1. **Rechtsgrundlagen des Datenschutzes**

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in Art. 6 Abs. 1 DS-GVO geregelt. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig,

* wenn eine Einwilligung der betroffenen Person vorliegt (siehe Kapitel „Einwilligung“),
* zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,
* zur Erfüllung einer rechtlichen Verpflichtung (z. B. Aufbewahrungspflichten),
* zum Schutze lebenswichtiger Interessen (z. B. Epidemien, Naturkatastrophen),
* zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt (z. B. Behördenhandlungen, Rettungsdienst) oder
* auf Grund einer Interessenabwägung erforderlich ist (z. B. Werbung bei den Mitgliedern).

Die Datenverarbeitung ist rechtmäßig, wenn einer der genannten Tatbestände vorliegt.

Im Grundsatz bleibt daher alles verboten, was nicht ausdrücklich erlaubt ist.

1. **Grundsätze des Datenschutzes**

Die Datenschutzgrundsätze sind in Art. 5 Abs. 1 DSGVO beschrieben und für die Datenverarbeitung verbindlich. Die Nichtbeachtung dieser Grundsätze ist gem. Art. 83 DSGVO mit Bußgeld bedroht. Bei Zweifelsfragen zur Interpretation der Grundsätze und deren Anwendung ist der Datenschutzbeauftragte zu konsultieren. Für den Umgang mit personenbezogenen Daten werden nachfolgende Grundsätze besonders beachtet.

* **Verarbeitung nach Treu und Glauben (fairer Umgang)**

Die [personenbezogenen Daten](https://eu-datenschutz-grundverordnung.net/personenbezogene-daten/) werden nur so [verarbeitet](https://eu-datenschutz-grundverordnung.net/verarbeitung/), wie es bei der Erhebung angegeben wurde und nicht anders. Die Verarbeitung darf nur in dem Umfang gemacht werden, auf welchen die [Person](https://eu-datenschutz-grundverordnung.net/betroffener_datensubjekt/) vertrauen hat dürfen.

* **Transparenz**

Der Grundsatz der Transparenz verlangt, dass jeder Betroffene wissen soll, wer welche Daten für welche Zwecke über ihn erhebt, speichert und verarbeitet und übermittelt und wie lange die Daten gespeichert werden und dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Natürliche Personen sind über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Datenverarbeitung zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. Hier sind die im Einzelnen geregelten Informationspflichten zu beachten.

* **Zweckbindung**

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Eine Verarbeitung oder Nutzung von personenbezogenen Daten für andere als den Betroffenen im Zusammenhang mit der Datenerhebung kommunizierten Zwecke ist nur unter den gesetzlich festgelegten Bedingungen (Art. 6 Abs. 5 DSGVO) und ansonsten nur mit Einwilligung der Betroffenen zulässig. Sollen erhobene Daten auch für einen anderen als den der Erhebung zugrundeliegenden Zweck verwendet werden, z. B. zu Zwecken der Werbung oder für Datenübermittlungen, sollte vorher der Datenschutzkoordinator/in konsultiert werden.

* **Datenminimierung**

Art und Umfang der Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dies schließt eine Begrenzung der Speicherfrist auf das erforderliche Mindestmaß ein. Hier ist darauf zu achten, dass nur diejenigen Daten von den Betroffenen erhoben werden, die für den jeweiligen Verarbeitungszweck auch wirklich erforderlich sind. Darüberhinausgehende Erhebungen und Verarbeitungen sind unzulässig.

* **Richtigkeit**

Personenbezogene Daten müssen im Hinblick auf die Zwecke ihrer Verarbeitung sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Verarbeitung unrichtiger Daten ist zu vermeiden. Unrichtige Daten sind unverzüglich zu berichtigen.

* **Nachvollziehbarkeit, Revisionsfähigkeit**

Die Verarbeitung und Veränderung von personenbezogenen Daten müssen nachvollziehbar und, soweit erforderlich, in geeigneter Weise dokumentiert und überprüfbar sein. Einzelheiten, insbesondere Protokollierungen, sind mit dem Datenschutzbeauftragten abzustimmen.

* **Speicherbegrenzung**

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie erhoben worden sind, erforderlich ist. Um sicherzustellen, dass die Daten nicht länger als nötig gespeichert werden, sind Fristen für ihre Löschung oder regelmäßige Überprüfung vorzusehen und die Daten regelmäßig zu löschen bzw. zu vernichten. Die Aufbewahrungsfristen sind festzulegen und die Löschung bzw. Vernichtung der Daten ist zu veranlassen bzw. zu überwachen.

* **Integrität und Vertraulichkeit**

Der Grundsatz der Integrität und Vertraulichkeit verlangt einen angemessenen Schutz und eine angemessene Sicherheit der personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Bei der Verarbeitung der personenbezogenen Daten ist durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten.

* **Rechenschaftspflicht**

Der Grundsatz der Rechenschaftspflicht verlangt, dass die Einhaltung der o. g. Datenschutzgrundsätze nachgewiesen werden kann. Zur Erfüllung dieser Rechenschaftspflicht ist ein in sich stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet. Auf der Grundlage der darüber geführten Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich.