

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**

**Allgemeine Information für Ortsgruppen**

**Naturfreunde Österreich**

**Viktoriagasse 6**

**1150 Wien**

**Inhaltsverzeichnis**

[1. Allgemeine Informationen 3](#_Toc513799702)

[2. Grundanforderungen DSGVO 4](#_Toc513799703)

[3. Schützenwerte Daten 4](#_Toc513799704)

[4. Beteiligte Parteien 5](#_Toc513799705)

[4.1. Verantwortlicher 5](#_Toc513799706)

[4.2. Betroffener 5](#_Toc513799707)

[4.3. Empfänger 5](#_Toc513799708)

[4.4. Auftragsdatenverarbeiter 5](#_Toc513799709)

[4.5. Zusammenhang 6](#_Toc513799710)

[5. Verarbeitungsgrundsätze 7](#_Toc513799711)

[6. Einwilligungserklärungen 8](#_Toc513799712)

[7. Betroffenenrechte 9](#_Toc513799713)

[7.1. Auskunftsrecht 9](#_Toc513799714)

[7.2. Löschrecht 10](#_Toc513799715)

[7.3. Informationsrecht 10](#_Toc513799716)

[7.4. Weitere Rechte 11](#_Toc513799717)

[8. Datenpannen 11](#_Toc513799718)

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 Landes-organisationen und Ortsgruppen weitestgehend abgedeckt ist.

Da jede Ortsgruppe und Landesorganisation als eigenständiger Verein bzw. Organisation aufgebaut ist, muss sich hier jeder Verein selbst um die Einhaltung der Datenschutzbestimmungen kümmern.

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!

# Grundanforderungen DSGVO

Die DSGVO gilt für alle Unternehmen, Vereine, NGO‘s, usw. wenn diese Daten von Europäischen Bürgern verarbeitet werden (ab dem 25. Mai 2018 gültig). Dabei müssen ab diesem Datum auch alle bereits vorhandenen Daten den neuen Anforderungen entsprechen.

# Schützenswerte Daten

Zu schützen sind alle „personenbezogenen Daten von natürlichen Personen“, d.h. von Menschen:

* Direkte Daten, wie z.B. Name, Adresse, E-Mailadresse, Geburtsdatum
* Indirekte Daten, also alle Daten welche Sie oder ein Dritter auf eine natürliche Person zurückrechnen können:
	+ KFZ-Kennzeichen (die Polizei kann den Halter ermitteln)
	+ IP-Adressen (der Provider kann den Anschluss identifizieren)
	+ Kundenummern (das jeweilige Unternehmen kann daraus eine Person machen)
* Sensible Daten (Daten mit besonderem Schutzbedarf)
	+ „Daten aus denen die **rassische und ethnische Herkunft**, **politische Meinungen**, **religiöse oder weltanschauliche Über-zeugungen** oder die **Gewerkschaftszugehörigkeit** hervorgehen, sowie die Verarbeitung von **genetischen Daten, biometrischen Daten** zur eindeutigen Identifizierung, **Gesundheitsdaten** oder **Daten zum Sexualleben** oder der **sexuellen Orientierung** einer natürlichen Person.“
	+ Z.B. Gesundheitsdaten, Krankmeldungen
	+ Sozialversicherungsnummer
	+ Teilweise Postings auf Facebook (mit politischem Bezug)
	+ Allergieinformation von Personen
	+ Fingerabdrucksensor

# Beteiligte Parteien

Die DSGVO kennt folgende an der Datenverarbeitung beteiligte Parteien. Detail am Rande: Es wird nicht geklärt, wer „Besitzer“ der jeweiligen Daten ist. Für die Verarbeitung ist dies jedoch auch nicht notwendig.

## Verantwortlicher

Als Verantwortlicher wird jene Organisation, Firma oder Verein bezeichnet, welcher die Datenverarbeitung durchführt. In unserem Fall also der jeweilige Verein der Naturfreunde.

Aufgrund der Datenschutzrichtlinie der Naturfreunde Österreich dürfen personen-bezogene Daten innerhalb der jeweiligen Vereine gemeinsam verarbeitet werden, wenn diese Verarbeitung notwendig ist. Da die Bundesorganisation die zentrale Mitgliederverwaltung bereitstellt, ist dies in unserem Fall notwendig.

## Betroffener

Als Betroffener wird jene Person bezeichnet, deren Daten verarbeitet werden. Betroffene können somit Kunden, Mitglieder, Mitarbeiter, Funktionäre oder auch Familienmitglieder sein.

## Empfänger

Wenn der Verantwortliche personenbezogene Daten weiterleiten möchte, so spricht man von Empfängern.

Hier ist es wichtig, dass jedem Betroffenen die Empfänger der Daten bekannt gemacht werden oder schon bekannt sind.

## Auftragsdatenverarbeiter

Auftragsdatenverarbeiter sind Empfänger, welche durch einen gemeinsamen Vertrag mit dem Verantwortlichen verbunden werden. Somit dürfen hier Daten weitergegeben werden, ohne dass dies dem Betroffenen sofort mitgeteilt werden muss.

Unter Auftragsdatenverarbeiter fallen z.B.:

* Steuerberater und Lohnverrechner
* IT-Dienstleister, Cloud-Anbieter
* Newsletter-Versender, Druckereien
* usw.

Hier ist wichtig, dass der Auftragsdatenverarbeiter keine Datenverarbeitung für den eigenen Nutzen durchführen darf und somit an den Auftrag des Ver-antwortlichen gebunden ist. Der Auftragsdatenverarbeiter, z.B. Druckerei, darf mit den erhaltenen Daten somit nur dies tun, wofür der Auftrag erteilt wurde.

Somit fallen viele Cloud-Anbieter (z.B. Dropbox) hier heraus, da diese die Daten für eigene Zwecke verarbeiten möchten und keine diesbezüglichen Auftrags-datenverarbeitungsverträge eingehen (möchten).

## Zusammenhang

Zusammenfassend kann man sagen, dass der Verantwortliche Daten von Betroffenen verarbeiten darf, wenn er die Verarbeitungsgrundsätze einhält und den Betroffenen ihre Rechte einräumt.

Die Weitergabe der Daten an Empfänger ist den jeweiligen Betroffenen mitzuteilen, außer es handelt sich um einen Auftragsdatenverarbeiter.



# Verarbeitungsgrundsätze

Grundsätzlich ist jede Datenverarbeitung verboten, außer es werden folgende Grundsätze eingehalten:

* Rechtmäßigkeit der Verarbeitung
	+ Bei nicht sensiblen Daten (vgl. 3) gibt es u.a. folgende Tatbestände für eine Erlaubnis:
		- Gesetzliche Verpflichtung (z.B. Rechnungen, usw.)
		- Vertrag mit dem Betroffenen (z.B. Beitritt zum Verein)
		- Einwilligung des Betroffenen
		- Interessensabwägung
	+ Bei sensiblen Daten (z.B. Gesundheitsdaten) gelten folgende Grundsätze:
		- Ausdrückliche Einwilligung
		- Im Sinne des Sozial-, Sicherheits- und Arbeitsgesetzes
* Zweckbindung
	+ Daten dürfen nur für den vereinbarten Zweck verarbeitet werden
* Datenminimierung, Löschung
	+ Nicht mehr notwendige Daten müssen gelöscht werden
	+ Wenn z.B. der Zweck wegfällt (Austritt des Mitglieds, Rechnungen nach 7 Jahren, usw.) sind die Daten zu löschen
	+ Wenn eine Einwilligung zurückgezogen wird, sind die betroffenen Daten ebenfalls zu löschen
* Richtigkeit
	+ Wenn Kenntnis über zu ändernde Daten erlangt wird, sind diese richtig zu stellen.
	+ So muss z.B. bei Adressänderung eines Mitglieds die neue Adresse verwendet werden (soweit diese Änderung auch bekannt ist oder bekannt gegeben wurde). Dies betrifft auch alle weiteren Speicher-orte und parallele Applikationen.
* Sicherheit
	+ Der Betroffene darf sich darauf verlassen, dass die Daten auch „sicher“ verwahrt werden.
	+ Dies ist immer im Bezug auf die „Brisanz“ der Daten und Möglich-keiten des Verantwortlichen zu sehen.

# Einwilligungserklärungen

Für viele gespeicherte Daten gibt es keine Gesetze oder Verträge als Rechtsgrund-lage zur Verarbeitung. Somit sind hierfür Einwilligungserklärungen zu erstellen.

Einwilligungserklärungen müssen über folgende Mindestanforderungen verfügen:

* Informationen über den Zweck
	+ Was genau wird eingewilligt?
* Freiwillige Willensbekundung
	+ Somit keine Kopplung mit anderen Zwecken
	+ Nicht vorausgefüllt oder in „AGBs versteckt“
* Einfach und lesbar für den Betroffenen
	+ Jeder muss verstehen, was er einwilligt
* Verweis auf Widerspruchsrecht
	+ „Sie können dieser Einwilligung jederzeit per Mail an ortsgruppenname@naturfreunde.at widersprechen.“
* Bei Kindern unter 16 Jahren (in Österreich 14 Jahre) ist die Einwilligung eines Erziehungsberechtigten notwendig.

Eine Einwilligung sollte daher immer mit den Worten „Ich willige ein, dass …“ oder „Ja, ich erlaube, dass …“ anfangen. Eine Art „Mir ist bekannt, dass …“ ist zu wenig.

Eine Einwilligung kann auch durch eindeutige Handlungen durchgeführt werden. Wenn z.B. ein Gruppenfoto erstellt wird und jedem bekannt ist, dass dies auf die eigene Website kommt, so gilt das Hinstellen und fotografieren lassen bereits als Einwilligung, solange kein Widerspruch zu erkennen ist.

Achtung: Der Verantwortliche ist in der Beweispflicht! Somit sind Einwilligungs-erklärungen möglichst schriftlich und für den genauen Zweck zu vereinbaren. Eine Unterschrift selbst ist grundsätzlich nicht notwendig, auch ein Bestätigungsmail kann hier ausreichen.

# Betroffenenrechte

Es sind nachfolgende Prozesse für die Betroffenen einzurichten: Alle diese Aufgaben müssen unverzüglich, innerhalb von 30 Tagen, durchgeführt werden.

Alle diese Rechte sind unentgeltlich, d.h. kostenlos einzuräumen, auch wenn diese sehr viel Aufwand im Einzelfall bedeuten können.

Weiters ist hierbei darauf Wert zu legen, dass keine Fehlauskünfte, fehlende Daten oder Auskünfte an falsche Personen passieren. Vergewissern Sie sich bitte, ob die Person auch wirklich jene ist, für welche sie sich ausgibt (Identitätsfeststellung).

## Auskunftsrecht

Jeder Betroffene hat das Recht, eine Kopie aller verarbeiteten Daten zu erhalten. Dazu zählen unter anderem (aber nicht ausschließlich):

* Daten aus der Mitgliederverwaltung
* E-Mails von allen Mitarbeitern oder Funktionären
* Briefe, Rechnungen, usw.

Diese Kopien sind in elektronischer Form zu übergeben. Betriebsgeheimnisse und Daten von weiteren Personen sind zu schwärzen! Der Betroffene ist auch über das Recht der Berichtigung und dem Löschrecht zu informieren. Dies kann z.B. mittels folgendem Satz erfolgen:

„Weiters haben Sie das Recht auf Berichtigung oder Löschung der Daten.“

Weiters sind folgende Informationen anzuschließen:

* Verarbeitungszwecke, Datenkategorien
* Empfänger der Daten, ggf. auch Drittstaateninformationen
* Speicher- und Löschfristen
* Herkunft der Daten (soweit möglich)
* Bei automatisierten Entscheidungen auch die Logik dazu (Profiling)
* Der Betroffener ist zu informieren, dass er ein Berichtigungs- und Lösch-recht besitzt!

## Löschrecht

Jede Person hat das Recht darauf, dass die verarbeiteten Daten gelöscht werden, wenn diese nicht mehr benötigt werden bzw. der Zweck wegfällt.

Bei Stellung eines Löschbegehrens ist zu prüfen, welche Daten verarbeitet werden und ob diese noch durch gesetzliche Aufbewahrungspflichten geschützt sind (z.B. Rechnungen sind nach BAO 7 Jahre aufzubewahren). Alle anderen Daten sind zu löschen.

Dem Betroffenen ist innerhalb der Frist mitzuteilen, warum manche Daten nicht gelöscht wurden. Weiters muss er auf sein Beschwerderecht bei der Datenschutz-behörde hingewiesen werden.

„Es wurden alle von Ihnen verarbeiteten personenbezogenen Daten gelöscht, ausgenommen von:

* Rechnungen der letzten 7 Jahre
* Gekaufte Produkte der letzten 3 Jahre wegen Gewährleistungsrechten

Sollten Sie der Ansicht sein, unsere Verarbeitung bzw. Weiterspeicherung der oben angeführten Daten entspräche nicht den Datenschutzgesetzen, haben Sie jederzeit die Möglichkeit sich bei der Österreichischen Datenschutzbehörde zu beschweren.“

## Informationsrecht

Jeder Betroffene hat das Recht darauf zu wissen, welche personenbezogenen Daten verarbeitet werden. Dazu zählen unter anderem folgende Informationen:

* Welche Daten (z.B. Name, Adresse, E-Mailadresse, usw.)
* Zweck und Rechtsgrundlage (vgl. 5)
* Empfänger der Daten (an wen werden die Daten weitergeleitet)
* Speicherdauer
* Falls Speicherung außerhalb der EU durchgeführt wird
* Betroffenenrechte inkl. Beschwerderecht
* Wenn Daten nicht vom Betroffenen selbst stammen auch die Quelle der Daten

Die Naturfreunde erfüllten diese Informationspflicht durch die Veröffentlichung der Datenschutzrichtlinien unter <http://www.naturfreunde.at/datenschutz>.

## Weitere Rechte

Es gibt noch weitere Rechte.

* Berichtigungsrecht
* Recht auf Verarbeitungseinschränkung
* Recht auf Datenübertragung

Details zu diesen und den oben genannten Rechten finden Sie z.B. unter: <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html>

# Datenpannen

Die DSGVO definiert eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbe-fugten Offenlegung führt.

Als „data breach“ kann daher z.B. ein Vorfall verstanden werden, durch den Unbefugten der Zugriff auf Daten möglich wird (z.B. Verlust eines Datenträgers, Hackerangriff, Verlust von Mitgliederlisten, etc.)

Daher sieht die DSGVO für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten folgende Melde- und Benachrichtigungspflichten vor:

* Meldung an die zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, sowie
* Benachrichtigung der betroffenen Person, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Ein mögliches Formular dazu erhalten Sie unter: <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html>