



Leitlinie Datenschutz

Revisionsverfolgung

Revision	Datum	Autor	Beschreibung der Änderung	Freigabe	Datum
1.0	05.04.2018	Klaus Pöpperl	Anpassung des Dokuments an SVE	Klaus Pöpperl	05.04.2018

Inhaltsverzeichnis

1	Leitgedanken	4
2	Grundsätze des Datenschutzes	4
3	Wahrung der Rechte betroffener Personen	5
4	Umsetzung	5
5	Fortlaufende Verbesserung	6
6	Verantwortung des Managements	6
7	Schlussbestimmungen	6

1 Leitgedanken

Für den SV Erolzheim ist Datenschutz nicht nur ein gesetzliches Erfordernis, sondern Ausdruck des ehrlichen und fairen Verhaltens gegenüber Funktionsträgern und Mitgliedern. Daher ist es ein erklärtes Ziel des Vereins, sowohl die Persönlichkeitsrechte der Mitglieder als auch der Funktionsträger zu schützen. Zu diesem Zweck schafft der SV Erolzheim ein angemessenes Datenschutzniveau im Sinne der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union.

Ein stets vorhandenes Bewusstsein im Bereich Datenschutz bei allen anfallenden Aktivitäten wird von jedem Mitglied erwartet. Jeder Funktionsträger ist verpflichtet, die Einhaltung der Vorschriften zum Datenschutz durch seine Mitarbeiter sicherzustellen und zu kontrollieren. Jedes Mitglied, das Schwachstellen im Bereich des Datenschutzes erkennt, ist verpflichtet, diese seinem Abteilungsleiter oder dem Vorstand zu melden.

2 Grundsätze des Datenschutzes

Alle Mitglieder insbesondere die Funktionsträger sind verpflichtet, die Grundsätze des Datenschutzes bei der Verarbeitung von Daten zu beachten.

Die Verarbeitung umfasst alle Arten des Umgangs mit personenbezogenen Daten, insbesondere:

- erheben
- erfassen
- organisieren
- ordnen
- speichern
- anpassen oder verändern
- auslesen
- abfragen
- verwenden
- übermitteln
- einschränken
- löschen oder vernichten

Hierzu gehören insbesondere:

Transparenz

Alle betroffenen Personen müssen über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Hierzu gehört insbesondere die Mitteilung über die erhobenen Daten sowie die zugehörigen Verarbeitungszwecke.

Zweckbindung und Löschung

Vor der Erhebung von personenbezogenen Daten muss ein eindeutiger und legitimer Verwendungszweck für die Verarbeitung festgelegt werden. Wenn personenbezogene Daten zu einem anderen Zweck weiterverarbeitet werden sollen, müssen diese Zweckänderung und die Legitimität der Verarbeitung erneut geprüft und dokumentiert werden. Werden personenbezogene Daten für den definierten Zweck nicht mehr benötigt, sind diese zu löschen.

Richtigkeit

Die erhobenen personenbezogenen Daten müssen sachlich richtig, vollständig und aktuell sein.

Datensparsamkeit

Jede Verarbeitung von personenbezogenen Daten durch Personen oder durch Informationssysteme ist so zu gestalten, dass nur solche personenbezogenen Daten erhoben und verarbeitet werden, die zur Arbeitserfüllung bzw. zur Verfolgung des Vereinszweckes erforderlich sind. Die Erhebung und Verarbeitung zusätzlicher Informationen ist zu vermeiden.

Technische und organisatorische Maßnahmen

Es müssen technische und organisatorische Maßnahmen zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten eingesetzt werden, d.h. Maßnahmen, die personenbezogene Daten vor unbefugtem Zugriff und unrechtmäßiger Verarbeitung sowie vor Manipulation, Verlust und Zerstörung schützen.

Besondere Kategorien personenbezogener Daten

Personen bezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie genetische Daten, biometrische Daten oder Gesundheitsdaten unterliegen einem besonderen Schutz. Solche Daten sind immer als – Streng vertraulich – einzuordnen. Ihre Verarbeitung ist grundsätzlich nur durch die Mitgliederverwaltung erlaubt.

3 Wahrung der Rechte betroffener Personen

Jede betroffene Person hat unabdingbare Rechte, wenn ihre personenbezogenen Daten verarbeitet werden. Für alle SVE- Mitglieder oder Funktionsträger besteht die Pflicht, sofern sie für die Verarbeitung personenbezogener Daten verantwortlich sind, Prozesse und Informationssystem so zu gestalten, dass nachfolgende Rechte gegenüber betroffenen Personen gewahrt werden:

- **Recht auf Auskunft** über die gespeicherten personenbezogenen Daten und die damit verbundene Datenverarbeitung.
- **Recht auf Informiert-Sein** über die gespeicherten personenbezogenen Daten und die damit verbundene Datenverarbeitung.
- **Recht auf Berichtigung** der gespeicherten und verarbeiteten personenbezogenen Daten.
- **Recht auf Löschung** der personenbezogenen Daten, wenn:
 - der Zweck der Verarbeitung erfüllt ist und die Daten deswegen nicht mehr benötigt werden,
 - die betroffene Person eine von ihr erteilte Einwilligung widerrufen hat,
 - die Daten unrechtmäßig erhoben oder verarbeitet wurden,
 - keine gesetzliche Pflicht zur Aufbewahrung der Daten mehr besteht.
- **Recht auf Widerspruch** einer erteilten Einwilligung bzw. einer Verarbeitung.

4 Umsetzung

Der SV Erolzheim setzt zur Sicherstellung der Umsetzung von Datenschutzanforderungen ein Datenschutzmanagementsystem (DSMS) in Anlehnung an den internationalen Standard ISO/IEC 27001:2013 ein. Das DSMS folgt dem dort empfohlenen kontinuierlichen Verbesserungsprozess auf Basis des PDCA-Modells (Plan, Do, Check, Act). Ziel ist es, nachweislich und regelmäßig die Angemessenheit, Vollständigkeit, Nachhaltigkeit, Effektivität und Effizienz im Datenschutz sicherzustellen.

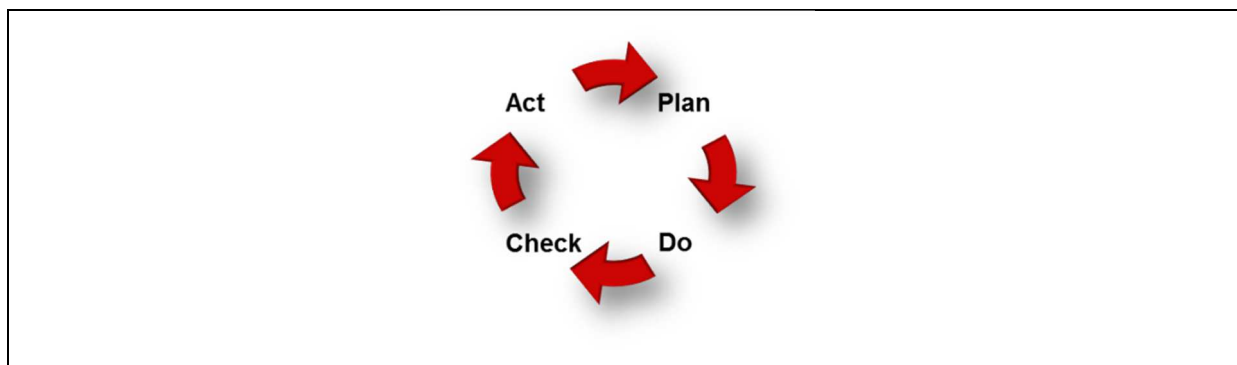


Abbildung 1: PDCA-Modell

PLAN - Festlegen des DSMS: Die Strategien, Ziele, Prozesse, Regelungen, Verfahren, Methoden, Werkzeuge und Verantwortlichkeiten des DSMS werden festgelegt.

DO - Umsetzen und Durchführen des DSMS: Die definierten Prozesse, Regelungen und Verfahren werden entsprechend der Ziele des DSMS umgesetzt. Ausgewählte Maßnahmen werden implementiert.

CHECK - Überwachen und Überprüfen des DSMS: Anhand praktischer Erfahrungen, den Ergebnissen von Audits und Managementbewertungen werden die Prozesse, Wirksamkeit und Effizienz der gewählten Ansätze und Maßnahmen gemessen und überprüft. Es wird identifiziert, ob Handlungsbedarf besteht und an welchen Stellen Optimierungsmöglichkeiten vorhanden sind.

ACT - Instandhalten und Verbessern des DSMS: Basierend auf den Ergebnissen der Phase Check und sonstiger Rückmeldungen (z.B. aktuelle Risikosituation / Bedrohungslage / Weiterentwicklungen / Anforderungen), werden Korrektur- und Vorbeugemaßnahmen ergriffen, die zu einer fortlaufenden Verbesserung des DSMS und des Sicherheitsniveaus führen. Die Behandlung von Sicherheitsvorfällen ist eine weitere Aufgabe dieser Phase.

5 Fortlaufende Verbesserung

Das Datenschutzmanagementsystem muss laufend auf Eignung, Angemessenheit und Wirksamkeit analysiert und verbessert werden. Hierzu berichten die Abteilungsleiter über Änderungs- und Verbesserungsvorschläge an den Vorstand des Vereins. Die Anpassung des Datenschutzmanagementsystems liegt in der Zuständigkeit des Vorstands.

6 Verantwortung des Vorstands

Die Leitung jeder Abteilung des SV Erolzheim ist unter Beachtung lokaler und organisatorischer Besonderheiten verantwortlich, die Vorgaben dieser Leitlinie und ihrer Anlagen in der Abteilung umzusetzen. Die Abteilungsleitung verpflichtet sich dabei, die hierfür erforderlichen personellen, organisatorischen und finanziellen Ressourcen bereitzustellen, um somit ein angemessenes Datenschutzniveau nach Maßgaben des DSMS zu etablieren, aufrechtzuerhalten und weiterzuentwickeln. Die Abteilungsleitung trägt insbesondere auch die Verantwortung für die Akzeptanz eventuell bestehender Restrisiken bei nicht realisierten Maßnahmen zur Reduzierung des Risikos für die betroffene Person.

7 Schlussbestimmungen

Die Anlagen zu dieser Leitlinie bestehen aus detaillierten Organisationsvorgaben und Managementprozessbeschreibungen. Sie werden regelmäßig überprüft und ggf. aktualisiert. Sie haben den gleichen Geltungsbereich wie diese Leitlinie und sind jeweils ab dem Zeitpunkt ihrer Veröffentlichung gültig.

Vorstand SV Erolzheim 1922 e.V.

Klaus Pöpperl

Vorsitzender

Monika Wastlbauer

Finanzvorstand/Mitgliederverwaltung

Übersicht Anlagen

Anlage	Inhalt
Anlage A	Datenschutzorganisation
Anlage B	Schutzziele und Schutzklassen