Richtlinie des Datenschutzes und der Vertraulichkeit von Informationen

(nachstehend auch „Datenschutz- und Vertraulichkeitsrichtlinie“ oder „IT-Sicherheitsrichtlinie“ genannt)

geltend zwischen

Pfadfinderleitern und Mitarbeitern der Gruppe 37 „Christoph Columbus“ der Wiener Pfadfinder und Pfadfinderinnen
(nachstehend „Auftragnehmer“)

und

Gruppe 37 „Christoph Columbus“ der Wiener Pfadfinder und Pfadfinderinnen
Brückengasse 7, 1060 Wien
(nachstehend „Verein“ genannt)

- beide einzeln oder gemeinsam nachfolgend „Parteien“ genannt –

- V2018-06 -
12. September 2018

INHALT

1 ÄNDERUNGSVERZEICHNIS

Versionsnummer	Datum	Bearbeiter	Änderung
0.1	10.06.2018	E. Weißenberger	Erstversion

2 ANSPRECHPARTNER

Name	Unternehmen	Fachbereich	Kontaktdaten
Ernst Weißenberger	Gruppe 37	ERO	e.weissenberger@a1.net

3 DEFINITIONEN

Im Sinne der Datenschutz- und Vertraulichkeitsrichtlinie haben die nachfolgend angeführten Begriffe die folgende Bedeutung:

DATENSCHUTZ- UND VERTRAULICHKEITSRICHTLINIE/ IT-SICHERHEITSRICHTLINIE/ RICHTLINIE DES DATENSCHUTZES UND DER VERTRAULICHKEIT VON INFORMATIONEN	Datenschutz- und Vertraulichkeitsvereinbarung zwischen dem Verein zum Zweck des konformen Umgangs mit Daten und Informationen des Vereins und des Mitglieds.
KUNDENVERTRAG	Vertrag zwischen dem Verein und dem Mitglied zur Erbringung von (Dienst-) leistungen.
KUNDE	Das Mitglied.
PROJEKTE	Die Summe aller unter dem Punkt „Leistungsgegenstand / Leistungsinhalt“ in den jeweiligen Einzelverträgen angeführten Lieferungen und Leistungen.
VERBUNDENE UNTERNEHMEN	Unternehmen, an denen der Verein beteiligt ist oder die am Verein beteiligt sind und deren verbundene Unternehmen.

Sämtliche personenbezogenen Aussagen sind geschlechtsneutral zu verstehen.

4 EINLEITUNG

4.1 Zweck und Inhalt der Datenschutz- und Vertraulichkeitsrichtlinie

Aufgrund verschärfter datenschutzrechtlicher Anforderungen und der gleichzeitigen Zunahme von Abschlüssen von Vertraulichkeitsvereinbarungen zwischen dem Mitglied und dem Verein soll die vorliegende Datenschutz- und Vertraulichkeitsrichtlinie dazu dienen, diesen Anforderungen gerecht werden zu können.
Diese Richtlinie stellt dabei einen Teil der von uns zu erfüllenden organisatorischen Maßnahmen dar, um den Regeln, die die anzuwendende Datenschutzgrundverordnung und das reformierte österreichische Datenschutzgesetz an uns stellen, vollumfänglich nachkommen zu können.
Die Datenschutz- und Vertraulichkeitsrichtlinie bietet den groben Rahmen der Pflichten für alle Auftragnehmer des Vereins, soweit diese Weisung der einzelnen hier geregelten Pflichten, die vollumfänglich zwingend einzuhalten sind. Gegenstand der Datenschutz- und Vertraulichkeitsrichtlinie ist die Festlegung der Rechte und Pflichten der Vertragspartner in Bezug auf den konformen Umgang mit Daten und Informationen der Mitglieder im Sinne des aktuell geltenden Datenschutzrechts und der geltenden Vertraulichkeitsverpflichtungen der Mitglieder. Inhaltlich orientiert sich der Umfang hierbei einerseits an den datenschutzrechtlichen nationalen und europarechtlichen Anforderungen und andererseits an den Inhalten der jeweiligen Vertraulichkeitsvereinbarungen unserer Mitglieder. Der Verein verpflichtet sich Daten seiner Mitglieder vor Missbrauch auf Basis des aktuell geltenden Datenschutzrechts (spez. "personenbezogene Daten") und der Vertraulichkeitsverpflichtungen (spez. "vertrauliche Informationen") seiner Mitglieder zu schützen. Um das von Gesetzes wegen geforderte Datenschutzniveau auch in Zukunft vollumfänglich erreichen zu können, werden fortlaufend technische und organisatorische Maßnahmen, die im Maßnahmenkatalog des Vereins zusammengefasst sind, getroffen.

Der Auftragnehmer nimmt zur Kenntnis, dass er die in dieser Richtlinie geregelten Rechte und Pflichten vollinhaltlich verstanden hat und seine zukünftige Leistung im Einklang mit den in dieser Vereinbarung geregelten Rechten und Pflichten erbringen wird.

4.2 Geltungsbereich

Die Datenschutz- und Vertraulichkeitsrichtlinie gilt für alle Auftragnehmer. Sollten einzelne Regelungen der Datenschutz- und Vertraulichkeitsrichtlinie mit anderen Richtlinien oder anderen vertraglichen Regelungen des Vereins in Konflikt stehen, so besteht für die Datenschutz- und Vertraulichkeitsrichtlinie ein Anwendungsvorrang gegenüber divergierenden Regelungen und ist im Zweifel vorrangig anzuwenden.
Um den datenschutzrechlichen und mitarbeiterspezifischen Anforderungen gerecht zu werden, steht die Richtlinie des Datenschutzes und der Vertraulichkeit von Informationen, wie die übrigen daten-

schutzrechtlich relevanten Arbeitsmaterialien, einer dynamischen Anpassung offen gegenüber und wird gegebenfalls unter Ankündigung optimiert und anschließend neuversioniert.

4.3 Verantwortlichkeit des Datenschutzes

Der Verein stellt sicher, dass die gesetzlichen und die in den datenschutzrechtlichen Arbeitsmaterialien (z.B. Vereinsübergreifende Datenschutzrichtlinie, Maßnahmenkatalog, IT-Sicherheitsrichtlinie, Richtlinie des Datenschutzes und der Vertraulichkeit von Informationen udgl.) enthaltenen Anforderungen tatsächlich berücksichtigt werden. Die Umsetzung dieser Vorgaben liegt in der Verantwortung aller Auftragnehmer.

4.4 Interne Zuständigkeit für Datenschutz & Schulungen

Die im Punkt 2 „Ansprechpartner“ definierten Personen stehen für datenschutzrechtliche Fragen zur Verfügung.

Der Verein trägt dafür Sorge, dass die Auftragnehmer die erforderlichen Schulungen, Anweisungen oder Informationen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind.

5 NORMATIVER BEREICH

5.1 Zutrittsschutz und Arbeitsplatz

- Räume sind, sofern möglich, beim Verlassen abzusperren und zu kontrollieren, ob elektronische Geräte, sofern zweckmäßig, ausgeschaltet bzw. in Standby gesetzt wurden.
- Die Nutzung der Bildschirme hat nach Möglichkeit so zu erfolgen, dass keine unbefugte Einsicht möglich ist.
- Datenträger und Ausdrucke sind vor Einsichtnahme zu schützen und sorgfältig zu verwahren.
- Verbindungen (z.B. VPN-Verbindungen) sind zu trennen, sobald diese nicht mehr benötigt werden.
- Vom Verein ausgehändigte Schlüssel sind vor unberechtigten Zugriffen stets sicher zu verwahren.
- Der Auftragnehmer hat bei Beendigung seiner Tätigkeit Sorge zu tragen, dass unaufgefordert sämtliche Schlüssel dem Verein auszuhändigen sind.
- Bei Aufenthalt in den Räumlichkeiten des Vereins ist der Auftragnehmer verpflichtet auf die Anwesenheit etwaiger fremder bzw. vereinsunbekannter Personen zu achten und gegebenenfalls den direkten Vorgesetzten über die Anwesenheit dieser Personen zu benachrichtigen.
- Sämtliche arbeitsbezogenen Unterlagen sind nach Beendigung sicher zu verwahren, sodass eine unberechtigte Einsicht auf den Inhalt dieser Dokumente nicht mehr möglich ist.

- Bei Verlassen des Arbeitsbereiches ist das Betriebssystem auf den Endgeräten zu sperren, herunterzufahren oder in den Standby-Modus zu versetzen.
- Das Endgerät muss nach Beendigung der Arbeit mitgenommen oder in einem versperrten Bereich aufbewahrt werden.

5.2 Einsichtsschutz

- Für die Wahl des Arbeitsbereiches für einen Notebook, einen PC, ein Tablet oder einem anderen technischen Gerät, bei dem Daten visuell ausgelesen werden können, ist dafür zu sorgen, dass der Standort so gewählt wird, dass nur der Verein und die dafür berechtigten Personen auf die Daten Einsicht haben können.

5.3 Passwörter und Benutzerkonten

- Die Erstellung von Benutzerkonten erfolgt durch den Administrator. Der Administrator hat ausschließlich für berechtigte Personen Benutzerkonten, die nur jene Rechte erhalten, welche sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen, anzulegen.
- Im Zuge der Aushändigung eines vereinseigenen Endgerätes ist das voreingestellte Domainpasswort unverzüglich zu ändern.
- Jedes Passwort hat folgende Merkmale aufzuweisen: Das Passwort muss aus einer Kombination aus Zahlen, Buchstaben und Sonderzeichen, zusammengestellt aus mindestens 6 Zeichen bestehen.
- Passwörter dürfen weder unverschlüsselt gespeichert oder aufgeschrieben noch an sichtbarer oder leicht zugänglicher Stelle aufbewahrt werden.
- Domainpasswörter auf vereinseigenen Endgeräten sind spätestens alle drei Monate zu ändern. Eine Änderung des Domainpassworts wird vom Verein alle drei Monate technisch erzwungen.
- Jedes Benutzerkonto muss immer über ein Passwort verfügen. Benutzerkonten ohne Verwendung von Passwörtern, sofern möglich, sind nicht zulässig.
- Benutzerkonten, die einer Sperrung unterliegen, dürfen nur durch den Administrator reaktiviert werden. Dabei erfolgt die Passwortvergabe analog zur Neuanlage.
- Die Verwendung eines Benutzerkontos ist ausschließlich für den dafür zugewiesenen Benutzer erlaubt. Die Weitergabe des Logins und Passworts des Benutzerkontos an andere Personen ist nicht erlaubt.
- Bei Verdacht auf unbefugte Nutzung hat der Auftragnehmer das Passwort unverzüglich zu ändern und den Administrator in Kenntnis zu setzen.
- Die Eingabe des Passworts hat stets unbeobachtet zu erfolgen.
- Die Passwortrichtlinien gelten auch für private Endgeräte, auf welchen vereinsbezogene Daten gespeichert oder verarbeitet werden.

5.4 Umgang mit externen Quellen

- Anhänge von E-Mails sind auf vereinseigenen Endgeräten stets in Bezug auf die IT-Sicherheit zu hinterfragen und dürfen nur geöffnet werden, wenn keine Sorge bezüglich eines möglichen Schadens besteht.

5.5 Umgang mit personenbezogenen Daten

- Unter personenbezogenen Daten versteht man Informationen, die eine bestimmte Person identifizieren oder eine Person identifizierbar machen. Beispiele dafür sind der Name, E-Mail, die Sozialversicherungsnummer, die Adresse, Geburtsdatum oder Telefonnummer.
- Personenbezogene Daten sind ausnahmslos vertraulich zu behandeln.

5.6 Umgang mit vertraulichen Informationen

Der Verein schließt in aller Regel Vertraulichkeits- bzw. Geheimhaltungsvereinbarung mit seinen Auftragnehmern ab. Auch die AGB des Vereins beinhalten Regelungen zur Vertraulichkeit von eigenen schützenswerten Informationen. Zur Erreichung der in diesen Vereinbarungen geregelten Pflichten gelten folgende Regelungen:

- Vertrauliche Informationen sowie alle sonstigen Informationen, die von einem Mitglied direkt oder indirekt erlangt werden, unabhängig davon, in welchem Zustand und auf welchem Datenträger sich diese vertraulichen Informationen befinden, unterliegen der Geheimhaltung.
- Sämtliche erhaltenen vertraulichen Informationen sind geheim zu halten und nur zum Zweck der Zusammenarbeit mit den Mitgliedern zu verwenden. Sie dürfen weder zum eigenen Gebrauch in irgendeiner Art und Weise verwertet, noch Dritten zugänglich gemacht werden.
- Die Geheimhaltungsverpflichtung gilt auch nach Beendigung der Vereinsmitgliedschaft.
- Kopien von vertraulichen Informationen sind nur in von Mitgliedern geregelten Ausnahmen und soweit für die Erfüllung des Auftrages benötigt, erlaubt.
- Der Auftragnehmer ist verpflichtet über diesen Punkt und über die jeweiligen abgeschlossenen Vertraulichkeitsvereinbarungen hinaus selbstständig technische und organisatorische Maßnahmen zu ergreifen, um die Geheimhaltung der vertraulichen Informationen zu wahren.
- Im Falle von Zweifel über den korrekten Umgang mit vertraulichen Informationen bzw. nach Beendigung des Projekts ist das Leitungsorgan des Vereins bzw. die in Punkt 2 definierten Kontaktpersonen zu fragen, wie mit den gespeicherten oder sonstigen abgelegten vertraulichen Informationen zu verfahren ist.

5.7 Allgemeine Sorgfaltspflichten

- Überlassene Endgeräte, wie beispielsweise PC's, Tablets, Notebooks oder Mobiltelefone, sind schonend und pfleglich zu behandeln, sodass eine Beschädigung der Hardware oder der Daten verhindert werden kann.

- Geräte sind vor übermäßiger Hitze (direkte Sonneneinstrahlung) und Kälte sowie Feuchtigkeit (Flüssigkeiten) und Erschütterungen / Stößen zu schützen.
- Der Transport hat in den vorgesehenen Notebooktaschen bzw. Rucksäcken zu erfolgen.
- Ein physischer Eingriff oder Öffnen (zerlegen, manipulieren etc.) von Geräten ist unzulässig und darf ausschließlich vom Verein zugewiesenen Personen durchgeführt werden.
- Der Austausch von Teilen (Speicher, Festplatte, SSD, Akku etc.) ist nur durch vom Verein befugten Personen bzw. durch einen autorisierten Wartungspartner gestattet.
- Notebooks dürfen keinesfalls in Kraftfahrzeugen von außen sichtbar hinterlassen werden.
- Die Geräte sind bei Nichtnutzung grundsätzlich in gesicherten Räumen / Schränken zu verwahren.
- Notebooks sind auf Reisen als Handgebäck zu transportieren und dürfen nicht als reguläres Gepäckstück eingecheckt werden.
- Diebstähle sind unverzüglich zu melden. Darüber hinaus ist eine polizeiliche Anzeige zu erstatten und die Anzeigebestätigung zu übermitteln.
- Software Updates (speziell Betriebssystemseitige Sicherheitsupdates) sind regelmäßig, mindestens jedoch einmal pro Monat, durchzuführen. Damit die entsprechenden Aktualisierungsjobs ordnungsgemäß ausgeführt werden können, muss das überlassene Endgerät mindestens einmal pro Monat im Netzwerk des Vereins angemeldet sein (nicht über SIM-Karte).

5.8 Gesetzliche Anforderungen

- Die vom Verein überlassenen Geräte dürfen nur in rechtlich zulässiger Weise, insbesondere im Einklang zum aktuell geltenden Datenschutzrecht, betrieben werden. Beim Gebrauch der Geräte ist auf die Einhaltung geltender Gesetze zu achten (insbesondere das Datenschutzgesetz (DSGVO iVm DSAnpG 2018), das Strafgesetzbuch (StGB), Urheberrechtsgesetz (UrhG) und Verbotsgesetz (VbtG)). Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Verhaltensweisen bzw. Nutzung, einen Missbrauch darstellen:
    - Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB)
    - Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)
    - Missbräuchliches Abfangen von Daten (§ 119a StGB)
    - Missbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 StGB)
    - Datenbeschädigung (§ 126a StGB)
    - Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)
    - Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB)
    - Pornographische Darstellungen Minderjähriger (§ 207a StGB)
    - Nationalsozialistisches Gedankengut (§ 3h VbtG)

5.9 Speicherung von Daten

- Der bereitgestellte Festplattenspeicherplatz (interne PC, Notebookfestplatte inkl. SSD, externe Festplatten, Datensticks und optische Datenträger) ist ausschließlich der vereinsinternen Nutzung vorbehalten.
- Eine Nutzung des Speicherplatzes für private Zwecke ist nicht erlaubt.
- Die Einhaltung der Reglungen des Punktes „Allgemeine Sorgfaltspflichten" gilt ebenso für an das Gerät angeschlossene Datenträger.
- Ebenso können Daten im Cloudspeicherdienst von Microsoft, OneDrive for Business, der jedem Benutzer zur Verfügung steht, abgelegt werden.
- Andere Cloudspeicherdienste sind nicht lizenziert und dürfen daher nicht verwendet werden (z.B. Google Drive, Dropbox, etc.). Eine berufliche Nutzung dieser Clouddienste mit privaten Accounts stellt üblicherweise auch einen Verstoß gegen die Lizenzbestimmungen des Anbieters dar.
- Jeder Auftragnehmer ist für die Datensicherung lokal gespeicherter Daten (Betriebssystem, Anwendungssoftware und betriebliche Nutzdaten) eigenverantwortlich.
- Die Datensicherungsmedien sind physisch getrennt vom Endgerät aufzubewahren.
- Die Pflege von Daten auf Sharepoint, OneDrive oder auf einem Ordner des Fileservers hat datenschutzkonform und im Einklang von Vertraulichkeitsvereinbarungen zu erfolgen.
- Datenträger, die nicht mehr verwendet werden sollen od. dürfen, müssen vollständig unlesbar bzw. nicht wiederherstellbar gemacht werden.
- Datenträger unbekannter oder nicht vertrauenswürdiger Herkunft dürfen nicht an das überlassene Endgerät angeschlossen und ausgelesen werden.

5.10 E-Mail

- Das Öffnen von etwaigen datenschutzgefährdenden erscheinenden Anhängen ist stets zu hinterfragen und darf nur nach sorgsamer Abwägung der Sicherheitsrisiken ausgeführt werden (beispielsweise *.exe, *.bat und Makrodateien).

- E-Mails und Kontakte, die nicht mehr benötigt werden, müssen, nach Abwägung der Brauchbarkeit und des Vorliegens eines datenschutzkonformen Datenverarbeitungszwecks, gelöscht werden.

5.11 Internet Nutzung mit dem Browser

- Im Zuge der Nutzung eines Browsers ist darauf zu achten, dass sämtliche Sicherheitsrisiken, ausgehend vom Besuchen einer Website, vermieden werden können.
- Eine Installation von Add-Ons ist nur in Abstimmung mit dem Administrator erlaubt.

5.12 Mobiltelefone (gültig nur für vom Verein zur Verfügung gestellten Geräte)

- Die Nutzung von bereitgestellten Mobiltelefonen ist nur mit einem PIN Code und einem gerätespezifischen Sperrcode erlaubt.
- Auf allen Mobiltelefonen ist eine mit der Sperrcodefunktion versehene Bildschirmsperre (inaktivitäts- oder benutzerbedingt) einzurichten.
- Der Verlust bzw. Diebstahl eines bereitgestellten Mobiltelefons ist unverzüglich an das Leitungsorgan und an eine der in Punkt 2 „Ansprechpartner“ definierten Personen zu melden.
- Die Installation und Nutzung von mit der Arbeitsleistung zusammenhängenden und datenschutzkonformen Programmen (Apps) ist erlaubt.

5.13 Datenschutzübertretungen

- Im Falle eines Verdachts auf einen datenschutzrechtlichen Verstoß oder im Falle einer datenschutzrechtlich relevanten Antragstellung sind die in Punkt 2 „Ansprechpartner“ erwähnten Personen zur Wahrung der jeweiligen kurzen Fristen unverzüglich zu benachrichtigen.
- Im Falle einer weiterführenden Aufklärung sind die Mitarbeiter verpflichtet zusammenzuarbeiten und an der Sachverhaltsaufklärung mitzuwirken.

Ich bestätige, dass mir der Inhalt der Richtlinie „Richtlinie des Datenschutzes und der Vertraulichkeit von Informationen V2018-06“ bekannt gemacht wurde, ich den Inhalt der Richtlinie verstanden habe und ich die in der Richtlinie geregelten Pflichten einhalten werde.

Ort, Datum .....

Name .....

Adresse .....

Unterschrift .....