzw. Passwortvorgaben (Mindestlänge, Komplexität) zu erstellen. | 1 | | |
| | Eine sichere Datenübertragung (z.B. Verschlüsse-lung von übertragenen Daten) ist zu gewährleisten. | 1 | | |
| | | | Es wurden Maßnahmen zur Installation von Software (z.B. Regelung von Administratorrechten) definiert. | 2 |
| **Zugangskontrolle** | Es sind Regelungen zum Umgang mit Schwachstellen (z.B. Einspielen von Security Patches) zu definieren. | 1 | | |
| | Die Daten sind vor Verlust zu schützen. Für die Speicherung/Backups sind externe Speichermedien zu nutzen. | 1 | | |
| | Die Speichermedien sind zu verschlüsseln. | 1 | | |
| **Zugriffskontrolle** | Es sind unterschiedliche Zugriffsrechte einzuteilen und zu dokumentieren. | 1 | | |
| | Verletzungen von Zugriffsrechten sind zu protokollieren. | 1 | | |
| | Es ist sicherzustellen, dass Zugriffsverletzungen zukünftig vorgebeugt werden kann. | 1 | | |
| | Datenträger/Datenblätter sind sicher zu entsorgen. | 1 | | |
| | Ein Kopierschutz/Bearbeitungsschutz ist einzurichten. | 1 | | |

| | | | | |
|---|---|---|---|---|
| **Zugriffskontrolle** | Es sind einheitliche Regelungen für Eintritt, Personenwechsel und Austritt einzurichten. | 1 | | |
| | Zuständigkeiten und Regelungen für die Rückgabe von Werten (z.B. Laptop, Smartphone, Software, Berechtigungen, Schlüssel, etc.) sind zu definieren. | 1 | | |
| | | | Nur besonders befugte Personen haben Zugriff auf personenbezogene Daten. | 2 |
| **Weitergabekontrolle** | Daten sind verschlüsselt weiterzugeben bzw. zu versenden. | 1 | | |
| | | | Es erfolgt eine regelmäßige Wartung und Prüfung der Datenverarbeitungssysteme. | 2 |
| | | | Veraltetes Equipment wird sicher entsorgt. | 2 |
| | Es sind Beschränkungen bei der Nutzung von privatem Equipment einzurichten. | 1 | | |
| **Eingabekontrolle** | Die Protokollierung von Erhebungen, Änderungen und Löschung personenbezogener Daten hat zu erfolgen. | 1 | | |
| | Die Protokollierung von Erhebungen, Änderungen und Löschung personenbezogener Daten in elektronischen Akten hat zu erfolgen. | 1 | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 || 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

| | PLAN (zu erledigen) | DO (wer / bis wann) | CHECK (erledigt und zu kontrollieren) | ACT (wer / wann) |
|---|---|---|---|---|
| **Privacy by Design / Privacy by Default** | Nur die notwendigsten Daten sind zu erheben (Datenminimierung). | 1 | | |
| **Dokumentation der Zutritts- und Zugriffsberechtigungen** | Es sind unterschiedliche Zugriffsrechte einzuteilen und zu dokumentieren. | 1 | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 || 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

## 4. Betroffenenrechte und Informationspflichten

Whitepaper für die Gewährung und Umsetzung der Rechte von Betroffenen

| | PLAN (zu erledigen) | DO (wer / bis wann) | CHECK (erledigt und zu kontrollieren) | ACT (wer / wann) |
|---|---|---|---|---|
| **Informationspflichten** | Die Betroffenen sind über die Erhebung und Speicherung ihrer personenbezogenen Daten zu informieren. | 1 | | |
| **Einwilligungserklärungen** | Es ist ein eindeutiges Einverständnis mit der Verarbeitung der personenbezogenen Daten vom Betroffenen einzuholen. | 1 | | |
| | Diese Einwilligungserklärung ist in verständlicher Form und klarer Sprache zu erstellen. | 1 | | |
| | Bei Betroffenen, die das 16. Lebensjahr noch nicht vollendet haben, ist die Einwilligung des gesetzlichen Vertreters (z.B. Eltern) einzuholen. | 1 | | |

| | | | | |
|---|---|---|---|---|
| | Das Vorliegen der Einwilligung ist nachzuweisen. | 1 | | |
| **Einwilligungserklärungen** | Bei Widerruf der Einwilligung ist sicherzustellen, dass die Daten nicht weiterverarbeitet werden. Es ist zu überprüfen, ob bestehende Einwilligungserklärungen an die DSGVO angepasst werden müssen. | 1 | | |
| **Einhaltung der datenschutzrechtlichen Anforderungen beim Auftragsverarbeiter** | Es ist sicherzustellen, dass die datenschutzrechtlichen Anforderungen auch beim Auftragsverarbeiter erfüllt werden. (Checkliste für die Erstkontrolle siehe Anlage 1: Datensicherheitskonzept) | 1 | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 || 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

## 5. Schulungen, Kontrollen, Weiterentwicklung

Regelmäßige Informationen und Schulungen der Mitarbeiter zum Datenschutz sowie Kontrollen und Anpassungen an aktuelle Gegebenheiten

| | **PLAN** (zu erledigen) | **DO** (wer / bis wann) | **CHECK** (erledigt und zu kontrollieren) | **ACT** (wer / wann) |
|---|---|---|---|---|
| **Mitarbeiter auf Datengeheimnis verpflichten** | Die Mitarbeiter, die Daten verarbeiten, werden zum Dioenstantritt zum Datengeheimnis verpflichten. | 1 | | |
| **Datenschutzanforderungen bei Neuanschaffungen / Änderungen von bestehenden Produkten, Dienstleistungen oder IT** | Es ist sicherzustellen, dass bei der Beschaffung von IT, Änderungen / Neuentwicklung von Produkten / Dienstleistungen die Datenschutzanforderungen von Anfang an berücksichtigt werden. | 1 | | |
| **Verzeichnis der Verarbeitungstätigkeiten** | Ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO wird angelegt. | 1 | | |
| | In diesem Verzeichnis sind die zutreffenden Verarbeitungstätigkeiten sowie die entsprechenden Zusatzangaben aufzuführen. | 1 | | |
| | | | | |

1 = verantwortlich: Gemeindeleiterin - Frist: bis 31.03.2020 || 2 = verantwortlich: Gemeindeleiterin - Aktualisierung: jährlich

# Verzeichnis der Verarbeitungstätigkeiten

## erstellt am

## 30.12.2019 für

## Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg

### Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO

Das Verarbeitungsverzeichnis ist auf Anfrage den Aufsichtsbehörden zur Verfügung zu stellen, anhand dessen ist es der Aufsichtsbehörde möglich, die durchgeführten Verarbeitungstätigkeiten zu kontrollieren.

### Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO)

| | |
|---|---|
| Verantwortlicher (=Legaleinheit) | Gemeindeleitung |
| Gesetzlicher Vertreter (= Geschäftsführung) | Gemeindeleiter/In |
| Verantwortlicher Mitarbeiter für Datenschutz | Siegmar Ahlvers |
| Datenschutzbeauftragten nach § 37 DSGVO | Hans-Peter Pfeifenbring (Gesamtgemeinde Hannover) |

Die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg ist nach Artikel 30 DSGVO zum Führen eines „Verzeichnisses von Verarbeitungstätigkeiten“ verpflichtet, um die Transparenz über die Verarbeitung personenbezogener Daten und die eigene rechtliche Absicherung zu gewährleisten. In der Gemeinde werden die nachfolgenden Verarbeitungstätigkeiten durchgeführt.

| | |
|---|---|
| **Bezeichnung der Verarbeitungstätigkeit** | **Lohn – und Gehaltsabrechnung** |
| **Verantwortliche Fachabteilung/Ansprechpartner** | Gesamtgemeindebüro/Schkalee |
| **Zweckbestimmung der Datenverarbeitung** | Ermittlung, Abrechnung und Auszahlung von Lohn und Gehalt, Dokumentation der Erstattung von Krankengeld seitens der Krankenkassen |
| **Kategorien betroffener Personen** | Mitarbeiter |
| | |
| **Beschreibung der Datenkategorien** | Vorname<br>Nachname<br>Titel<br>Anschrift (privat)<br>Telefonnummer (privat)<br>Familienstand<br>Angaben zu Angehörigen (z.B. Kindern)<br>Geburtsdatum<br>Angaben zu Steuerklassen<br>Lohn- und Gehaltsdaten<br>Angaben zu Lohnpfändungen<br>Sozialversicherungsdaten<br>Religionszugehörigkeit<br>Krankheitstage (ohne Befund)<br>Bankverbindung<br>Daten zu erworbenen Waren oder Dienstleistungen |
| **Kategorien besonderer personenbezogener Daten** | Religionszugehörigkeit<br>Gewerkschaftszugehörigkeit |
| **Einwilligung / Rechtsgrundlage** | Art. 6 DSGVO, § 4 Abs. 2 LStDV |
| **Empfängerkategorien** | Mitarbeiter Gemeindebüro<br>Steuerberater, Wirtschaftsprüfer<br>Sozialversicherungsstellen und Krankenkassen<br>Finanzamt<br>Versicherer für betriebliche Altersversorgung<br>Personalausschuss der Gemeindeleitung |
| **Datenübermittlung in Drittstaaten** | Nein |
| **Löschfristen** | Art. 17 Abs. 3 lit. b DSGVO Löschung erfolgt unverzüglich nach Widerruf der Einwilligung oder nach Widerspruch;<br>Art. 147 Abs. 3 AO, Steuerrelevante Daten werden zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist, gespeichert - Aufbewahrungspflicht!<br>Alle anderen Daten zwei Jahre. |

| | |
|---|---|
| **Bezeichnung der Verarbeitungstätigkeit** | **Gemeindekasse/Spendenbuchhaltung, Kontaktverwaltung** |
| **Verantwortliche Fachabteilung/Ansprechpartner** | Vera Schmidt |
| **Zweckbestimmung der Datenverarbeitung** | Durchführung der Finanzbuchhaltung, und Kontaktverwaltung |
| **Kategorien betroffener Personen** | Mitglieder und Freunde<br>Mitarbeiter |
| **Beschreibung der Datenkategorien** | Vorname<br>Nachname<br>Geschlecht<br>Geburtsdatum<br>Geburtsort<br>Geburtsname<br>Anschrift<br>E-Mail-Adresse<br>Telefonnummer<br>Bankverbindung<br>Taufdaten<br>Familienstand<br>Familienverbund<br>Hochzeitsdatum<br>Mitgliedsbeginn<br>Mitgliedsbeginn / Grund<br>Mitgliedsende<br>Mitgliedsende/ Grund<br>Umsatzdaten |
| **Kategorien besonderer personenbezogener Daten** | nein |
| **Einwilligung / Rechtsgrundlage** | Art. 6 DSGVO |
| **Empfängerkategorien** | Spender<br>Kassenprüfer, Steuerberater, Wirtschaftsprüfer<br>Finanzamt |
| **Datenübermittlung in Drittstaaten** | Nein |
| **Löschfristen** | Art. 17 Abs. 3 lit. b DSGVO Löschung erfolgt unverzüglich nach Widerruf der Einwilligung oder nach Widerspruch; Art. 147 Abs. 3 AO, Steuerrelevante Daten werden zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist, gespeichert - Aufbewahrungspflicht! Alle anderen Daten zwei Jahre. |

| | |
|---|---|
| **Bezeichnung der Verarbeitungstätigkeit** | **Beschaffung/Einkauf** |
| **Verantwortliche Fachabteilung/Ansprechpartner** | Vera Schmidt |
| **Zweckbestimmung der Datenverarbeitung** | Einkauf von Waren und Dienstleistungen |
| **Kategorien betroffener Personen** | Mitarbeiter<br>Lieferanten<br>Dienstleister |
| **Beschreibung der Datenkategorien** | Vorname<br>Nachname<br>Name des Unternehmens<br>Anschrift (geschäftlich)<br>Lieferanschrift<br>E-Mail-Adresse<br>Position<br>Bankverbindung<br>Umsatzsteueridentifikationsnummer<br>Daten zu erworbenen Waren oder Dienstleistungen<br>Vertragsdaten<br>Umsatzdaten |
| **Kategorien besonderer personenbezogener Daten** | nein |
| **Einwilligung / Rechtsgrundlage** | Art. 6 DSGVO |
| **Empfängerkategorien** | Mitarbeiter o. Arbeitsbereiche, die Waren oder Dienstleistungen in Anspruch nehmen<br>Dritte |
| **Datenübermittlung in Drittstaaten** | nein |
| **Löschfristen** | Art. 17 Abs. 3 lit. A und b DSGVO Löschung erfolgt unverzüglich nach Widerruf der Einwilligung oder nach Widerspruch;<br>§ 257 HGB, GodBArt. Art 147 Abs. 3 AO, sechs bzw. zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist - Aufbewahrungspflicht! |

| | |
|---|---|
| **Bezeichnung der Verarbeitungstätigkeit** | **Veranstaltungsorganisation, z.B. Gottesdienstplanung** |
| **Verantwortliche Fachabteilung/Ansprechpartner** | Angelika Illg |
| **Zweckbestimmung der Datenverarbeitung** | Planung, Vereinbarung und Organisation von Terminen per Telefon, E-Mail und persönliche Absprachen |
| **Kategorien betroffener Personen** | Mitarbeiter<br>Gäste |
| **Beschreibung der Datenkategorien** | Vorname<br>Nachname<br>E-Mail-Adresse<br>Telefonnummer<br>Telefonnummer (privat)<br>Termindaten |
| **Kategorien besonderer personenbezogener Daten** | nein |
| **Einwilligung / Rechtsgrundlage** | Art. 6 a und b DSGVO |
| **Empfängerkategorien** | Mitarbeiter<br>Kunden<br>Auftragsverarbeiter (Cloudanbieter) |
| **Datenübermittlung in Drittstaaten** | nein |
| **Löschfristen** | Art 17 Abs 1 a DSGVO Löschung erfolgt unverzüglich nach Widerruf der Einwilligung oder nach Widerspruch |

| | |
|---|---|
| **Bezeichnung der Verarbeitungstätigkeit** | **Vertragsmanagement** |
| **Verantwortliche Fachabteilung/Ansprechpartner** | Angelika Illg |
| **Zweckbestimmung der Datenverarbeitung** | Verwaltung von Projekten in der Gemeinde |
| **Kategorien betroffener Personen** | Mitarbeiter<br>Dienstleister<br>Dritte |
| **Beschreibung der Datenkategorien** | Vorname<br>Nachname<br>Name des Unternehmens<br>Anschrift (geschäftlich)<br>Branche<br>E-Mail-Adresse<br>Telefonnummer<br>Position<br>Termindaten<br>Vertragsdaten |
| **Kategorien besonderer personenbezogener Daten** | Nein |
| **Einwilligung / Rechtsgrundlage** | Art. 6 a und b DSGVO |
| **Empfängerkategorien** | Mitarbeiter<br>Kunden<br>Dritte<br>Auftragsverarbeiter (Cloudanbieter) |
| **Datenübermittlung in Drittstaaten** | nein |
| **Löschfristen** | Art 17 Abs. 1 a DSGVO Löschung erfolgt unverzüglich nach Widerruf der Einwilligung oder nach Widerspruch; § 257 HGB, GodBArt. Art 147 Abs. 3 AO, sechs bzw. zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist - Aufbewahrungspflicht! |

# Risikoabschätzung zur

# Umsetzung des DSGVO

## erstellt am 30.12.2019

## für die

## Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg

## Warum ist eine Risikoabschätzung für die Gemeinde notwendig?

Die EU-Grundrechte-Charta regelt in Art. 8. den Schutz personenbezogener Daten. Jede Person hat das Recht auf Schutz der Sie betreffenden personenbezogener Daten.

## Was sind personenbezogene Daten?

Nach DSGVO Art. 4 (1) umfassen „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer (beispielsweise Mitgliedsnummern oder Ausweisnummern), zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

## Verbot der Datenverarbeitung mit Erlaubnisvorbehalt

Grundsätzlich gilt das Verbot der Verarbeitung von personenbezogenen Daten, es sei denn, es liegt ein Erlaubnistatbestand vor. Diese Daten dürfen nur für festgelegte Zwecke und mit Einwilligungen der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage (Rechtsgrundlage) verarbeitet werden. Das ist beispielsweise dann der Fall, wenn jemand Gemeindemitglied werden will. Für die Mitgliedschaft oder auch nur die Anbahnung sind personenbezogene Daten des Interessenten unabdingbar. In diesem Fall stellt das Interesse an Mitgliedschaft eine gesetzlich geregelte Rechtsgrundlage dar (Art. 6 Abs. 1 lit. b DSGVO).

## Welche Schäden können im Umgang mit personenbezogenen Daten verursacht werden?

Neben materiellen Schaden gibt es zukünftig auch den immateriellen Schaden. Grundsätzlich dürfte niemand ein Interesse daran haben, dass unbefugt Dritte Zugriff auf möglicherweise sensible personenbezogene Daten haben. Bei Daten wie dem eigenen Namen mag die Gefahr eines Schadens noch überschaubar und nicht sehr gravierend sein. Anders verhält es sich jedoch mit Finanzdaten und anderen personenbezogenen Daten. Die Risiken, die bei unbefugtem Zugriff auf solche Daten bestehen, können gravierende Folgen haben.

Zum Beispiel besteht die Gefahr, dass ein Bewerber eine Anstellung nicht erhält, weil der potentielle Arbeitgeber unbefugt Kenntnis von berufsrelevanten Gesundheitsdaten erlangt hat. Der daraus resultierende Schaden, den der Betroffene dann gegenüber dem Verantwortlichen geltend machen kann, kann existenzvernichtend sein, ganz abgesehen von den möglichen Bußgeldern. Hierbei handelt es sich um ein drastisches Beispiel zur Veranschaulichung.

Das Schadensersatzrecht ist – neben dem Recht auf Löschung, Sperrung und Berichtigung – das Wiedergutmachungsrecht des Betroffenen bei Datenschutzverstößen. Denn nach DSGVO Art. 82 (1) hat zukünftig jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Vor diesem Hintergrund ist eine Risikoanalyse unabdingbar. Mit einer solchen Risikoanalyse ermitteln wir die mögliche Gefahr für die Rechte und Freiheiten der betroffenen Personen. Im Rahmen dieser Abschätzung nehmen wir die Beurteilung einer Schadenswahrscheinlichkeit (wie wahrscheinlich ist unbefugter Zugriff) vor und eine Bewertung, wie gravierend ein Datenschutzverstoß aufgrund der konkret gefährdeten Daten für die Rechte und Freiheiten des Betroffenen sind. Es ist daher für alle bei uns stattfindenden Verarbeitungstätigkeiten eine separate Risikoabschätzung durchzuführen. Außerdem ist bei einem hohen Risiko der Verarbeitungstätigkeit eine sogenannte

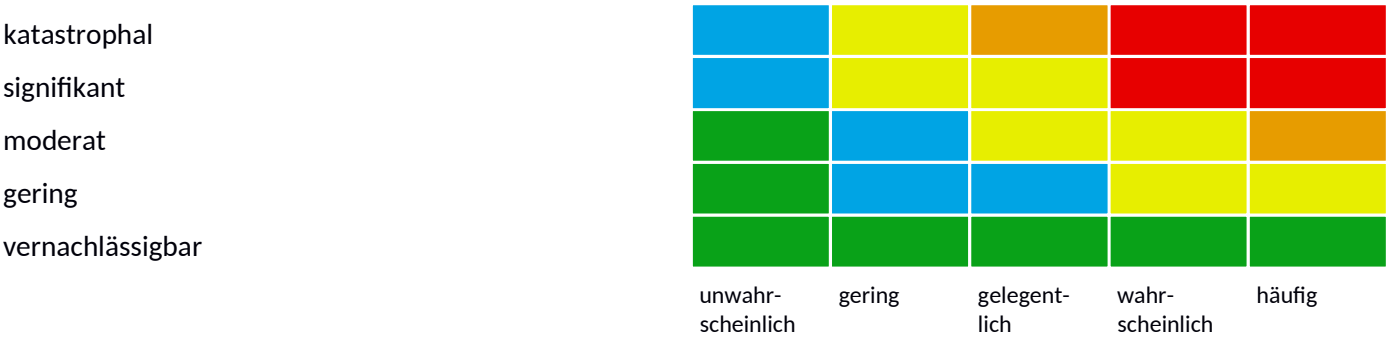
Datenschutzfolgenabschätzung gesetzlich vorgeschrieben, Art. 35 DSGVO. Diese wiederum löst die Pflicht aus, einen Datenschutzbeauftragten zu bestellen. Die Risikoabschätzung ist damit eine elementare Maßnahme, um die eigene Datenschutzkonformität bestimmen und einhalten zu können.

## Wie führen man eine Risikoabschätzung durch?

Beispiele typischer Verarbeitungstätigkeiten:

- Personalmanagement (Lohnabrechnung, Arbeitszeiterfassung, Bewerber, Bewertung)
- Mitgliedermanagement (Mitgliederstammdaten, relevante Daten, etc.)
- Mobile Applikation (Verhaltensprofile, Inhalte)
- Marketingmaßnahmen (Tracking & Remarketing, Newsletter, Postmailings)
- Sicherheit (Videoüberwachung, Chipkarten, Serverprotokollierung)
-
-

Die mit diesen Tätigkeiten verbundenen Risiken können nun über die folgende Risikomatrix bewertet werden.




Dazu geht man wie folgt vor:

Wir betrachten eine Verarbeitungstätigkeit unter zwei Gesichtspunkten. Zuerst fragen wir uns, mit welcher Wahrscheinlichkeit im Rahmen dieser Verarbeitungstätigkeit ein Datenverstoß (unbefugter Zugriff, Verlust der Daten) eintreten kann. Relevante Aspekte sind hier die tatsächliche Zugriffsmöglichkeit, also der zu betreibende Aufwand, um an die Daten zu gelangen sowie das potentielle Interesse an diesen Daten.

Für die Eintrittswahrscheinlichkeiten lassen sich folgende Richtwerte definieren:

| | | |
|---|---|---|
| häufig | | Einmal pro Woche oder öfter |
| wahrscheinlich | | Maximal einmal pro Monat |
| gelegentlich | | Maximal einmal in 6 Monaten |
| gering | | Maximal einmal in 2 Jahren |
| unwahrscheinlich | | Alle 10 Jahre oder seltener |

In einem zweiten Schritt muss beurteilt werden, welches Risiko für den Betroffenen besteht, wenn seine Daten verloren gehen oder Unbefugten in die Hände gelangen. An dieser Stelle sollte das Risiko eher zu hoch als zu gering eingestuft werden. Maßgebliche Aspekte, die heranzuziehen sind, sind die Art der Daten (Personalien, Gesundheitsdaten, Finanzdaten, etc.) und ob bzw. wie die Daten verschlüsselt sind. Ebenso zu berücksichtigen sind alle weiteren Schutzmaßnahmen im Zusammenhang mit der jeweiligen Verarbeitungstätigkeit.

Die Risiken lassen sich wie folgt definieren:

| | | |
|---|---|---|
| Katastrophal | | Schwerwiegende Beeinträchtigungen der Rechte und Freiheiten von Personen |
| Signifikant | | Beeinträchtigungen der Rechte und Freiheiten von Personen mit konkreten aber nicht schwerwiegenden Nachteilen |
| Moderat | | Personen werden in Ihren Rechten und Freiheiten beeinträchtigt, Ihnen entstehen aber daraus keinen konkreten Nachteile |
| Gering | | Beeinträchtigungen von Personen sind vorhanden, haben aber keine praktischen Konsequenzen für deren Rechte und Freiheiten |
| vernachlässigbar | | Keine praktischen Auswirkungen auf Personen |

Anhand dieser Beurteilungen kommen wir mithilfe der obigen Risikomatrix zu einer Bewertung des spezifischen Risikos.

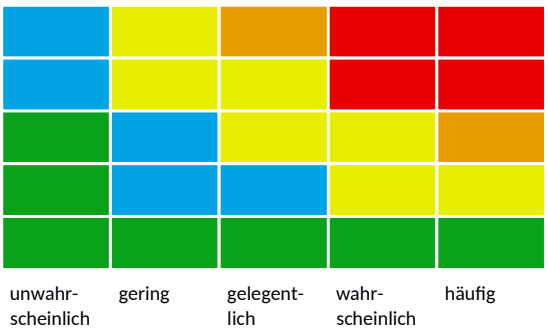
Aus dem erzielten Ergebnis Ihrer Risikoabschätzung resultieren nun die folgenden Maßnahmen:

| | | |
|---|---|---|
| Katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| Unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| Unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| Akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

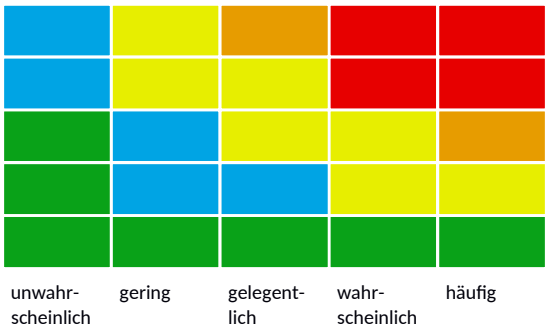
Lässt sich das Risiko nicht durch Schutzmaßnahmen intern minimieren, müssen wir eine sogenannte Datenschutzfolgenabschätzung vornehmen. Diese Pflicht hat ebenfalls zur Folge, dass wir einen (internen oder externen) Datenschutzbeauftragten bestellen müssen. Dieser berät bei der Durchführung einer solchen Datenschutzfolgenabschätzung.

Das Ergebnis der Risikoabschätzung ist zu dokumentieren. Hierzu bietet sich folgendes Muster an, das an die konkreten Verarbeitungstätigkeiten anzupassen ist:

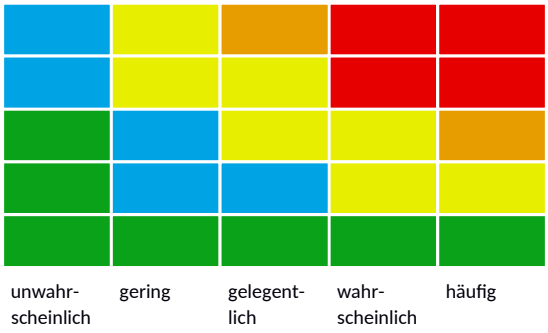
## Protokoll (Muster) Risikoabschätzung

| | |
|---|---|
| Verarbeitungstätigkeit: | Lohn- und Gehaltsabrechnung |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Angestellte Mitarbeiter |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  <br> |
| Ergebnis / Folgemaßnahmen: | |

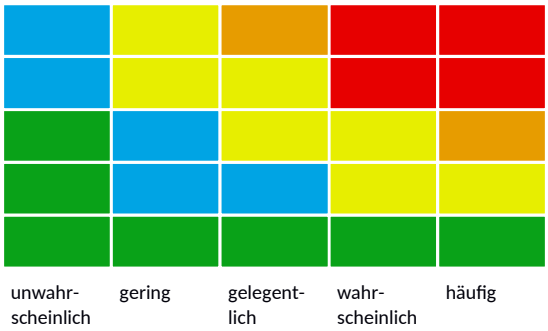
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | Spendenbuchhaltung |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  <br> |
| Ergebnis / Folgemaßnahmen: | |

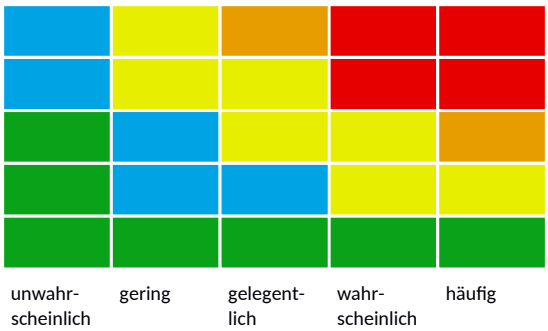
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | Beschaffung / Einkauf |
| Risiko: | erwünscht |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte<br>Dienstleister |
| Schutzmaßnahmen: | Verarbeitungstätigkeit ist unbedenklich |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

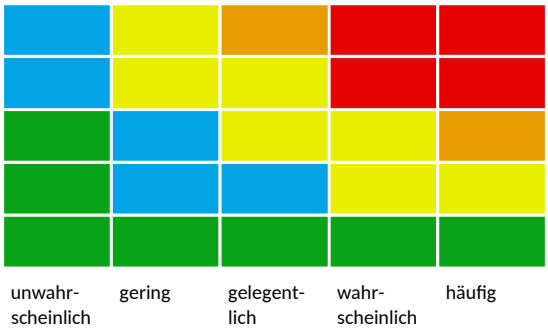
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | Verwaltung / Organisation |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

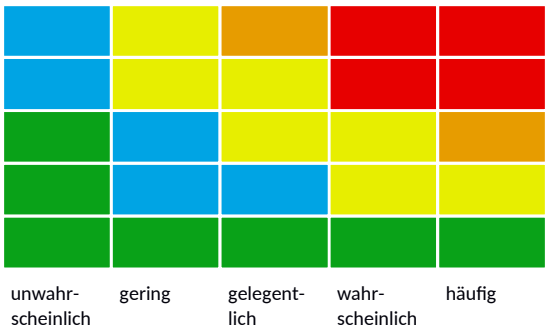
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | Kontaktverwaltung |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  <br> |
| Ergebnis / Folgemaßnahmen: | |

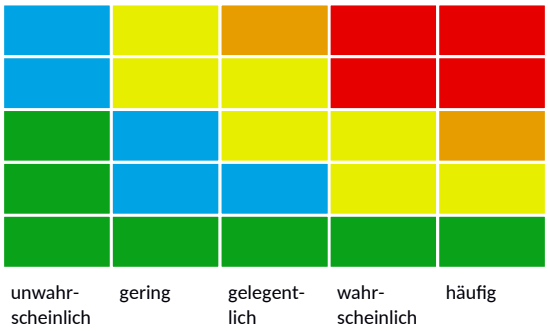
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | Terminvereinbarung |
| Risiko: | erwünscht |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte<br>Dienstleister |
| Schutzmaßnahmen: | Verarbeitungstätigkeit ist unbedenklich |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

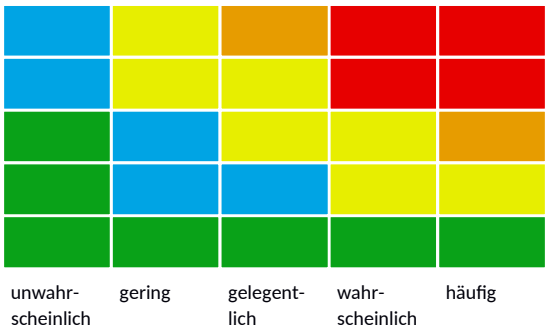
| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

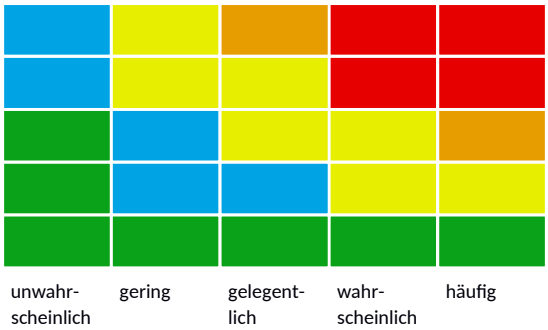
| | |
|---|---|
| Verarbeitungstätigkeit: | Projektmanagement |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

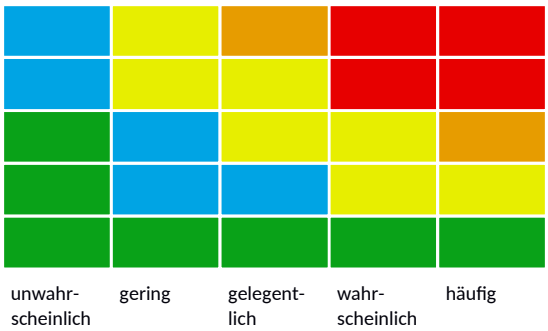
| | |
|---|---|
| Verarbeitungstätigkeit: | Mitgliederverwaltung |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

<table>
<tr><td>Verarbeitungstätigkeit:</td><td>Einladeaktionen</td></tr>
<tr><td>Risiko:</td><td>erwünscht</td></tr>
<tr><td>Datenkategorien zur Risikoabschätzung:</td><td>Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich</td></tr>
<tr><td>Betroffene:</td><td>Mitglieder<br>Freunde<br>Dritte<br>Dienstleister</td></tr>
<tr><td>Schutzmaßnahmen:</td><td>Verarbeitungstätigkeit ist unbedenklich</td></tr>
<tr><td>Einstufung des Risikos (physisch, materiell, immateriell):</td><td>katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  <br></td></tr>
<tr><td>Ergebnis / Folgemaßnahmen:</td><td><table>
<tr><td>katastrophal</td><td></td><td>Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden</td></tr>
<tr><td>unakzeptabel</td><td></td><td>Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden</td></tr>
<tr><td>unerwünscht</td><td></td><td>Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden</td></tr>
<tr><td>akzeptabel</td><td></td><td>Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden</td></tr>
<tr><td>erwünscht</td><td></td><td>Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich</td></tr>
</table></td></tr>
</table>

| | |
|---|---|
| Verarbeitungstätigkeit: | IT-Management |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  |
| Ergebnis / Folgemaßnahmen: | |

| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

| | |
|---|---|
| Verarbeitungstätigkeit: | E-Mailverarbeitung |
| Risiko: | akzeptabel |
| Datenkategorien zur Risikoabschätzung: | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| Betroffene: | Mitglieder<br>Freunde<br>Dritte |
| Schutzmaßnahmen: | Verarbeitungstätigkeit sollten beobachtet werden |
| Einstufung des Risikos (physisch, materiell, immateriell): | katastrophal<br>signifikant<br>moderat<br>gering<br>vernachlässigbar<br>  <br> |
| Ergebnis / Folgemaßnahmen: | |

| | | |
|---|---|---|
| katastrophal | | Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit muss umgestaltet werden |
| unakzeptabel | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen erweitert werden |
| unerwünscht | | Datenschutzfolgeabschätzung erforderlich / Schutzmaßnahmen müssen überprüft und ggf. erweitert werden |
| akzeptabel | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit sollten beobachtet werden |
| erwünscht | | Keine Datenschutzfolgeabschätzung erforderlich / Verarbeitungstätigkeit ist unbedenklich |

# Datenschutzhinweise Webseite

**erstellt am**

**30.12.2019**

**für**

**Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg**

## Datenschutzerklärung

Ihr Vertrauen ist uns wichtig. Die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg nimmt den Schutz Ihrer persönlichen Daten sehr ernst. Personenbezogene Daten werden nur dann erhoben, verarbeitet oder genutzt, wenn der Betroffene eingewilligt hat, diese für unser Miteinander erforderlich sind oder ein Gesetz die Erhebung, Verarbeitung oder Nutzung erlaubt oder vorschreibt.

Mit dieser Datenschutzerklärung möchten wir Sie über Einzelheiten der Datenerhebung und Datenverarbeitung sowie über die Ihnen in diesem Zusammenhang zustehenden Rechte informieren.

## 1. Name und Anschrift des Verantwortlichen

Verantwortlicher im Sinne der Datenschutz-Grundverordnung, anderer in den Mitgliedstaaten der Europäischen Union geltenden Datenschutzgesetze und sonstiger datenschutzrechtlicher Bestimmungen ist die:

Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg, Thie 1, 30539 Hannover;
E-Mail.: webmaster@baptisten-kronsberg.de

## 2. Grundsätzliches zur Verarbeitung personenbezogener Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg verarbeitet personenbezogene Daten grundsätzlich nur, wenn der Nutzer hierzu seine Einwilligung erteilt oder die Datenverarbeitung durch gesetzliche Vorschriften erlaubt ist. Rechtsgrundlage ist Art. 6 Abs. 1 EU-Datenschutzgrundverordnung (DSGVO). Nach dieser Vorschrift ist eine Verarbeitung personenbezogener Daten nur zulässig, wenn die betroffene Person einwilligt (Art. 6 Abs.1 lit. a DSGVO) oder die Verarbeitung zu einer der folgenden Zwecke erforderlich ist:

- Zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person (Art. 6 Abs.1 lit. b DSGVO).
- Zur Erfüllung einer rechtlichen Verbindlichkeit (Art. 6 Abs.1 lit. c DSGVO).
- Zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person (Art. 6 Abs.1 lit. d DSGVO).
- Zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder die uns von der öffentlichen Verwaltung übertragen wurde (Art. 6 Abs.1 lit. e DSGVO).
- Zur Wahrung eines berechtigten Interesses unserer Gemeinde oder eines Dritten, sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person zum Schutz personenbezogener Daten überwiegen (Art. 6 Abs.1 lit. f DSGVO).

## 3. Speicherdauer und Datenlöschung

Die personenbezogenen Daten der betroffenen Person werden gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt. Eine Speicherung kann darüber hinaus erfolgen, wenn dies durch den Gesetzgeber vorgesehen wurde. Eine Sperrung oder Löschung der Daten erfolgt auch dann, wenn eine durch die genannten Normen vorgeschriebene Speicherfrist abläuft, es sei denn, dass eine Erforderlichkeit zur

weiteren Speicherung der Daten für eine Vertragserfüllung besteht. Vorgeschriebene Speicherfristen in diesem Sinne sind z.B. steuerrechtliche oder handelsrechtliche Aufbewahrungsfristen.

## 4. Erfassung von Zugriffsdaten (Erstellung von Logfiles)

Die Internetseite der Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg erfasst bei jedem Aufruf automatisiert allgemeine Daten und Informationen vom Computersystem des aufrufenden Rechners, welche in den Logfiles des Servers gespeichert werden. Erfasst werden hierbei folgende Daten und Informationen:

- Browsertyp einschließlich verwendeter Version
- Verwendetes Betriebssystem des aufrufenden Rechners
- Datum und Zeit des Aufrufs
- IP-Adresse des Nutzers
- Internet-Service-Provider des Nutzers
- Webseite, von denen unsere Internetseite aufgerufen wird
- Webseiten und Unterwebseiten, die von unserer Internetseite aufgerufen werden
- Sonstige ähnliche Daten und Informationen, die der Gefahrenabwehr bei Angriffen auf unserem System dienen

Die Daten werden anonym in den Logfiles unseres Systems gespeichert. Dabei erfolgt keine Verknüpfung mit anderen personenbezogenen Daten des Nutzers, die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg zieht keine Rückschlüsse auf die betroffene Person.

Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs.1 lit. f DSGVO. Die Speicherung ist erforderlich, um die Funktionsfähigkeit unserer Internetseite und die korrekte Darstellung der Inhalte zu gewährleisten. Weiterhin dienen die Daten unserer Statistik und der ständigen Optimierung unserer Inhalte. Schließlich erfolgt eine Speicherung, um Strafverfolgungsbehörden im Falle eines Cyberangriffes die zur Strafverfolgung notwendigen Informationen zur Verfügung zu stellen.

Es erfolgt keine Weitergabe der Daten an Dritte, sofern keine gesetzliche Offenbarungspflicht besteht.

Da die Erfassung und Speicherung der Daten in den Logfiles für einen störungsfreien Betrieb der Internetseite zwingend erforderlich ist, besteht für den Nutzer keine Widerspruchsmöglichkeit.

Die Daten werden gelöscht, sobald sie für die Erreichung des Zweckes ihrer Erhebung nicht mehr erforderlich sind. Soweit die Erhebung zur funktionsfreien Bereitstellung der Internetseite erfolgte, ist dies mit Beendigung der Internetsitzung der Fall.

## 5. Cookies

Wir verwenden auf unserer Internetseite Cookies. Bei Cookies handelt es sich um Textdateien, welche von unserem Server auf Ihrem Computer abgelegt und so bestimmte Daten gespeichert werden. Cookies enthalten in der Regel eine charakteristische Zeichenfolge, welche eine eindeutige Zuordnung des Internetbrowsers ermöglicht, wenn der Nutzer die Internetseite erneut aufruft. Hierdurch kann der aufrufende Browser wiedererkannt und identifiziert werden.
Cookies helfen uns, Ihnen die Nutzung der Internetseite zu erleichtern. Durch die Wiedererkennung des Browsers und die Speicherung früher eingegebener Daten können die Angebote und Inhalte unserer Internetseite individuell optimiert werden, indem von Ihnen eingegebene Daten (z.B. Zugangsdaten, Suchbegriffe) nicht bei jedem Besuch der Internetseite erneut eingegeben werden müssen. Rechtsgrundlage hierfür ist Art. 6 Abs.1 lit. f DSGVO.
Darüber hinaus verwenden wir auf unserer Internetseite Cookies, die eine Analyse des Surfverhaltens der

Nutzer ermöglichen. Die so erhobenen Daten werden jedoch pseudonymisiert, d.h. die personenbezogenen Daten werden durch andere Kennzeichen (Pseudonyme) ersetzt, so dass ohne Hinzuziehung zusätzlicher Informationen keine Identifikation der betroffenen Person mehr möglich ist. Da hierzu bei Aufruf der Internetseite Ihre Einwilligung eingeholt wird, ist Rechtsgrundlage für die Verarbeitung personenbezogener Daten mittels Analyse-Cookies Art. 6 Abs.1 lit. a DSGVO.

Da Cookies auf dem Rechner des Nutzers gespeichert werden, haben Sie als Nutzer auch die volle Kontrolle über die Verwendung von Cookies. Durch eine Änderung der Einstellungen in Ihrem Internetbrowser können Sie die Übertragung von Cookies deaktivieren oder einschränken. Bereits gespeicherte Cookies können von Ihnen jederzeit gelöscht werden. Werden Cookies für unsere Internetseite deaktiviert, können jedoch möglicherweise nicht mehr alle Funktionen der Website vollumfänglich genutzt werden.

## 6. Ihre Rechte als betroffene Person

Werden personenbezogene Daten von Ihnen verarbeitet, sind Sie betroffene Person i.S.d. DSGVO und es stehen Ihnen folgende Rechte gegenüber uns als Verantwortlichem zu:

### a) Recht auf Bestätigung und Auskunft

Sie können von uns jederzeit eine Bestätigung verlangen, ob personenbezogene Daten, die Sie betreffen, von uns verarbeitet werden. Ist dies der Fall, haben Sie einen Auskunftsanspruch, von uns über folgende Umstände in Kenntnis gesetzt zu werden:

- die Kategorien von personenbezogenen Daten, welche verarbeitet werden;
- die Empfänger bzw. die Kategorien von Empfängern, gegenüber denen die Sie betreffenden personenbezogenen Daten offengelegt wurden oder noch
- offengelegt werden; die geplante Dauer der Speicherung der Sie betreffenden personenbezogenen Daten oder, falls konkrete Angaben hierzu nicht möglich
- sind, Kriterien für die Festlegung der Speicherdauer;

das Bestehen eines Rechts auf Berichtigung oder Löschung der Sie betreffenden personenbezogenen Daten, eines Rechts auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden; das
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Darüber hinaus steht Ihnen ein Auskunftsrecht zu, ob personenbezogene Daten in einen Staat, der nicht Mitglied der EU ist (sog. Drittland), oder an eine internationale Organisation übermittelt werden. In diesem Zusammenhang können Sie verlangen, über die geeigneten Garantien gem. Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

### b) Recht auf Berichtigung

Sie haben das Recht, die unverzügliche Berichtigung bezüglich Sie betreffender unrichtiger personenbezogener Daten von uns zu verlangen. Ferner steht Ihnen das Recht zu, von uns unter Berücksichtigung der Zwecke der Verarbeitung, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

## c) Recht auf Löschung (Recht auf Vergessen werden)

Sie können von uns verlangen, dass die Sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, wenn einer der folgenden Gründe vorliegt:

- Die Sie betreffenden personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Sie widerrufen Ihre Einwilligung, auf die sich die Verarbeitung gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO stützte, und es fehlt an einer anderweitigen
- Rechtsgrundlage für die Verarbeitung. Sie legen gem. Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder Sie legen gem. Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein.
- Die Sie betreffenden personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der Sie betreffenden personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die Sie betreffenden personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Wurden die Sie betreffenden personenbezogenen Daten von der Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg öffentlich gemacht und sind wir nach obenstehenden Grundsätzen zur Löschung der personenbezogenen Daten verpflichtet, so trifft uns ebenfalls die Pflicht andere für die Datenverarbeitung Verantwortliche darüber in Kenntnis zu setzen, dass Sie als betroffene Person die Löschung sämtlicher Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt haben.

Wir ergreifen diesbezüglich, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um diesen Pflichten nachzukommen, jedenfalls soweit die Verarbeitung nicht weiterhin erforderlich ist, also gesetzliche Vorgaben dies vorschreiben oder berechtigte Interessen der Löschung entgegenstehen.

## d) Recht auf Einschränkung der Verarbeitung

Sie können unter den folgenden Voraussetzungen von uns die Einschränkung der Verarbeitung der Sie betreffenden personenbezogenen Daten verlangen:

- Die Richtigkeit der personenbezogenen Daten wird Ihnen bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der
- personenbezogenen Daten zu überprüfen. Die Verarbeitung ist unrechtmäßig und Sie verlangen anstatt einer Löschung die Einschränkung der Nutzung der
- personenbezogenen Daten.

Die personenbezogenen Daten werden von uns nicht länger für die Zwecke der Verarbeitung benötigt, jedoch benötigen Sie diese Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

- Sie haben Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DSGVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe der Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg gegenüber Ihren Gründen überwiegen.

Wurde die Verarbeitung der Sie betreffenden personenbezogenen Daten eingeschränkt, dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Ihrer Einwilligung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen

Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden. In diesem Fall werden Sie zudem von uns unterrichtet, bevor die Einschränkung aufgehoben wird.

## e) Recht auf Unterrichtung

Haben Sie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung geltend gemacht, sind wir verpflichtet, allen Empfängern, denen die Sie betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung oder Löschung der Daten oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Insoweit können Sie von uns verlangen, über diese Empfänger unterrichtet zu werden.

## f) Recht auf Datenübertragbarkeit („Datenportabilität“)

Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, welche Sie uns zur Verfügung gestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Des Weiteren haben Sie das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf der Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a DSGVO oder Art. 9 Abs. 2 Buchstabe a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 Buchstabe b DSGVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, sofern die Verarbeitung nicht für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem Verantwortlichen übertragen wurde.

Ferner können Sie bei der Ausübung Ihres Rechts auf Datenübertragbarkeit gemäß Art. 20 Abs. 1 DSGVO verlangen, dass die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist und sofern hierdurch keine die Rechte und Freiheiten anderer Personen beeinträchtigt werden.

## g) Widerspruchsrecht

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, von uns jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f DSGVO erfolgt, Widerspruch einzulegen. Dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.

Die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg verarbeitet die personenbezogenen Daten im Falle des Widerspruchs nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Werden die Sie betreffenden personenbezogenen Daten verarbeitet, um Direktwerbung zu betreiben, haben Sie das Recht, jederzeit Widerspruch gegen die Verarbeitung der Sie betreffenden personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden die Sie betreffenden personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

Sie haben die Möglichkeit, im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft – ungeachtet der Richtlinie 2002/58/EG – Ihr Widerspruchsrecht mittels automatisierter Verfahren auszuüben, bei denen technische Spezifikationen verwendet werden.

## h) Recht auf Widerruf einer datenschutzrechtlichen Einwilligung

Sofern Sie eine datenschutzrechtliche Einwilligung erteilt haben, steht Ihnen das Recht zu, diese Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

## i) Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Sie haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die Ihnen gegenüber rechtliche Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt, sofern die Entscheidung

- nicht für das Miteinander zwischen Ihnen und der Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg erforderlich ist, oder
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedsstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Allerdings dürfen diese Entscheidungen nicht auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen, sofern nicht Art. 9 Abs. 2 lit. a oder g DSGVO gilt und angemessene Maßnahmen
zum Schutz der Rechte und Freiheiten sowie Ihrer berechtigten Interessen getroffen wurden.

Ist die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich oder erfolgt sie mit ausdrücklicher Einwilligung der betroffenen Person, trifft die Evangelisch-Freikirchliche Gemeinde Hannover-Kronsberg angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

## j) Recht auf Beschwerde bei der Aufsichtsbehörde

Ungeachtet der gegenüber uns bestehenden Rechte, steht Ihnen auch das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedsstaat Ihres Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet Sie über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Art. 78 DSGVO.