



Schutzziele und Schutzklassen

Anlage B zur Leitlinie Datenschutz

Revisionsverfolgung

Revision	Datum	Autor	Beschreibung der Änderung	Freigabe	Datum
1.0	01.05.18	Klaus Pöpperl	Erstellung des Dokuments	Klaus Pöpperl	01.05.18

Inhaltsverzeichnis

1	Ziel und Zweck	4
2	Definition	4
3	Schutzziele und ihre Schutzklassen	5
3.1	Schutzklassen des Schutzziels Vertraulichkeit	6
3.2	Schutzklassen des Schutzziels Integrität	8
3.3	Schutzklassen des Schutzziels Verfügbarkeit / Belastbarkeit.....	10

1 Ziel und Zweck

Um personenbezogene Daten durch technische und organisatorische Schutzmaßnahmen angemessen schützen zu können, ist es wichtig festzulegen, welchen grundsätzlichen Schutzbedarf die verarbeiteten Daten haben.

Die Kernidee dahinter ist: Ein hoher Schutzbedarf, etwa für einen als besonders sensibel eingestuften Vereinsprozess, bedeutet den Einsatz von zusätzlichen und stärker dimensionierten technischen und organisatorischen Schutzmaßnahmen.

Es wird von jedem Funktionsträger bei der täglich anfallenden Arbeit erwartet, dass er die vorgegebenen Schutzmaßnahmen beim Umgang mit personenbezogenen Daten kennt und einhält. Jeder Funktionsträger ist verpflichtet, die Mitglieder bei Anfragen über die Schutzmaßnahmen zu informieren und die Einhaltung dieser Schutzmaßnahmen sicherzustellen und zu kontrollieren.

2 Definition

Um den Schutzbedarf strukturiert festzuschreiben und entsprechend klassifizieren zu können, werden die nachfolgenden Schutzziele definiert:

Schutzziel	Definition
Vertraulichkeit	Vertraulichkeit bedeutet, dass personenbezogene Daten nur dem jeweils berechtigten Personenkreis bekannt und zugänglich sind und lediglich durch berechnigte Personen auf diese zugegriffen werden darf. Dies gilt sowohl für elektronisch verarbeitete Daten, physisch verwendete Informationen, als auch das gesprochene Wort.
Integrität	Integrität bestimmt, dass personenbezogene Daten über einen bestimmten oder unbestimmten Zeitraum vollständig und unverändert sein sollen. Eine Veränderung (Manipulation) könnte absichtlich, unabsichtlich oder durch einen technischen Fehler auftreten. Integrität dient damit dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung.
Verfügbarkeit / Belastbarkeit	Das Schutzziel der Verfügbarkeit und Belastbarkeit dient dem Schutz personenbezogener Daten vor unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung und soll gewährleisten, dass diese im Bedarfsfall zur Verfügung stehen.

Abbildung 1: Schutzziele

Für jedes Schutzziel gibt es unterschiedliche Schutzklassen, die in Kapitel 3 ausführlich beschrieben werden.

3 Schutzziele und ihre Schutzklassen

Jedes Schutzziel ist in vier Schutzklassen (0 bis 3) kategorisiert, wobei 0 die geringste und 3 die höchste Anforderungsstufe an die Schutzwürdigkeit beschreibt.

Ein allgemeines Klassifikationskriterium bei der Verwendung von Schutzklassen ist der (potentielle) Schaden oder die Gefährdung, die bei einer möglichen Verletzung eines oder mehrerer Schutzziele zu erwarten ist. Die folgende Darstellung fasst die Zusammenhänge von Schutzzielen, Schutzbedarf und Schutzklassen zusammen.

	Schutz- klasse	Schutzziele			Potentieller Schaden bei einer Verletzung
		Vertraulichkeit	Integrität	Verfügbarkeit/ Belastbarkeit	
Schutzbedarf ↓	0	Öffentlich	Gering	Gering	Gering Keine oder geringfügige Auswirkungen für die Rechte und Freiheiten der betroffenen Person.
	1	Intern	Mittel	Mittel	Mittel Moderate Auswirkungen für die Rechte und Freiheiten der betroffenen Person
	2	Vertraulich	Hoch	Hoch	Hoch Nachteile für die Rechte und Freiheiten der betroffenen Person; wirtschaftliche und soziale Beeinträchtigungen
	3	Streng vertraulich	Sehr hoch	Sehr hoch	Sehr hoch erhebliche Nachteile für die betroffene Person; wirtschaftliche und soziale Beeinträchtigungen; diskriminierende Wirkung; Möglichkeit des Identitätsdiebstahls

Abbildung 2: Schutzklassen

3.1 Schutzklassen des Schutzziels Vertraulichkeit

Klassifizierung Erläuterung zu Vertraulichkeit - Umgang

Öffentlich	<p><u>Personenkreis:</u> Informationen, die Jedermann innerhalb und außerhalb des Unternehmens bekannt gemacht werden dürfen.</p> <p><u>Merkmale:</u> Die Informationen sind von der betroffenen Person für die Öffentlichkeit bestimmt oder für die Öffentlichkeit freigegeben. Eine Kenntnisnahme ist Jedermann gestattet.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Spielberichte• Spieler- Passwesen• Kontaktdaten von Vereinsansprechpartnern• Vorstand im Impressum
Intern	<p><u>Personenkreis:</u> Informationen, die innerhalb der Vereinsorganisation (Mitglieder, Abteilungen etc.) zur Verfügung stehen, jedoch nicht ohne weiteres öffentlich zugänglich sind.</p> <p><u>Merkmale:</u> Die Kenntnisnahme der Daten durch Personen außerhalb der Unternehmensorganisation kann mit geringen negativen Auswirkungen für die Rechte und Freiheiten der betroffenen Person verbunden sein. Innerhalb der Vereinsorganisation ist jedoch nicht von nachteiligen Folgen für die betroffene Person auszugehen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Organisationsdokumentation• Internes Telefonbuch mit Kontaktdaten von Funktionsträgern• Mitteilungen an Abteilungsleiter• Protokolle
Vertraulich	<p><u>Personenkreis:</u> Informationen, die nur einem eingeschränkten Personenkreis innerhalb des Vereins (i. d. R. nur der Vorstand und Abteilungsleiter) bekannt sein dürfen.</p> <p><u>Merkmale:</u> Die unbefugte Kenntnisnahme der Daten wäre mit negativen Auswirkungen für die Rechte und Freiheiten der betroffenen Person verbunden. Der Zugang zu solchen Daten muss daher auf bestimmte Bereiche oder Personenkreise im Unternehmen beschränkt werden.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Unfälle• Geburtstage und Jubiläen• Daten der Mitarbeiterverwaltung

Klassifizierung Erläuterung zu Vertraulichkeit - Umgang

Streng
vertraulich

Personenkreis:

Informationen, die innerhalb des Vereins nur von einem stark eingeschränkten Personenkreis eingesehen werden dürfen.

Merkmale:

Die unberechtigte Kenntnisnahme der Daten hat erhebliche Auswirkungen für die Rechte und Freiheiten der betroffenen Person und kann mit wirtschaftlichen oder sozialen Nachteilen verbunden sein. Es ist mit diskriminierenden Wirkungen zu rechnen.

Beispiele:

- Aktuell nicht zutreffend für den SV Erolzheim.

[Abbildung 3: Schutzklassen der Vertraulichkeit](#)

-

3.2 Schutzklassen des Schutzziels Integrität

Klassifizierung	Erläuterung
0 - Kein Integritätsbedarf Gewährleistung der Integrität nicht erforderlich	<p><u>Personenkreis:</u> Die Änderung des Inhalts von personenbezogenen Daten ist jedermann gestattet.</p> <p><u>Merkmale:</u> Absichtlich oder unabsichtlich verfälschte oder unvollständige Daten führen zu keinen negativen Auswirkungen für die Rechte natürlicher Personen.</p> <p><u>Beispiele:</u> Anonymisierte oder pseudonymisierte Daten in Testanwendungen</p>
1 – Mittlerer Integritätsbedarf Gewährleistung der Integrität erforderlich	<p><u>Personenkreis:</u> Die Änderung des Inhalts ist wenigen Berechtigten gestattet. Veränderungen müssen nicht nachvollziehbar sein.</p> <p><u>Merkmale:</u> Absichtlich oder unabsichtlich verfälschte oder unvollständige Daten können unerhebliche Nachteile für die betroffenen Personen nach sich ziehen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Kontaktdaten• Hallenbelegungsplan
2 – Hoher Integritätsbedarf Gewährleistung der Integrität erforderlich	<p><u>Personenkreis:</u> Die Änderung des Inhalts ist nur wenigen Berechtigten gestattet. Änderungen müssen nachvollziehbar (dokumentiert) sein (wer hat geändert, was wurde geändert und wann wurde es geändert).</p> <p><u>Merkmale:</u> Absichtlich oder unabsichtlich verfälschte oder unvollständige Daten können wesentliche soziale, gesellschaftliche oder wirtschaftliche Nachteile für die betroffenen Personen nach sich ziehen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Homepage• Mitgliederverwaltung• Berechtigungsmanagement

Klassifizierung	Erläuterung
3 – Sehr hoher Integritätsbedarf Gewährleistung der Integrität ist essentiell	<p><u>Personenkreis:</u> Die inhaltliche Änderung ist grundsätzlich nicht gestattet.</p> <p><u>Merkmale:</u> Die absichtliche oder unabsichtliche Verfälschung oder Veränderung führte zu erheblichen Nachteilen für die betroffenen Personen und könnte ggf. die Möglichkeit des Identitätsdiebstahls oder -betrugs eröffnen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Finanzwesen• Digitale Signaturen

Abbildung 4: Schutzklassen der Integrität

3.3 Schutzklassen des Schutzziels Verfügbarkeit / Belastbarkeit

Klassifizierung	Erläuterung
0 - Gering	<p><u>Merkmale:</u> Der (dauerhafte) Verlust oder die Zerstörung der Daten ist gänzlich unbedeutend für die betroffenen Personen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Anonymisierte oder pseudonymisierte Daten in Testanwendungen
1 - Mittel	<p><u>Merkmale:</u> Der Verlust oder die Zerstörung der Daten kann mit negativen Auswirkungen für die Rechte und Freiheiten der betroffenen Personen verbunden sein. Eine längere temporäre Nichtverfügbarkeit (max. 5 Tage) hätte jedoch keine oder nur geringe Auswirkungen.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Adressbuch und Kontaktdaten• Hallenbelegungsplan
2 - Hoch	<p><u>Merkmale:</u> Der Verlust oder die Zerstörung der Daten ist mit negativen Auswirkungen für die Rechte und Freiheiten der betroffenen Personen verbunden. Nur eine kurzfristige Nichtverfügbarkeit (max. 24 Stunden) ist tolerabel.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Finanzdatenbank• Mitgliederdatenbank
3 – Sehr Hoch	<p><u>Merkmale:</u> Der Verlust oder die Zerstörung der Daten ist mit erheblichen negativen Auswirkungen für die Rechte und Freiheiten der betroffenen Personen verbunden. Auch eine kurzfristige Nichtverfügbarkeit der Information ist nicht tolerabel.</p> <p><u>Beispiele:</u></p> <ul style="list-style-type: none">• Geldtransaktionen im Zahlungsverkehr• Medizinische Daten in Krankenhäusern

Abbildung 5: Schutzklassen der Verfügbarkeit