Anleitung zum Erarbeiten eines Datenschutzkonzeptes nach DSGVO für einen Ausbildungs-Verein

Sie finden die notwendige Vorlage unter
https://www.dataprivacydoctors.at/vorlagen/

Bei Änderungen in der Gesetzeslage oder neuen Informationen bieten wir allen Interessierten an, Sie über notwendige Ergänzungen, Änderungen oder Streichungen in diesem Dokument per Email zu informieren. Wir empfehlen eine Nutzung dieses unentgeltlichen Services, wodurch Ihr Datenschutzkonzept als lebendes Dokument aktuell gehalten werden kann. Bei Interesse melden Sie sich bitte bei unserem Newsletter an:
https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung

Wir wünschen Ihnen viel Erfolg bei der Umsetzung,
Ihr Christopher Temt und Michael Werzowa

Einleitung

Diese Anleitung und das Konzept haben wir für (Ausbildungs-) **Vereine für Psychotherapeuten** erstellt, ...

- bei denen mehr als eine Person Zugriff auf personenbezogenen (=pb) Daten haben
- unabhängig ob der Verein gemeinnützig ist oder nicht
  (Bitte halten Sie ggf. Rückfrage mit Ihrer Steuerberatung bzw. Rechtsvertretung)
- die mindestens eine Person, sei es auch halbtags oder geringfügig, im Angestelltenverhältnis haben
- und die nicht umfangreich und/oder als Kerntätigkeit sowie als Vereinszweck Art 9 Daten besonderer Kategorien, oft auch „sensibel" genannt, verarbeiten. Diese Daten betreffen sämtliche Informationen, die zu Diskriminierung führen können sowie strafrechtliche, gesundheitsbezogene oder biometrische Daten, zB. politische Einstellung, sexuelle Orientierung, Religionszugehörigkeit, Strafregisterauszug, Fingerabdruck, Röntgenbilder, udglm. (siehe auch **Datenschutzbeauftragter).**
  - Bei Ausbildungsvereine ist die Kerntätigkeit Ausbildung und nicht das Verarbeiten von „sensiblen Daten", die nur notwendig sind, um den Vereinszweck zu erfüllen.

Anleitung

Im Weiteren werden alle notwendigen Schritte vorgestellt, um als Verein eine DSGVO-konforme Dokumentation zB. bei Anfragen der Datenschutzbehörde vorweisen zu können.
Wichtig: Bitte lesen Sie den Disclaimer auf der letzten Seite.

Alle gelb markierten Textstellen sind entsprechend Ihrer individuellen Situation anzupassen

Grün bedeutet, dass hier Ihr IT-Berater oder Software-Anbieter helfen sollte

Blau bedeutet, dass hier Ihre Steuerberater/Bilanzbuchhalterin helfen sollte

Insbesondere bei Verträgen bzw. Statutenänderungen sollte eine Rechtsanwaltskanzlei für rechtsverbindliche, schriftliche Auskünfte kontaktiert werden. Tipp: Rechtsschutzversicherungen bieten häufig kostenlose Beratungsoptionen als Erstgespräch an.

Newsletter Verein dort, wo wir jetzt schon wissen, dass es strittige oder offene Fragen gibt und wir sie gerne über Änderungen usw. informieren wollen (mit jederzeitigem Widerspruchsrecht).
https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung

Vorschlag: Datenschutz-Info-Veranstaltung für alle Mitarbeiter und Funktionäre

Siehe: https://www.dataprivacydoctors.at/angebot/

Fotos bei Veranstaltungen

Wie man als Verein mit dem Fotografieren bei Veranstaltungen umgehen sollte, finden Sie hier: https://www.dataprotect.at/2018/05/15/verwendung-von-fotos-von-veranstaltungen-nach-dem-25-05-2018/ , wobei wir ergänzend hinzufügen wollen, dass Sie das Fotografieren auch zeitlich und/oder örtlich eingrenzen sollten, denn es sollten auch Leute auf Ihre Veranstaltungen kommen können, die nicht unbedingt fotografiert werden wollen!
Zeitlich: Nur von 19 bis 20 Uhr oder nur bei der Siegerehrung/Preisverleihung oder …
Örtlich: Bei Ausstellungen z.B. nur in den markierten Räumen oder bei Vorträgen, ..nur bis in die ersten 10 Reihen oder nur Tribüne A oder ……..

Deckblatt und allgemeiner Teil

- Bitte die gelb markierten Felder mit Ihren (Vereins-) Daten ersetzen
- ZVR-Zahl des Vereins gemäß § 18 Abs. 3: eintragen
- Disclaimer löschen
- Wenn fertig, Inhaltsverzeichnis neu erstellen
- Regelmäßige Weiterbildung auch im Bereich des Datenschutzes ist anzuraten.
  Hinweis: Hier bietet die Initiative KMU DIGITAL für WKO-Mitglieder sinnvolle Förderungen, womit 50% der Kosten von einschlägigen Weiterbildungsmaßnahmen rückvergütet werden.

Verarbeitungsverzeichnisse

- Bitte die gelb markierten Felder mit Ihren Daten ersetzen

Mitgliederverwaltung und Vereins- bzw. Geschäftsabwicklung:

- Bei Vereinen mit mehreren Personen mit Zugang zu pb Daten ist der Verantwortliche der Obmann/frau bzw gemäß Statuten und im Sinne der DSGVO

Bitte vermeiden sie den Begriff Datenschutzbeauftragter, außer Sie braucht einen, denn Datenschutzbeauftragte sind (arbeits-) rechtlich besonders geschützt.

- **Kategorien der verarbeiten Daten**
  - Die Felder für Datenkategorien bitte mit den Feldern aus Ihrer Software, aus Ihrer Praxis ersetzen oder wenn nicht benötigt, streichen. Sollten mehrere Ihrer Daten unter eine Datenkategorie fallen, so nehmen Sie die allgemeinere hier.
  - Auszahlungen, Aufwandsentschädigungen usw. an Funktionäre und Mitglieder werden auch hier und nicht im Personalwesen erfasst. Rücksprache mit Steuerberater!
  - Wir haben nicht die Daten, die an Ihren IT-Dienstleister (mit Fernwartung) bzw Software-Anbieter mit Fernwartung und ähnliche in die Spalte ganz rechts eingetragen. Da Sie aber einen Datenverarbeitungsvereinbarung nach Art 28 mit den Genannten abschließen müssen, werden in dieser Vereinbarung alle pb Daten erfasst und sie brauchen dann nur „**6, 7, ...**“ in das jeweilige Feld der Spalte dazu schreiben. Aber dies können Sie später machen, wenn wir im Anhang dann zu den Art 28 Vereinbarungen kommen.
  - Mögliche weitere Datenverarbeiter für Vereine:
    siehe **Anhang „Mustervereinbarung für Auftragsverarbeitung“**

- **Kategorien der Empfänger**
  - Falls Sie Fernwartungen Ihres Computers zulassen, so müssen Sie es hier dokumentieren.

Ausbildung

Bitte hier die Daten eintragen, die Sie von Auszubildenden erhalten, brauchen bzw erfassen und verarbeiten

09	Leumund-Zeugnis	Art 10	3 - 4
10	Lebenslauf	Vertraulich	3 - 4
11	Daten gemäß Schulungsbeschreibungen	Vertraulich	3 - 4
12	Daten gemäß Schulungsbeschreibungen	Vertraulich	3 - 4
13	Daten gemäß Schulungsbeschreibungen	Vertraulich	3 - 4
14	Gesundheitsdaten	Art 9	3 - 4

Kommunikation

- **Kategorien der verarbeiten Daten**
  - Die Felder für Datenkategorien bitte mit den Feldern aus Ihrer Software, aus Ihrer Praxis ersetzen oder wenn nicht benötigt, streichen. Sollten mehrere Ihrer Daten unter eine

Datenkategorie fallen, so nehmen Sie die Allgemeinere hier.

- **Newsletter:**
  Bitte in der letzten Spalte schreibt entweder intern, wenn Sie Newsletter selber versendet oder extern, wenn Sie einen Newsletter-Tool-Anbieter aus der EU bzw DACH– eher nicht USA – verwendet, denn Sie müssen auch eine (deutschsprachige) Vereinbarung abschließen (siehe Anhang).

- **Sichere und verschlüsselte Datendiensten für Ihre Kommunikation**

  - Es gibt mehrere sehr gute und vertrauenswürdige Anbieter von verschlüsselten und sicheren Kommunikations-Apps, wie zB telegram, wire oder signal.

    Wir verwenden schon seit Jahren www.signal.org sowohl auf unseren Handys als auch auf unseren Desktops und sind zufrieden damit, aber die anderen Anbieter sind sicher genauso gut – **Ihre Wahl** und dann in die Zeile Empfänger eintragen

    Mehr zu signal.org: https://support.signal.org/hc/en-us/articles/212477768-Is-it-private-Can-I-trust-it- Da signal.org keinen Zugang zu den gesendeten Daten, SMS und Gesprächen hat und ebenso nicht zu den Telefonnummern, werden keine pb Daten an signal.org übertragen und Sie brauchen daher nichts in die Spalte eintragen und es bedarf daher auch keiner Vereinbarung gemäß Art 28 DSGVO. Sollte die Datenschutzbehörde zu einer anderen Meinung gelangen,
    Newsletter

Personalwesen

Funktionäre und Vereinsmitglieder mögen zB Aufwandsentschädigungen und ähnliches erhalten, dies wird aber nicht hier, sondern beim 1sten Verezeichnis „Mitgliederverwaltung“ erfasst.

Tipp, sehr hilfreich: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html

- Um das Risiko für die Mitarbeiter und die Betroffenen gering zu halten, sollen die Verträge von einem Rechtsanwalt erstellt/gegengelesen werden und die TOMs soweit als möglich und vertretbar durchgeführt worden sein, um auch die Mitarbeiter zu schützen!

- Geheimhaltungsvereinbarung mit Mitarbeitern und Funktionären siehe Anhang

- DSGVO-Schulung der Mitarbeitern und auch der Funktionäre ist ausdrücklich angeraten!

Weitere Verarbeitungsverzeichnisse

Es kann leicht sein, dass Sie pB Daten auch anderswo verarbeiten, erfassen, einsetzen usw. Sollte daher die obigen Verzeichnisse nicht alle Ihre Verarbeitungen abdecken, so findet Sie hier **weitere Verarbeitungsverzeichnisse** und da ist höchstwahrscheinlich auch die von Ihnen gesuchte dabei

1. Sehr gute Muster und Vorlagen auch für Vereine nutzbar (zB: Online-Shop, Aushang, …..) https://www.wko.at/branchen/handel/datenschutzgrundverordnung-in-handelsunternehmen.html

2. Verarbeitungsverzeichnisse für diverse Berufe und möglichen Vereinszweck https://www.lda.bayern.de/de/kleine-unternehmen.html

3. Eine sehr gute Liste mit diversen weiteren Verarbeitungsverzeichnissen: https://www.datenschutz-guru.de/verzeichnis-von-verarbeitungstaetigkeiten/

TIPP

Bei mehr als 3 oder 4 Verzeichnissen, raten wir Ihnen eine Excel-Datei zu benutzen, da es so einfacher und übersichtlicher wird.

Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Checkliste – IT Safe (WKO)

Bitte unbedingt machen: Wir, Funktionäre und auch die aktiven Mitglieder, sind die wirklich hilfreiche IT-Checkliste für EPUs unter https://itsafe.wkoratgeber.at/ durch gegangen und konnten feststellen, ob und wo es in unserem Verein Probleme im IT-Bereich geben könnte. Die daraus folgenden Maßnahmen siehe TOMs.

Selbstschutz

Wir versuche unser Such- und Surfverhalten soweit wie möglich „sicher" zu gestalten und verwenden daher zB den europäischen Open Source Browser https://cliqz.com/ inklusive Ghostery (verhindert und zeigt mir die Trackingversuche) und zB die europäische Suchmaschine: https://www.startpage.com statt Google .

Handy

Wir habe ein Handy (für die private Kommunikation und ein Handy ausschließlich) für unsere Vereinstätigkeit als Funktionäre. Statt WhatsApp verwende wir zB https://www.signal.org/

UnserHandy ist durch 6-stelliges Passwort bzw. Biometrie geschützt. Es gibt die Möglichkeit die Daten „fern zu löschen" bei Apple, bei anderen Handys bitte Security-App downloaden. Bluetooth-Funktion ist nur beim Autofahren eingeschaltet. WLAN ist abgeschaltet. In öffentliche WLAN-Netze wähle ich mich nicht ein und es gibt auch keine automatische Verbindung mit mir bekannten WLANs. Wenn wir ein neues Handy/Laptop/Computer kaufen, so lasse wir unser altes Handy Laptop/Computer von meinem IT-Fachmann immer vollständig löschen (Vereinbarung gemäß Art 28 DSGVO). Falls wir USB-Sticks verwende, so sind die Daten darauf verschlüsselt und ein Passwort ist notwendig, um auf die Daten zu zugreifen.

Impressum

Impressum bzw Datenschutzerklärung werden oft vom Homepage-Ersteller oder Betreiber für den Therapeuten als kostenloses Service DSGVO-konform erstellt und verlinkt.

- Das Impressum für vereine: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Das-korrekte-Website-Impressum-Verein.pdf
- Mit dem ECG-Service können Sie mit ein paar Klicks ein rechtlich gültiges Impressum erstellen.
- Wir raten Ihnen ausdrücklich von http://www…… zu **https://.....** zu wechseln.
- Wenn Ihre Homepage mit WordPress erstellt wurde, so findet Sie oder der Ersteller/Betreiber hier wichtige Tipps: https://www.blogmojo.de/wordpress-plugins-dsgvo

Statuten
Wie in der Generalversammlung beschlossen,

Datenschutzerklärung
Hier eine Anleitung für Ihre Datenschutzerklärung: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/muster-informationspflichten-website-datenschutzerklaerung.html

- **Gemäß Informationspflicht**
  müssen Sie in Ihrer Datenschutzerklärung auch allgemein beschreiben welche Daten Sie wie verarbeiten (siehe Ihr Verzeichnisse bei Zweck und Datenkategorien)
- **Dauer**
  und wie lange:

zb Bei einem bestehenden oder abgeschlossenem Vertrag aufgrund der gesetzlichen Aufbewahrungsfristen wie z. B. § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen.

- Hier hilft Ihnen https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

  Am Ende des Ratgebers erhalten Sie ein **Merkblatt mit Textbausteinen** für Ihre Informationspflicht, die Sie für Ihre Datenschutzerklärung , aber auch bei der Einwilligungs-Erklärung verwenden können.

- **Wir arbeiten bei Datenschutzerklärungen mit**: **https://datenschutz-generator.de/**
  Kostenpflichtig 99,- Euro! Aber es zahlt sich aus!!!

TOMs als Fließtext

In der Vorlage finden sie eine Excel-ToDo-Liste, eine Liste der Maßnahmen, die Sie umsetzten sollten. Wenn sie eine Maßnahme umsetzen sollten Sie aus der TOM-Beschreibung einen Fließtext, ganze Sätze machen, ähnlich wie Ärzte es in ihrer Dokumentation machen http://www.aek-wien.at/documents/4771581/22586874/DSGVO+Verzeichnis+Muster+EP/c8ddf437-3f23-4020-9b74-278915cc608f)

Als Beispiel:

Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

X	Passwortvergabe		Authentifikation mit biometrischen Verfahren

Unsere Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.
Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Der Vorteil: *Sie sehen mit einem Blick, was Sie schon umgesetzt haben (Fließtext) und was noch zu tun ist (Excel-Liste).*

TOMs - Einzelne Maßnahmen

- Organisatorische Maßnahmen und z. B. abschließbarer Aktenschrank usw. können Sie selber machen, bei einigen IT-Maßnahmen sollte Ihr es in Absprache mit IT-Berater bzw Software-anbieter machen, wie zB

- Verschlüsselung aller (Vereins-) Computer, Laptops, Handys, USB und regelmäßiges Backups

- Bei Verschlüsselungen ist der Prozess wie folgt und ein IT-Experte beizuziehen:
  1. Schritt: Backup
  2. Schritt: kontrollieren ob Backup funktioniert
  3. Schritt: Verschlüsseln

- siehe Workshops: https://www.dataprivacydoctors.at/angebot/

- Bitte – auch in Absprache mit IT-Berater bzw Software-Anbieter – umgesetzten TOMs ankreuzen und anderen entfernen

- Rotes X bei den Feldern sind Maßnahmen, die wir als Mindeststandart empfehlen

- Schwarze X sollten Sie auch schnellst möglich umsetzen.

    - Ein Kontroll- und Verbesserungsprozess sollte mindestens 1x jährlich durchgeführt werden, so auch die DSGVO. Datenschutz ist ein Prozess!

Prozesse betreffs Betroffenenrechte

Quelle: http://www.aekwien.at/documents/4771581/22586874/DSGVO+Verzeichnis+Muster+EP/c8ddf437-3f23-4020-9b74-278915cc608f)

Feststellung der Identität:

- „Sehr geehrte Frau/Herr …!
  Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen, wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scan Ihres Personalausweises/Reisepasses zukommen zu lassen. Der Identitätsnachweis wird nach Zweckerfüllung umgehend gelöscht.
  Ich danke Ihnen für Ihr Verständnis

  oder

- Das sicherst wäre den Betroffenen zu bitten, seinen Ausweis/Führerschein vor die Handykamera zu halten. Dies mag bei sensiblen Daten nach Art 9 und vor allem bei Erziehungsberechtigten wohl der einzige gangbare Weg sein, die Identität sicher fest zu stellen.

Wir raten Ihnen daher hier **Ihre eigene Risikoanalyse** (siehe dort) zu machen und dann entsprechend Ihrer Einschätzung vorzugehen und dies in der Vorlage zu dokumentieren.

Sollte Ihnen Ihr Programm bessere Möglichkeiten bieten, als die (Stamm) Daten des Betroffenen per **Screenshot** zu erfassen, so verwenden sie natürlich diesen Weg. Leider können aber die meisten Programme dies (noch) nicht.

Leider kann man bei vielen Programmen zB die Rechnung usw **nicht** nach 7 Jahren löschen oder bei Antrag auf Löschung **nicht** sofort löschen, da hilft – solange der Anbieter der Software es nicht geändert hat – nur die Funktion „Auftragssperre", die es bei den meisten Programmen gibt!

E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)

- Eine sehr gute Listung der DSGVO-konformen Newsletter-Tool-Anbieter findet Sie hier: https://www.blogmojo.de/adv-vertraege/

- Die reine **Ankündigung einer Generalversammlung** ist kein Newsletter sondern eine notwendige Information aller Ihrer Mitglieder, so dass sie ihre Rechte als stimmberechtigte Vereinsmitglieder geltend machen können! Sie muss daher trotz eines etwaigen Widerspruchs eines Mitgliedes zum Newsletter erfolgen!

Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

Wir haben Ihnen hier eine Teil-Risikoanalyse gemacht.
ABER Sie müssen sie trotzdem für Ihren Verein noch einmal machen bzw vervollständigen, da es immer vom
konkreten Fall, den individuellen Umständen
UND den gesetzten TOMs abhängig ist!

Schutzbedarfsanalyse

Unsere Vorabanalyse ergab, dass es sich bei folgende pb Daten der Mitglieder, Lieferanten, Geschäftspartner und an der Vereinstätigkeit mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, da sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht und auch allgemeine TOMs gemäß DSGVO gesetzt wurden:

> *Öffentlich zugängliche Daten, Ordnungsnummer, Name, Firma oder sonstige Geschäftsbezeichnung, Anrede/Geschlecht, Anschrift, Homepage, Kontaktdaten (Tel., Skyp, Mail, Fax,), Berufs-, Branchen- und Geschäftsbezeichnung, Firmenbuchdaten, Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer, Korrespondenzsprache, Namen der Kontaktpersonen/Erziehungsberechtigte, Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.), Funktion/Rolle der Kontaktperson usw.)*

Weiters ergab unsere Vorabanalyse, dass es sich bei folgende pb Daten der Mitglieder, Lieferanten, Geschäftspartner und an der Vereinstätigkeit mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit einen **hohen** und **sehr hohen** Schutzbedarf handelt und daher eine erweiterte Risiko-Analyse durchgeführt werden muss.

> *Alle Daten gemäß Art 9 (Mitarbeiter/Auszubildende) und möglicherweise Art 8 (Kinder) des DSGVO, Leumund, Lebenslauf, Personenstand, Geburtsdatum, Bankverbindungen, Kreditkartennummern und -unternehmen, (Beratungs-) Vertragstext und Korrespondenzen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch und Mitschriften und Fotos, ….. (siehe Verarbeitungsverzeichnisse! Die pb Daten von dort hier eintragen*

Risikoanalyse ohne Maßnahmen

Analysieren Sie bitte Ihre Daten und tragen Sie sie in die entsprechenden **Risikokategorien** in die Vorlage ein.
Wir haben schon Kategorie 1 + 4 in die **Risiko-Matrix** eingetragen, die anderen machen Sie bitte gemäß Ihrer Einschätzung (siehe unten Schwere und Eintrittswahrscheinlichkeit) selber!

Bewertungsmaßstäbe

Hier die Bewertungsmaßstäbe um die Daten in das entsprechende Feld der **Risiko-Matrix** eintragen zu können:

Schwere:

Schwere	Auswirkung auf Betroffene	Folgen überwinden	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, …
Begrenzt	Wesentliche Unannehmlichkeiten	Unannehmlichkeiten sollten sich – trotz Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, …
Wesentlich	Wesentliche Folgen	Unannehmlichkeiten sollten sich – trotz großer Schwierigkeiten – überwinden lassen	Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte, Gerüchte, …
Existenz-gefährdend	Irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	**Bekanntwerden zB der Diagnose führen zu finanzielle Not, Kündigung, Familientragödien, Selbstmord, …** und/oder vertrauliche Mitschriften werden Öffentlichkeit bekannt und gefährden Betrieb; Beruf, Identitätsdiebstahl; … langfristige Beschwerden, Tod, …

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Eintrittswahrscheinlichkeit:

EWK	Wahrscheinlichkeit	Beispiele
Vernachlässigbar	0-24% Wahrscheinlichkeit	zB Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw pb Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	zB Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	zB Ausfall durch einen Festplattenausfall, Festplatten halten ca 3 – 5 Jahre! Datenverluste durch technische Fehler

Maßnahmen

Siehe TOMs, insbesondere
Sie müsst schauen, dass Sie die Kategorien in der Risiko-Matrix **von rechts oben in Rot => nach links unten in Grün mit Hilfe Ihre Maßnahmen bekommen!**

Risiko-Matrix mit Maßnahmen

Bitte hier die Kategorien 1 - 4 gemäß Ihrer Maßnahmen eintragen!

Unser angemessenes Datenschutzniveau

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
	Mit Datenschutzbehörde **kommunizieren**	
1. Betroffene sind nicht zu informieren		

- Für den Verein, der uns bei der Erstellung geholfen hat, war dann dieses Datenschutzniveau angemessen und wieder in Wir-**Form:**

  - Die pb Daten der Kategorie 1 haben wir trotz TOMs „Risiko“ zugeordnet, da bei einer **möglichen** Datenschutzverletzung die Folgen **begrenzt** sind, nichts desto trotz muss aber hier eine Risikoanalyse gemacht werden und bei Risiko wird die Behörde über diesen Fällen informiert, bei hohem Risiko auch die Betroffenen.

  - Als Verantwortlicher ist mir/uns so auch bewusster, dass einmal gesetzte TOMS nicht für alle Zeiten alle möglichen und vor allem neuartige (kriminelle) Datenschutzverletzungen auffangen können und ich bleibe so acht und wachsam. **=> Datenschutz ist ein Prozess!**

Zusammenfassung

Sehr geehrter Verein!

Wir wollen ausdrücklich festhalten, dass niemand zum jetzigen Zeitpunkt ein perfektes und juristisch wasserdichtes Konzept abliefern kann, zu viele Punkte sind offen, strittig und es fehlen die letztinstanzlichen Gerichtsentscheidungen, aber dass Sie, wenn Sie diese Vorlage sorgfältig ausfüllen, eine Risikoanalyse durchführen, die vorgeschlagenen TOMs auch wirklich als Mindeststandart umsetzen, DSGVO-Beratung/Workshops in Anspruch nehmen und sich per Newsletter updaten, die Behörde höchstwahrscheinlich von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen wird und Sie vor allem gegenüber Ihren Mitgliedern mit gutem Gewissen sagen können:

„Liebe Mitglieder!
Vertrauen zwischen mir als Verantwortliche /r Obmann/frau und Ihnen ist die Grundlage und Voraussetzung für eine gedeihliches Vereinsleben, daher sind auch alle Ihre persönlichen Daten bei uns in guten Händen.

Ich sichere Ihnen zu, dass wir sorgsam und streng vertraulich damit umgehen und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen sind.

Ihr Obmann/frau

Wir wünschen Ihnen gutes Gelingen und verbleiben
Hochachtungsvoll
Christopher Temt und Michael Werzowa

Anhang

Muster Datenschutzverletzung (WKO)

Sollte Ihnen eine Datenschutzverletzung passiert sein oder Ihnen bekannt geworden sein, die ein Risiko für die Betroffenen bedeutet (siehe Risko-Matrix gelb), so müssen Sie innerhalb von 72 Stunden die zuständige Datenschutzbehörde informieren.

Sollte ein **hohes Risiko** für die Betroffenen bestehen, so müssen Sie auch innerhalb von 72 Stunden **alle** Betroffene informieren.

- Bitte die gelb markierten Felder mit Ihren Daten ersetzen

Mustervertrag Auftragsverarbeitung (WKO)

- Typische **Aufragsverarbeitungen für Vereine** nach Art 28 und daher eine **Vereinbarung Art 28 DSGVO mit Ihnen notwendig,** sind Dienstleistungen wie:
  - Datendiensten bzw Hosting der Webseiten
  - Anbieter verschlüsselter und sicherer Datenübertragung
  - IT-Anbieter (mit Fernwartung)
  - Software-Anbieter mit Fernwartung
  - Newsletter-Tool-Anbieter

- Wir haben Ihnen in der Vereinbarung den Zusatz für Fernwartung dazugeschrieben für
  - Hier muss auch der IT-Anbieter bzw Software-Anbieter mit Fernwartung angeben, welche Daten er von Ihnen übertragen bekommt, Diese dann bitte unter **Ziffer 6, 7, ….**in das Verarbeitungsverzeichnis dann eintragen!

- weitere mögliche sind:
  - Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten, das Einscannen von Dokumenten, die Backup-Sicherheitsspeicherung und andere Archivierungen, Datenträgerentsorgung,…

Keine Aufragsverarbeitung und damit Verantwortliche und somit **keine Vereinbarung gemäß Art 28 DSGVO notwendig sind** die Auslagerung von Aufgaben/Funktonen oder die externe Inanspruchnahme von Fachleistungen an/von einem Dritten mit dort **eigenverantwortlicher** Wahrnehmung wie:

- Personalverwaltung, Mitarbeiterrekruterung, Vertragskundenbetreuung, Finanzberatung, **Steuerberatung**, Unternehmens/DSGVO-Beratung, Wirtschafsprüfung, Rechtsanwälte, Notar, Therapeuten, Apotheken, Anbieter von Telefonleitungen, bzw Internetleitungen, Post, Transport, Ärzte, Krankenhäuser, Sozialversicherung, Inkassotätgkeit mit Forderungsübertragung, Sachveständigen- bzw. Gutachterbeaufragung, usw.

- Bei diesen, da Verantwortliche, müssen Sie nichts tun!

  Es wäre aber anzuraten, das Sie sich vergewissern, dass diese Verantwortlichen auch eine Dokumentation gemäß DSGVO betreffs des Datenschutz haben.

Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

- In allen Fällen, wo Dritte in Ausübung ihrer beruflichen/ehrenamtliche Tätigkeit bzw in Ausbildung voraussichtlich **Kenntnis** über teilweise sehr sensible personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse **erhalten könnten**

Einwilligungserklärung – Mitglieder

- Hier haben wir Ihnen nur die drei Mindesterfordernisse aufgezählt
- Vieles lässt sich über die Statuten regeln, hier ist aber eine Rechtsanwaltkanzlei unbedingt zu Rate zu ziehen!
- **Informationspflicht**

  Die Datenschutz-Grundverordnung (DSGVO) verpflichtet jeden Verantwortlichen, die betroffene Person in präziser, transparenter, verständlicher und leicht zugänglicher Form über die wichtigsten Aspekte einer Datenverarbeitung zu informieren. Dies hat schriftlich (einschließlich elektronisch) zu erfolgen. Werden die Daten direkt bei der betroffenen Person erhoben, **wie hier**, so hat diese Information sogleich zu erfolgen.

  Hier hilft Ihnen https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

  Am Ende des Ratgebers erhalten Sie ein **Merkblatt mit Textbausteinen** für Ihre Informationspflicht, die Sie für Ihre Datenschutzerklärung ebenso verwenden können.

Ende

Workshops für Vereine

https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung

DISCLAIMER

Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Die Autoren, Christopher Temt und Michael Werzowa, übernehmen jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen wie WKO, Ärztekammer). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine **konkrete Prüfung im Einzelfall,** und meist auch Änderungen in den eigenen Prozessen, weshalb die Beiziehung eines Datenschutzberaters (z.B. https://www.dataprivacydoctors.at/) sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Christopher Temt, und/oder Michael Werzowa welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Die Autoren behalten es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.