**Königsberger Ladungssicherungskreis e.V.**

# IT-Sicherheitsrichtlinie

Scholwin, Mathias (Verkehrsüberwachungsdienst)

**Königsberger Ladungssicherungskreis e.V.**

Heisterbacher Straße 239, 53639 Königswinter

geschaeftsstelle@klsk.de

Stand:
24.04.2020

# Inhalt

# 1. Einleitung

Diese IT-Richtlinie soll die vom Verein getroffenen Maßnahmen zum Schutz von (personenbezogenen) Daten vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeiter, Mitglieder unterstützen und darüber hinaus eine grundlegende Information für alle Mitarbeiter und Mitglieder im Hinblick auf den Umgang mit Daten sein.

IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Diese umfasst die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).

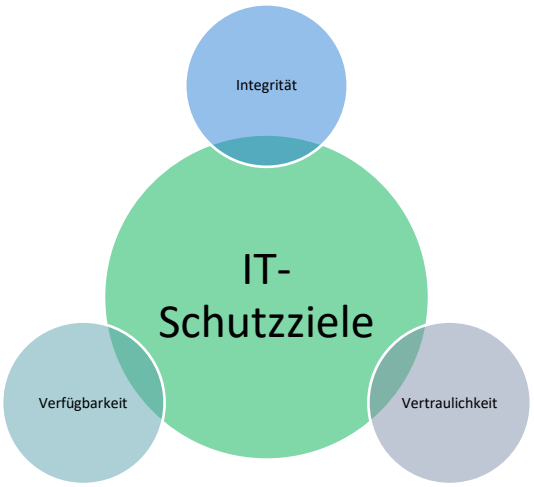


*Abbildung 1: IT-Schutzziele der Informationssicherheit*

Die Vorgaben des Datenschutzes werden unter anderem durch die EU-Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz geregelt. Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung und den Umgang seiner personenbezogenen Daten in dem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Alle Mitarbeiter sowie Projektmitglieder sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten.

Siehe: *Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung der datenschutzrechtlichen Regelungen*

Es sind technisch-organisatorische Maßnahmen gemäß Art 32 DSGVO zu entwickeln. Ziel ist die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung und die Einsichtnahme in bestehende Daten.


*Abbildung 2: Betroffenenrechte nach DSGVO*

## 2. Geltungsbereich

Diese IT-Sicherheitsrichtlinie gilt für alle Mitarbeiter und Projektmitglieder des Königsberger Ladungssicherungskreises e.V (KLSK®).

Dazu gehören alle Mitglieder die aktiv, unterstützend oder in sonstiger Form im Vorstand, Beirat oder Fachausschüssen tätig sind oder diese bei Ihrer Arbeit unterstützen.

Die Richtlinie gilt für alle Formen der Verarbeitung von personenbezogenen Daten. Hierzu zählen nach Art. 4 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Diese Richtlinie gilt auch für externe Personen die unterstützend oder in anderer Form für den Verein bei Erreichung seiner satzungsmäßigen Ziele tätig werden.

## 3. Begriffsbestimmungen

| | |
|---|---|
| **Betroffener (Art. 4 Nr. 1 DSGVO)** | • jede identifizierte oder identifizierbare natürliche Person |
| **Datenverarbeitung (Art. 4 Nr. 2 DSGVO)** | • jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten<br>• erheben, erfassen, organisieren, ordnen, speichern, anpassen, auslesen, abfragen, löschen, einschränken etc. |
| **Mitarbeiter** | • Vereinsmitglieder die im Vorstand, Beirat, Geschäftsstelle aktiv tätig sind |
| **personenbezogene Daten (Art. 4 Nr. 1 DSGVO)** | • alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen |
| **Projektmitglied** | • Mitglieder oder externe Personen die in Fachausschüssen tätig sind<br>• Mitglieder die als Kassenprüfer aktiv sind |

## 4. Einhaltung von Rechtsvorschriften

Bei der Benutzung von IT-Systemen und Applikationen im Verein sind die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Datenschutzordnung des KLSK® einzuhalten. Sollten Mitarbeiter oder Projektmitglieder unsicher sein, ob und inwieweit Rechtsvorschriften oder Vereinsregelungen einzuhalten sind, ist der Vorstand zur Klärung anzurufen.

## 5. Allgemeine Regelungen

Die Nutzung von IT-Systemen und Applikationen im KLSK® hat unter größtmöglicher Gewährleistung des Datenschutzes zu erfolgen.

Vom Verein genutzte Applikationen und Software darf nur für die Organisation und Verwaltung der Vereinsarbeit genutzt werden.

## 6. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern oder Projektmitgliedern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein.

Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter oder das Projektmitglied sich „abmelden“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme – insbesondere die Bildschirme – 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.

## 7. Passwort-Gebrauch

Soweit technisch möglich sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers zugänglich. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen sowie mit Zeichen und/oder Sonderzeichen) zu gestalten. Die genannten Anforderungen sind nach Möglichkeit auch bei der Nutzung von Software und Applikationen zu beachten.

Jeder Mitarbeiter oder jedes Projektmitglied ist 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. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter sollten regelmäßig gewechselt werden. Bereits genutzte Passwörter dürfen nicht noch einmal wiederverwendet werden.

## 8. Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten auf dem IT-System sollte eigenverantwortlich ein Virenschutzprogramm eingesetzt werden. Insbesondere eingehende E-Mail-Kommunikation soll durch das eingesetzte Virenschutzprogramm überprüft werden. Automatische Updates sollen aktiviert sein. Dabei muss sichergestellt werden, dass auch mobile Endgeräte ausreichend geschützt sind.

Bei unbekannten oder verdächtigem E-Mailanhängen sollten diese nicht geöffnet werden. Weiter ist auf unbekannte oder verdächtige E-Mailabsender und den vorsichtigen Umgang mit entsprechenden Mails zu achten.

## 9. Nutzung von E-Mail/Internet

Bei der Nutzung von E-Mail oder Internet-Programmen bzw. Applikationen ist auf die Aktualität der Programme zu achten. Es sollen regelmäßig die veröffentlichten sicherheitsrelevanten Updates und Patches installiert werden und die jeweils aktuelle Version der Software, Applikation genutzt werden.

## 10. Verhalten bei Sicherheitsvorfällen und Datenpannen

Sollte der Mitarbeiter oder das Projektmitglied merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, ist unverzüglich der Vorstand des KLSK® zu informieren. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

Sollte es zu einer Verletzung des Schutzes von personenbezogenen Daten kommen oder gekommen sein, so ist unverzüglich der Vorstand über die Datenpanne zu informieren. Eine Datenpanne kann vorliegen, wenn z.B. ein Hackerangriff erfolgt ist oder mobile Datenträger mit personenbezogenen Daten des KLSK® verloren gegangen sind.

Durch den Vorstand ist in diesen Fällen unter Umständen die datenschutzrechtliche Aufsichtsbehörde zu informieren.

## 11. Änderungshistorie

| Datum | Beschreibung der Änderung | Änderung durch |
|---|---|---|
| **24.02.2020** | Erstellung der Richtlinie | Scholwin, Mathias |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |