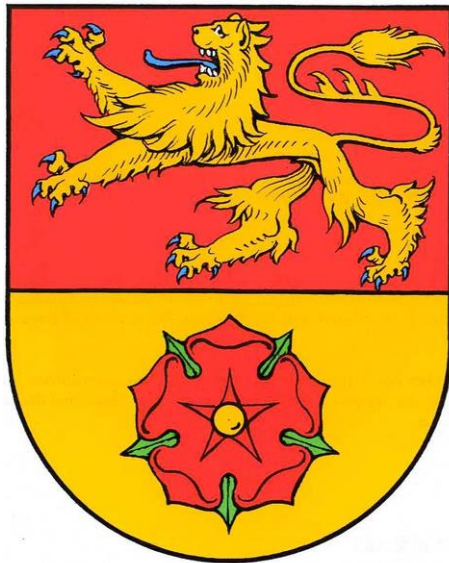

Datenschutzrichtlinie

Schützenverein Evern von 1928 e.V.



Version: 1.0

Sachstand: 23.07.2018

Freigegeben durch den Vorstand am xx.xx.xxxx

Zweck der Datenschutzrichtlinie

Die Datenschutzrichtlinie des Schützenverein Evern von 1928 e.V. regelt, ergänzend zu der Vereinssatzung, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung von personenbezogenen Daten im Schützenverein Evern.

Verantwortlichkeiten

Verantwortlich ist der Schützenverein Evern von 1928 e.V. Vertreten durch die/den 1. Vorsitzende(n).

Inhaltsverzeichnis

Zweck der Datenschutzrichtlinie	2
Verantwortlichkeiten	2
Erhebung und Verarbeitung von personenbezogenen Daten	3
Sicherung und Schutz von Daten.....	5
Datenschutz-Verpflichtung von Funktionsträgern	5

Erhebung und Verarbeitung von personenbezogenen Daten

- 1) Der Verein erhebt, verarbeitet und nutzt personenbezogene Daten seiner Mitglieder (Einzelangaben über persönliche und sachliche Verhältnisse) unter Einsatz von Datenverarbeitungsanlagen (EDV) zur Erfüllung der gemäß dieser Satzung zulässigen Zwecke und Aufgaben, beispielsweise im Rahmen der Mitgliederverwaltung.

Hierbei handelt es sich insbesondere um folgende Mitgliederdaten:

- Name und Anschrift,
 - Bankverbindung (wenn Lastschriftinzug vereinbart ist),
 - Telefonnummern (Festnetz und Mobile) sowie
 - E-Mail-Adresse,
 - Geburtsdatum,
 - Staatsangehörigkeit
 - Lizenz(en),
 - Ehrungen,
 - Funktion(en) im Verein,
 - Wettkampfergebnisse,
 - Zugehörigkeit zu Mannschaften,
 - Startrechte und ausgeübte Wettbewerbe,

 - gegebenenfalls Angaben im Hinblick auf das Waffenrecht.
- 2) Der Verein hat Versicherungen abgeschlossen oder schließt solche ab, aus denen er und / oder seine Mitglieder Leistungen beziehen können. Soweit dies zur Begründung, Durchführung oder Beendigung dieser Verträge erforderlich ist, übermittelt der Verein personenbezogene Daten seiner Mitglieder (Name, Adresse, Geburtsdatum oder Alter, Funktion(en) im Verein, etc.) an das zuständige Versicherungsunternehmen. Der Verein stellt hierbei vertraglich sicher, dass der (die) Empfänger(in) die Daten ausschließlich dem Übermittlungszweck gemäß verwendet.
 - 3) Im Zusammenhang mit seinem Sportbetrieb, sowie sonstigen satzungsgemäßen Veranstaltungen veröffentlicht der Verein personenbezogene Daten und Fotos seiner Mitglieder auf seiner Internet Präsenz bei „Evern-Online“ und übermittelt Daten und Fotos zur Veröffentlichung an Print- und Telemedien sowie elektronische Medien. Dies betrifft insbesondere Start- und Teilnehmerlisten, Mannschaftsaufstellungen, Ergebnisse, Wahlergebnisse sowie bei sportlichen oder sonstigen Veranstaltungen anwesende Vorstandsmitglieder und sonstige Funktionäre. Die Veröffentlichung / Übermittlung von Daten beschränkt sich hierbei auf Daten, die zur Organisation des Vereins und des Sportbetriebes nötig sind. Hierzu gehören, Name, Anschrift, Vereins- und Abteilungszugehörigkeit, Funktion im Verein, Alter oder Geburtsjahrgang sowie Einstufungen in Behindertenklassen.
Ein Mitglied kann jederzeit gegenüber dem Vorstand der Veröffentlichung von Einzelfotos seiner Person widersprechen. Ab Zugang des Widerspruchs unterbleibt die Veröffentlichung / Übermittlung. ~~und der Verein entfernt vorhandene Fotos von seiner Homepage.~~
 - 4) Als Mitglied des Deutschen Schützenbundes ist der Verein verpflichtet, bestimmte personenbezogene Daten über seinen Landesverband dorthin zu melden.

Im Zusammenhang mit der Organisation und der Entwicklung des Landes- bzw. Bundesverbandes, des Sportbetriebes in den entsprechenden jeweiligen übergeordneten Verbandshierarchien sowie sonstigen satzungsgemäßen Veranstaltungen der übergeordneten Verbandshierarchien übermittelt der Verein personenbezogene Daten und gegebenenfalls Fotos seiner Mitglieder an diese zur Bearbeitung und Veröffentlichung.

Übermittelt werden an **KSV Burgdorf**, der Name, Anschrift, Geburtsdatum, Wettkampfergebnisse, Startberechtigungen, Mannschaftsaufstellungen, praktizierte Wettbewerbe, Lizenzen, Vereins- und Abteilungszugehörigkeit, Informationen zur Einstufung in Behindertenklassen sowie bei Vereinsfunktionen auch Telefonnummern, Faxnummern und E-Mail-Adresse.

Ein Mitglied kann jederzeit gegenüber dem Vorstand des verarbeitenden Verbandes der Veröffentlichung von Einzelfotos seiner Person widersprechen. Ab Zugang des Widerspruchs unterbleibt die Veröffentlichung / Übermittlung und der Verein entfernt vorhandene Einzelfotos von seiner Homepage.

- 5) ~~In seiner Vereinszeitung sowie auf seiner Homepage berichtet der Verein auch über Ehrungen und Geburtstage seiner Mitglieder [ggf. andere Ereignisse mit anderen Daten]. Hierbei werden Fotos von Mitgliedern und folgende personenbezogene Mitgliederdaten veröffentlicht: Name, Vereins- sowie Abteilungszugehörigkeit und deren Dauer, Funktion im Verein und – soweit erforderlich – Alter, Geburtsjahrgang oder Geburtstag. Berichte über Ehrungen nebst Fotos darf der Verein – unter Meldung von Name, Funktion im Verein, Vereins- sowie Abteilungszugehörigkeit und deren Dauer – auch an andere Print- und Telemedien sowie elektronische Medien übermitteln. Im Hinblick auf Ehrungen und Geburtstage kann das betroffene Mitglied jederzeit gegenüber dem Vorstand der Veröffentlichung / Übermittlung von Einzelfotos sowie seiner personenbezogenen Daten allgemein oder für einzelne Ereignisse widersprechen. Der Verein informiert das Mitglied rechtzeitig über eine beabsichtigte Veröffentlichung / Übermittlung in diesem Bereich und teilt hierbei auch mit, bis zu welchem Zeitpunkt ein Widerspruch erfolgen kann. Wird der Widerspruch fristgemäß ausgeübt, unterbleibt die Veröffentlichung / Übermittlung. Anderenfalls entfernt der Verein Daten und Einzelfotos des widersprechenden Mitglieds von seiner Homepage und verzichtet auf künftige Veröffentlichungen / Übermittlungen.~~
- 6) Mitgliederlisten werden als Datei oder in gedruckter Form soweit an Vorstandsmitglieder, sonstige Funktionäre und Mitglieder herausgegeben, wie deren Funktion oder besondere Aufgabenstellung im Verein die Kenntnisnahme erfordern. Macht ein Mitglied glaubhaft, dass es die Mitgliederliste zur Wahrnehmung seiner satzungsgemäßen Rechte (z. B. Minderheitenrechte) benötigt, wird ihm eine gedruckte Kopie der Liste gegen die schriftliche Versicherung ausgehändigt, dass Namen, Adressen und sonstige Daten nicht zu anderen Zwecken Verwendung finden.
- 7) Diese Informationen werden in dem vereinseigenen EDV-System gespeichert. Jedem Vereinsmitglied wird dabei eine Mitgliedsnummer zugeordnet. Die personenbezogenen Daten werden dabei durch geeignete technische und organisatorische Maßnahmen vor der Kenntnisnahme Dritter geschützt.

Sonstige Informationen und Informationen über Nichtmitglieder werden von dem Verein intern nur verarbeitet, wenn sie zur Förderung des Vereinszweckes nützlich sind und keine Anhaltspunkte

bestehen, dass die betroffene Person ein schutzwürdiges Interesse hat, das der Verarbeitung entgegensteht.

- 8) Durch ihre Mitgliedschaft und die damit verbundene Anerkennung dieser Satzung stimmen die Mitglieder der Erhebung, Verarbeitung (Speicherung, Veränderung, Übermittlung) und Nutzung ihrer personenbezogenen Daten in dem vorgenannten Ausmaß und Umfang zu. Eine anderweitige, über die Erfüllung seiner satzungsgemäßen Aufgaben und Zwecke hinausgehende, Datenverwendung ist dem Verein nur erlaubt, sofern er aus gesetzlichen Gründen hierzu verpflichtet ist. Ein Datenverkauf ist nicht statthaft.
- 9) Jedes Mitglied hat im Rahmen der gesetzlichen Vorschriften des Bundesdatenschutzgesetzes (insbesondere §§ 34, 35) das Recht auf Auskunft über die zu seiner Person gespeicherten Daten, deren Empfänger und den Zweck der Speicherung sowie auf Berichtigung, Löschung oder Sperrung seiner Daten.

Sicherung und Schutz von Daten

- 1) Die erhobenen Daten der Vereinsmitglieder werden innerhalb einer Vereinssoftware auf einem Einzelplatz Rechner (PC) erfasst und gespeichert. Eine Sicherungskopie der Daten wird in einem „Cloud Speicher“ der Deutschen Telekom AG abgelegt.
- 2) Schieß- und Wettkampf Ergebnisse werden in Schießbüchern erfasst. Diese Schießbücher werden in verschließbaren Schränken im Schützenhaus Evern abgelegt.

Datenschutz-Verpflichtung von Funktionsträgern

Die ehrenamtlichen Funktionsträger sind mit der Aufnahme ihrer Tätigkeit im Verein über den Umgang mit personenbezogenen Daten zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO erfolgt. Der Nachweis erfolgt mit der *Verpflichtungserklärung zum Datenschutz für das Ehrenamt* im SV-Evern.

Technisch organisatorische Maßnahmen (TOM)

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Datenschutz-Grundverordnung – DSGVO

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit Erfassung, Speicherung und Übermittlung von Mitgliederdaten	Dokumenten Stand: 24.07.2018
Vereinsname und Postanschrift, E-Mail-Adresse, Telefonnummer Schützenverein Evern von 1928 e.V. Rethmarsche Str. 13, 31319 Sehnde OT Evern e-mail: vorstand@sv-evern.de	
Name und Kontaktdaten des Vorstands (Postanschrift, E-Mail-Adresse, Telefonnummer) Eleonore Bumcke. Kapellenweg 13A 31319 Sehnde OT Evern Tel.: 05138 9060 e-mail: vorstand@sv-evern.de	

2. Zwecke der Datenverarbeitung

Organisation des Vereins und des vereinsinternen Sportbetriebs sowie Übermittlung der Daten an hierarchisch übergeordnete Fach- und Sportverbände zu deren Organisation ihres Verbandes und ihrer Sportbetriebe

3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten
1	Titel, Name, Vorname
2	Anschrift
3	Geburtsdatum
4	Kommunikationsdaten (Telefon, Mobilnummer, Fax, E-Mail)
5	Bankverbindung
6	Lizenzen
7	Zusätzliche Daten zur Organisation des Sportbetriebes (Staatsangehörigkeit, Behindertenklasse, Wettkampfergebnisse, Zugehörigkeit zu Mannschaften, Startrechte, ausgeübte Wettbewerbe)
8	Ehrungen
9	Zusätzliche Daten zur Organisation des Vereins (Funktionen im Verein / Abteilungen, Zugehörigkeit zu Arbeitsgruppen)
10	Einzelfotos

4. Kategorien der betroffenen Personen

Lfd. Nr.	Lfd. Nr. von Ziffer 3	Bezeichnung der Daten
1	alle	Mitglieder
2	1,2,3,4,6,7,10	Schießsportleiter
3	1,2,3,4,6,7,10	Vorstandsmitglieder
4	1,2,4,6,9,10	Funktionsträger

5. Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

Lfd. Nr.	Lfd. Nr. von Ziffer 3	Lfd. Nr. von Ziffer 4	Empfänger	Anlass der Offenlegung
1	1,2,3,6,7,8,9,10	1,2,3,	Kreisverband	Organisation und Entwicklung des Verbandes und des Sportbetriebs
4	1,2,3,4,6,7,8,9,10	1,	Landesverband	Organisation und Entwicklung des Verbandes und des Sportbetriebs
5	1,2,3,4,6,7,8,9,10	1,	Bundesverband	Organisation und Entwicklung des Verbandes und des Sportbetriebs
7	1,2,3,6,7,8,9,10	1,	Kreissportbund	Organisation und Entwicklung des Verbandes und des Sportbetriebs

6. Falls zutreffend: Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Lfd. Nr.	Lfd. Nr. von Ziffer 4	Drittland oder internationale Organisation	Geeignete Garantien im Falle einer Übermittlung nach Art. 49 Abs. 1 DSGVO

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr. von Ziffer 3	Löschungsfrist
1	Titel, Name, Vorname für Chronik dürfen Informationen noch gespeichert bleiben
2	Mit Ausscheiden des Mitgliedes
3	Mit Ausscheiden des Mitgliedes
4	Mit Ausscheiden des Mitgliedes
5	10 Jahre nach Ausscheiden, sofern keine offenen Forderungen mehr bestehen
6	Mit Ausscheiden des Mitgliedes
7	Aus der Datenbank: Mit Ausscheiden des Mitgliedes; Aus den online verfügbaren Medien (Facebook, Internet...) ist eine Löschung aus veröffentlichten Startlisten, Ergebnislisten praktisch nicht möglich. für Chronik dürfen Informationen (z.B. Bestenlisten, Teilnahme an olympischen Spielen...) noch gespeichert bleiben
8	Mit Ausscheiden des Mitgliedes; für Chronik dürfen Informationen noch gespeichert bleiben
9	Mit Ausscheiden des Mitgliedes
10	Einzelfotos aus der Datenbank: Mit Ausscheiden des Mitgliedes; Aus den online verfügbaren Medien (Facebook, Internet...) ist dies praktisch nicht möglich.

8. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO / § 64 Absatz 3 BDSG neu

Lfd. Nr.	Maßnahme	Umsetzung der Maßnahme
1	Zugangskontrolle Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Die Einzelplatz PC befinden sich in Privaträumen der Vorstandsmitglieder und sind ausgestattet mit - Passwortschutz - Firewall - Anti-Viren-Software - Bildschirm Sperre

2	<p>Zugriffskontrolle</p> <p>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.</p>	<p><i>Die Zugriffsberechtigung ist auf die Mitglieder des Vereinsvorstands beschränkt. Ein Berechtigungskonzept mit unterschiedliche Rollen regelt den Zugriff auf benötigte Daten.</i></p>
3	<p>Transportkontrolle</p> <p>Es ist zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.</p>	<ul style="list-style-type: none"> - <i>HTTPS-Verschlüsselung</i> - <i>Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen</i> - <i>Übermittlung möglich durch: Datenbank, Applikation, Export, Schnittstellen, Druckfunktion</i>
4	<p>Übertragungskontrolle</p> <p>Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können</p>	<ul style="list-style-type: none"> - <i>Berechtigungskonzept für unterschiedliche Rollen in dem System selbst.</i> - <i>Aufzeichnung von Zugriffen auf die Datenbank durch das System.</i>
5	<p>Datenträgerkontrolle</p> <p>Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden.</p>	<ul style="list-style-type: none"> - <i>HTTPS-Verschlüsselung</i> - <i>Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen</i> - <i>Übermittlung möglich durch: Datenbank, Applikation, Export, Schnittstellen, Druckfunktion</i>
6	<p>Benutzerkontrolle</p> <p>Es ist zu verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung nutzen.</p>	<p><i>Reduzierte Zahl der Zugriffsberechtigten.</i></p> <p><i>Berechtigungskonzept für unterschiedliche Rollen in dem System selbst.</i></p> <ul style="list-style-type: none"> - <i>HTTPS-Verschlüsselung</i> - <i>Bearbeitung in nicht der Öffentlichkeit zugänglichen Büroräumen / Privaträumen</i>
7	<p>Eingabekontrolle</p> <p>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.</p>	<ul style="list-style-type: none"> - <i>My SQL-Log auf dem Server</i> - <i>Logging über Software</i>
8	<p>Wiederherstellbarkeit</p> <p>Es ist zu gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.</p>	<ul style="list-style-type: none"> - <i>Back-Up Systeme</i> - <i>Spiegelung von Festplatten</i>
9	<p>Zuverlässigkeit</p>	

	Es ist zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.	<ul style="list-style-type: none"> - <i>Regelmäßiges Aufspielen von System updates</i> - <i>Nutzung von Programmen zur Fehleranalyse</i>
10	Datenintegrität Es ist zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.	<ul style="list-style-type: none"> - <i>Regelmäßiges Aufspielen von System updates</i>
11	Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.	<ul style="list-style-type: none"> - <i>Weisung laut Vereinbarung zur Auftragsdatenverarbeitung</i>
12	Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	<p><i>Daten liegen in einem vom Verein beauftragten Rechenzentrum.</i></p> <ul style="list-style-type: none"> - <i>Backup</i> - <i>Sicherheitstests der Software werden vom Anbieter garantiert.</i>
13	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	<ul style="list-style-type: none"> - <i>Logische Trennung der Daten über Tabellen und Mandate</i>

Erläuterungen

Allgemeines

Das Verzeichnis von Verarbeitungstätigkeiten ist nach Art. 30 Abs. 1 DSGVO vom Verantwortlichen zu führen. Diese Vorschrift lautet wie folgt:

„(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;*
- b) die Zwecke der Verarbeitung;*
- c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;*
- d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;*
- e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;*
- f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;*
- g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.“*

Zu Nr. 1 (Allgemeine Angaben)

Die Bezeichnung der Verarbeitungstätigkeit soll allgemeinverständlich sein. Beispiele: "Personaldaten", „Melderegister der Gemeinde ...“. Für Außenstehende unverständliche Abkürzungen sind zu vermeiden.

Zu Nr. 3 (Kategorien der personenbezogenen Daten)

Unter Kategorien sind aussagefähige Oberbegriffe zu verstehen, z.B. „Name und Vornamen“, „Anschrift“, „Staatsangehörigkeit“. Angaben rein technischer Art (z.B. Feldnummern, Schlüsselnummern usw.) sind nicht erforderlich.

Zu Nr. 6 (Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation)

Im Falle einer Übermittlung an ein Drittland oder eine internationale Organisation nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO sind die geeigneten Garantien, in Bezug auf den Schutz personenbezogener Daten in Spalte 3 festzuhalten - soweit erforderlich ist dazu auf ergänzende Dokumente zu verweisen.

Zu Nr. 8 (Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO / § 64 Absatz 3 BDSG neu)

Soweit möglich sind die technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO hier zu beschreiben. Diese Vorschrift lautet wie folgt:

„(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“*