

ITSCON GmbH & Co KG
Glognerweg 17a
A-4030 Linz

Tel: +43 / 676 / 6047 072
Mail: office@itscon.at

<http://www.itscon.at>

D
S
G
V
O

**Datenschutz**

**Leitfaden für Ortsgruppen**

**Naturfreunde Österreich**

**Viktoriagasse 6**

**1150 Wien**

**Inhaltsverzeichnis**

[1. Allgemeine Informationen 3](#_Toc513808009)

[2. Checkliste 4](#_Toc513808010)

[3. Datenschutzrichtlinie 5](#_Toc513808011)

[4. Newsletter 5](#_Toc513808012)

[5. Paralleldatenbanken 6](#_Toc513808013)

[6. Informationspflicht 7](#_Toc513808014)

[7. Datenweitergabe 8](#_Toc513808015)

[8. Erstellung und Verwendung von Fotos 9](#_Toc513808016)

[9. DSGVO Prozesse in der Bundesorganisation 10](#_Toc513808017)

[9.1. Auskunft, Löschung 10](#_Toc513808018)

[9.2. Berichtigungsrecht 11](#_Toc513808019)

[9.3. Datenpannen 11](#_Toc513808020)

[10. DSGVO Prozesse in Ortsgruppen und Landesorg. 11](#_Toc513808021)

[10.1. Datenpannen](#_Toc513808022) 11

[11. Webseiten und E-Mailadressen 12](#_Toc513808024)

[11.1. Webseiten 12](#_Toc513808025)

[11.2. E-Mailadressen 12](#_Toc513808026)

[12. IT-Sicherheit 12](#_Toc513808027)

Allgemeine Informationen

Aufgrund der neuen Anforderungen bezüglich Datenschutz durch die DSGVO ab 25. Mai 2018 sind weitreichende Änderungen beim Umgang mit personenbezogenen Daten zu beachten.

Die Naturfreunde Österreich Bundesorganisation betreibt ein Datenschutz-Managementsystem, wodurch die zentrale Datenhaltung für die Landesorganisationen und Ortsgruppen weitestgehend abgedeckt ist.

Alle von der Bundesorganisation zur Verfügung gestellten Programme und Webseiten sind durch die Bundesorganisation datenschutzrechtlich behandelt.

Da jede Ortsgruppe und Landesorganisation als eigenständiger Verein bzw. Organisation aufgebaut ist, muss sich hier jeder Verein selbst um die Einhaltung der Datenschutzbestimmungen kümmern. Dies betrifft auch jede Datenerweiterung. Wenn die Ortsgruppe weitere Daten erhebt oder auf Webseiten darstellt, so sind diese durch die Ortsgruppen datenschutzrechtlich selbst zu vertreten.

Die Bundesorganisation unterstützt hierbei durch Vorlagen, bei zentralen Dokumenten und Prozessen (z.B. Mitgliederverwaltung).

**Das vorliegende Dokument stellt die wichtigsten Informationen für Ortgruppen und Landesorganisationen zusammen. Es ersetzt in keinem Fall die genaue Analyse der DSGVO Anforderungen oder Einarbeitungen im jeweiligen Verein!**

Diese Unterlage wurde in Zusammenarbeit mit der Naturfreunde Österreich Bundesorganisation und der Fa. ITSCON GmbH & Co KG erstellt.

Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der ITSCON GmbH & Co KG oder der Naturfreunde Österreich Bundesorganisation ist ausgeschlossen. Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter!

# Checkliste

Um die Datenschutzanforderungen jeder Ortsgruppe zu prüfen und sicherzustellen, empfehlen wir anhand folgender Checkliste vorzugehen:

1. **Feststellung des IST-Zustands**
Prüfen Sie anhand des vorliegenden Dokuments, welche Bereiche aus dem Datenschutz für Sie notwendig sind und noch nicht durch die Bundesorganisation abgedeckt wurden.
2. **Aktualisieren Sie Ihre Newsletter**Prüfen Sie, ob Sie Newsletter auch an **NICHT-MITGLIEDER** versenden (vgl. Kapitel 4). Falls ja, brauchen Sie ab 25. Mai 2018 eine Einwilligung nach neuem Muster (siehe Datenschutz-Grundlagen). Diese Einwilligung sollte ehestmöglich eingeholt werden.
3. **Prüfen Sie welche weiteren Daten Sie erheben**Wenn Sie mehr personenbezogene Daten als in der Mitgliederverwaltung vorhanden, erheben oder auch Daten von Nicht-Mitgliedern haben, so müssen Sie das Verfahrensverzeichnis für Ihre Zwecke erweitern (vgl. Kapitel 5). Verarbeiten sie **NUR** die zentralen Mitgliederdaten, über die Mitgliederverwaltung, sind **keine Anpassungen notwendig.**
4. **Prüfen Sie ob alle Datenweitergaben den neuen Anforderungen entsprechen**Die Weitergabe von personenbezogenen Daten darf nur mehr für notwendige und dokumentierte Bereiche erfolgen. Jede weitere Datenweiterleitung benötigt die Einwilligung der Mitglieder (vgl. Kapitel 7).
5. **Löschen Sie nicht mehr benötigte Daten**Da personenbezogene Daten nur noch verwendet werden dürfen, wenn der damit verbundene Zweck noch gilt, sind viele Daten nicht mehr notwendig und somit zu löschen. Dazu zählen z.B. alte Bibliothekslisten oder Teilnehmerlisten von länger zurückliegenden Kursen.
6. **Stellen Sie die Betroffenen-Prozesse sicher**Definieren Sie einen internen Ansprechpartner (OG-Vorsitzender, Schriftführer oder eigener Datenschutzkoordinator, etc.) für alle Belange des Datenschutzes. Dieser ist auch dafür zuständig, dass alle Informationen von und zur Bundesorganisation fließen.
7. **Schulen Sie Ihre Funktionäre und Kursleiter**Informieren Sie Ihre Funktionäre und Kursleiter, welche Änderungen zur jetzigen Praxis in der Ortsgruppe notwendig sind. Es ist wichtig, dass diese Personen die neuen Regeln kennen und auch anwenden.
8. **Prüfen Sie die IT-Sicherheit**Stellen Sie sicher, dass alle Anwendungen auf ausreichend geschützten Computern erfolgen (vgl. Kapitel 12).

# Datenschutzrichtlinie & Beschluss im OG-Vorstand

Die Naturfreunde Österreich stellen eine Datenschutzrichtlinie für alle Ortsgruppen und Landesorganisationen zur Verfügung, in der u.a. geregelt wird, wie mit den Betroffenenrechten umzugehen ist.

Auch ersichtlich unter: <http://www.naturfreunde.at/datenschutz>

Weiters werden Funktionären, Mitgliedern und externen Unterstützern Richtlinien zur Einhaltung bei der Datenverarbeitung zur Verfügung gestellt. Durch einen Beschluss im jeweiligen Vorstand gelten diese dann für alle.

Durch die Verabschiedung dieser Richtlinie (z.B. bei der nächsten Vorstandssitzung) werden die für die DSGVO notwendigen Vertraulichkeitsvereinbarungen für alle Funktionäre und Mitglieder bindend.

# Newsletter

Die Naturfreunde informieren viele Mitglieder und Nicht-Mitglieder über Newsletter oder ähnliche Medien. Die nachfolgenden Regelungen gelten für Mails mit mehr als 50 Empfängern.

**Mails an Mitglieder und Funktionäre dürfen weiterhin wie bisher durchgeführt werden.**

Alle anderen müssen eine Einwilligung erteilt haben. Dazu zählt unter anderem:

* Double-Opt-In (Anmeldung, Mail mit Link zur Bestätigung, erst dann Newsletter-Zusendung)
* Aktives Ankreuzen auf Formularen

Ältere Einwilligungen, z.B. Anmeldungen ohne Double-Opt-In sind leider nicht mehr gültig!

Grundsätzlich gilt bei Newslettern:

* Es muss der Verantwortliche klar ersichtlich sein
* Abmeldefunktion muss bei jeder Aussendung vorhanden sein (z.B. kann der Hinweis in der Fußzeile eingebettet sein)
* Die Empfänger dürfen sich gegenseitig nicht sehen (bei manuellem Versand nur über BCC Feld!)

Die Newsletter von der Naturfreunde-Webseite mit allen Unterportalen erfüllen diese Anforderungen. Bei eigenen Newsletter Tools oder eigen verwalteten Webseiten sind diese Anforderungen selbst zu erfüllen.

Weitere Details dazu:

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html>

# Paralleldatenbanken zusätzlich zur zentralen Mitgliederdatenbank

Wenn personenbezogene Daten abseits der zentralen Mitgliederverwaltung gespeichert werden, entweder in Paralleldatenbanken oder Excel-Tabellen, so sind weitere Anforderungen zu prüfen.

Grundsätzlich ist eine Speicherung von zentralen Mitgliederdaten in anderen Datenbanken oder Exceltabellen erlaubt. Durch die Betroffenenrechte sind jedoch auch für diese Systeme folgende Anforderungen sicherzustellen:

* Bei Auskunftsbegehren sind diese Daten ebenfalls einzufügen
* Bei Löschungen (von Mitgliedern oder Ablauf der Speicherfristen) sind diese ebenfalls hier zu löschen
* Richtigstellungen müssen ebenfalls nachgezogen werden
* Verarbeitung auf „ausreichend sicheren IT-Systemen“
* Bei externer Verarbeitung sind Auftragsdatenverarbeitungsverträge abzuschließen

Für die Einhaltung dieser Grundsätze ist der jeweilige Betreiber selbst verantwortlich!

**Wenn andere Daten als in der zentralen Mitgliederverwaltung gespeichert werden, so ist ein eigenes Verarbeitungsverzeichnis zu führen!**

Die Vorlage des zentralen Verarbeitungsverzeichnisses der Bundesorganisation erhalten Sie bei Günter Neunteufel.

Alte Kurslisten, Bibliothekslisten, usw. sind ehestmöglich zu löschen, sofern diese nicht mehr benötigt werden. Diese dürfen nur maximal 7 Jahren aufbewahrt werden, außer sie sind historisch für die Dokumentation, beispielsweise einer Ortsgruppe, relevant.

# Informationspflicht

Die DSGVO verpflichtet jeden Verantwortlichen zur Einhaltung vieler Informationspflichten. Vereinfacht kann gesagt werden, dass jedes Mitglied jederzeit Kenntniss über die verarbeiteten Daten haben muss.

Diesbezüglich ist für die Naturfreunde folgendes sehr wesentlich:

* Welche Daten werden verarbeitet
	+ Daten aus dem normalen Vereinsleben (Name, Geburtsdatum, event. Bankverbindung, Beitritt, Zahlung, usw.) sind bereits durch die Information der Bundesorganisation abgedeckt

## Weitere Informationspflicht bei Abwicklung von Veranstaltungen, Kursen, Reisen, etc.

* Wozu werden diese Daten verarbeitet?
* Welche Rechtsgrundlage wird angewandt?
	+ Gesetzliche Bestimmung
	+ Vertrag (z.B. Mitgliederverwaltung aufgrund Beitritt, Anmeldung an Kursen oder Veranstaltungen)
	+ Einwilligungserklärung
* Die Dauer der Datenspeicherung?
	+ Falls diese von den Standardwerten abweicht
* Wer ist Empfänger der Daten?
	+ Z.B. Kursleiter, Hotel, Busunternehmen, Bergbahnen, usw.
* Findet Übermittlung in ein NICHT-EU-Land statt?
* Wenn Daten nicht vom Mitglied selbst kommen, muss auch die Quelle übermittelt werden

Eine Information kann entfallen, wenn dem Mitglied bereits alles bekannt ist!

Ein paar Beispiele:

* **Es muss jedem bekannt sein, dass er Mitglied der Naturfreunde ist (KEINE Ausnahmen!)**
* Wenn die Anmeldung nicht selbst erfolgt (z.B. Lehrer, Schikurs über Kindergarten oder Ehepartner), so sind die Betroffenen darüber zu informieren oder mit dem Datenübermittler (nachweislich) muss vereinbart werden, dass er sich um die Information an die Betroffenen (Mitglieder) kümmert.
* Versand einer Teilnehmerliste an alle Teilnehmer ist erst NACH deren Einwilligung erlaubt

# Datenweitergabe

Jede Datenweitergabe ist mit den Mitgliedern abzustimmen. Ausgenommen sind Auftragsdatenverarbeiter (Firmen die personalisieren, wie Druckereien, etc.). Mit diesen muss ein gesonderter Datenverarbeitungsvertrag abgeschlossen werden. Das diesbezügliche Muster finden Sie in der Anlage und im Intranet unter Datenschutz. <http://intranet.naturfreunde.at/datenschutz>

Wenn die Datenweitergabe bereits in der Datenschutzrichtlinie unter <http://www.naturfreunde.at/datenschutz> definiert ist (z.B. Mitgliederverwaltung), ist keine extra Information mehr notwendig.

Achtung: Bereits eine Kurs-, Reise- oder Übernachtungsabwicklung kann eine Weiterleitung der Daten sein, wenn Externe (also **KEINE** Instruktoren, Übungsleiter oder Funktionäre der Naturfreunde) mit der Bearbeitung betraut sind (z.B. Hotels, Busunternehmen, usw.).

Bitte informieren Sie Ihre Mitglieder darüber, welche Unternehmen ihre Daten übermittelt bekommen. Dies kann gleich bei der Ausschreibung/Anmeldung eines gemeinsamen Hotelaufenthalts erfolgen.

Beispiel 1: „Die gemeinsame Übernachtung wird im Hotel XY erfolgen. Die Meldedaten zur Zimmereinteilung werden übermittelt“.

Es muss jedem Teilnehmer immer bekannt sein, wer seine Daten und für welchen Zweck erhalten hat.

Beispiel 2: In einer Ausschreibung für eine Wanderung ist Treffpunkt X angeführt. Zwecks Bildung von Fahrgemeinschaften müssen bei der Anmeldung Einverständniserklärungen aller Teilnehmer unterschrieben werden, damit ihre Kontaktdaten weitergegeben werden dürfen.

# Erstellung und Verwendung von Fotos

Wenn auf Fotos Personen erkannt werden können (auch im Hintergrund), so stellen diese Fotos ebenfalls personenbezogene Daten dar. Die Rechtslage bei Fotos ist leider nicht einfach anzuwenden, daher sind hier neue Grundregeln einzuhalten.

Normalerweise kann man hier weder Gesetze noch Verträge als Rechtsgrundlage anführen, somit bleibt zumeist nur die Einwilligungserklärung. Diese müssen den Anforderungen aus Kapitel 2.4 entsprechen (siehe Beilage oder unter <http://intranet.naturfreunde.at/datenschutz/formulare-zur-dsgv/>

Bitte regeln Sie vor Erstellung von Fotos gleich deren Verwendungszweck und vereinbaren Sie mit den abgebildeten Personen, was Sie damit machen dürfen.

Beispieltext für die Erstellung von eigenen Einverständniserklärungen: „Ich willige dazu ein, dass bei diesem Kurs Fotos erstellt werden und diese auf der Vereinswebsite und in der Vereinszeitung veröffentlicht werden. Ein Widerruf ist jederzeit möglich, bitte informieren Sie dazu den Kursleiter.“

Anmerkung: Aufgrund der schwierigen Einwilligungsverwaltung bei größeren Veranstaltungen sind einige Juristen der Meinung, dass eine „sehr offensichtliche Information über die Fotoerstellung mit einer einfachen Widerspruchsmöglichkeit“ ausreicht. Ich empfehle jedoch, speziell bei kleineren Kursen dies mittels Formular zu regeln. Speziell die Fotoverwendung ist hier ebenfalls zu berücksichtigen.

Wir empfehlen daher folgende Grundregeln einzuhalten, um möglichst viele Einwilligungen zu erhalten:

* Verzicht auf Fotos, wenn unbeteiligte Personen abgebildet würden
* Bereits bei Anmeldungen darauf hinweisen, dass fotografiert wird
* Bei größeren Veranstaltungen einen gut lesbaren Aushang aufstellen
„Hier wird fotografiert. Sollten Sie nicht fotografiert werden wollen, so sagen Sie dies direkt dem Fotografen oder dem Veranstalter“
* Bei Kursen mit kleineren Gruppen diese bei Kursbeginn fragen, ob auch alle fotografiert werden dürfen
* Bei wenigen Personen bzw. Einzelfotos immer direkt mit der Person reden

**Achtung: Diese Informationen müssen gut lesbar sein und dürfen nicht in „AGBs versteckt werden“!**

# DSGVO Prozesse in der Bundesorganisation

Wenn Mitglieder ihre Rechte bei der Bundesorganisation anfordern (z.B. Auskunft oder Löschung), so ist eine Mitwirkung bei der jeweiligen Ortsgruppe und Landesorganisation notwendig, um wirklich alle personenbezogenen Daten zu erhalten.

## Auskunft, Löschung

Bei einem Auskunfts- oder Löschbegehren wird die Anforderung geprüft und soweit gültig bearbeitet. Um alle (auch dezentralen) Daten zu erreichen, ist eine gemeinsame Bearbeitung unter Einbeziehung des Datenschutzkoordinators Günter Neunteufel in der Bundesorganisation notwendig.

Dazu wird die Bundesorganisation Kontakt mit den jeweiligen Verantwortlichen (z.B. Landesgeschäftsführer oder Ortsgruppen-Vorsitzender) aufnehmen, um die Prozesse zu koordinieren.

## Berichtigungsrecht

Änderungen von z.B. Adressen werden in der zentralen Mitgliederverwaltung durchgeführt. Dazu bekommen die betroffenen Ortsgruppen und Landesorganisationen regelmäßig Änderungs- bzw. Löschlisten.

Bitte diese Änderungen und Löschungen auch in allen dezentralen Datenbanken und Tabellen durchführen. Es ist hier **unbedingt notwendig**, dass hier korrekte Daten verwendet werden. In diesem Zusammenhang sind auch Strafen durch die Datenschutzbehörde nicht auszuschließen.

## Datenpannen

Bei Entdeckung von relevanten Datenpannen wird die Bundesorganisation neben der Behörde auch die jeweils betroffenen Landesorganisationen und Ortsgruppen informieren, um den Informationsfluss aufrecht zu erhalten.

# DSGVO Prozesse in Ortsgruppen und Landesorganisationen

Wenn sich Mitglieder in den Ortsgruppen oder Landesorganisationen melden, um ihre Betroffenenrechte geltend zu machen, so ist auch der Datenschutzkoordinator Günter Neunteufel zu kontaktieren.

Die Bundesorganisation kann Sie bei der Abwicklung der Prozesse unterstützen. Für die Durchführung ist jedoch die jeweilige Ortsgruppe selbst verantwortlich.

Bitte weisen Sie unbedingt darauf hin, welcher Verantwortliche, also welche Ortsgruppe, hier den Prozess bearbeitet hat. Nur so ist es für das Mitglied klar, dass die Anfrage auch nur diesen Bereich abdeckt.

## Datenpannen

Wenn es zu Datenpannen kommt, ist eine Meldung an die Bundesorganisation innerhalb von 72 Stunden **UNBEDINGT** notwendig, damit wir gemeinsam die Auswirkungen für die Betroffenen bewerten und verringern können. Im Bedarfsfall entscheidet die Bundesorganisation gemeinsam mit dem Datenschutzbeauftragten, ob eine Meldung an die Behörde notwendig ist.

# Webseiten und E-Mailadressen

Wenn Ortsgruppen eigene Webseiten betreiben, die nicht am Naturfreunde-Portal liegen, so gilt es auch hier die Einhaltung der DSGVO sicherzustellen.

## Webseiten

Die DSGVO sieht vor, dass zumindest folgende Anforderungen abgedeckt sind:

* Information über Cookies (falls diese verwendet werden)
* Datenschutzrichtlinie über die Verwendung und Weiterleitung von personenbezogenen Daten. Dazu gibt es fertige Generatoren im Internet, z.B.: <https://www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator/>
* Wenn personenbezogene Daten übertragen werden (z.B. Kontaktformular oder Webshop) ist HTTPS (SSL) zu verwenden

## E-Mailadressen

Bei der Verwendung von privaten E-Mailadressen zur Vereinstätigkeit ist zu beachten, dass die Daten dabei an den E-Mailprovider übertragen werden.

Weiters finanzieren sich Gratis-E-Mailadressen ja dadurch, dass die E-Mails durchsucht und die gefundenen Daten für deren Zwecke verwendet werden können. Dies stellt bereits eine Weitergabe der Daten dar.

In der Datenschutzrichtlinie weisen wir zwar darauf hin, dass E-Mails auch über private E-Mailadressen von Funktionären oder Kursleitern versendet werden können, es sollte aber trotzdem weitestgehend vermieden werden.

# IT-Sicherheit

Jedes Mitglied darf davon ausgehen, dass die überlassenen Daten auch ausreichend gesichert werden. Für die zentralen Systeme (z.B. Mitgliederverwaltung) führt die Bundesorganisation die notwendigen Maßnahmen, bei allen eigenen Verarbeitungen ist die jeweilige Ortsgruppe bzw. Landesorganisation selbst dafür zuständig.

Die wesentlichen Anforderungen:

* Kein Windows XP oder älter (bei Servern kein Windows Server 2003)
* Windows Updates müssen aktiviert sein
* Virenscanner muss vorhanden und aktuell sein
* Kennwörter müssen verwendet werden
	+ Mindestes 8 Stellen (gerne auch viel länger)
	+ Klein-Groß-Zahlen sollten vorkommen
	+ Kennwörter sind regelmäßig zu ändern
	+ Kennwörter nicht oder nur im notwendigen Umfang weitergeben
	+ Unterschiedliche Kennwörter für unterschiedliche Systeme
* Backup der Daten
* Mobile Datenträger (externe HDDs, USB-Sticks)
	+ Datenträger sind DatenTRÄGER kein DatenSPEICHER!
	+ Sichere Verwahrung (damit kein Verlust passieren kann)
	+ Wenn möglich Verschlüsselung aktiveren
* Zugangsschutz und örtliche Sicherheit
	+ Kein IT-Gerät unbewacht in öffentlichen Räumen oder offen in Fahrzeugen
* Tablets und Mobiltelefone
	+ PIN muss aktiviert sein
	+ Fernlöschmöglichkeit ist zu aktiveren
	+ Updates aktiveren (somit keine alten Geräte für Vereinszwecke verwenden)
	+ So wenig wie möglich Daten darauf speichern (Achtung: alte Fotos, usw.)