# → Datenschutzrichtlinie

## Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten bei PluSport Behindertensport Schweiz. Alle Mitarbeitenden, auch externe, Sportclubs-Verantwortliche und weitere autorisierte Personen mit Zugang zu den Informations-Systemen von PluSport (über App, Webschnittstellen etc.), sind zur Einhaltung dieser Richtlinie verpflichtet.

## Datenschutzverantwortliche:r

Die/der Datenschutzverantwortliche wird von der Geschäftsleitung bestimmt. Sie kann ebenso eine:n Datenschutzberater:in ernennen.

## Erheben, Verarbeiten und Nutzen personenbezogener Daten

PluSport Behindertensport Schweiz ist bemüht, sämtliche Personen- und Firmendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Da PluSport ein Sportverband für Menschen mit Beeinträchtigung ist, stehen alle Angestellten und Personen mit Zugriff auf unsere Datenbank (insbesondere Mitgliederverwaltung) und auf physische Dokumente in einer Vertrauensstellung und sind in ganz besonderem Masse zur Diskretion und zur vertraulichen Behandlung der ihnen anvertrauten Angelegenheiten verpflichtet.

Die Mitarbeitenden sind sich bewusst, dass ihnen bei der Ausführung der Arbeiten bei PluSport Daten, Unterlagen und Informationen von Mitgliedern, Vorständen und Leitenden der Sportclubs, Teilnehmenden und Leitenden von Sportcamps, Trainings, Events und Ausbildungskursen, Vorstands- und Kommissionsmitgliedern, Mitarbeitenden, Personen mit Bezug zur Mittelbeschaffung usw. zugänglich werden können, welche besonderen Geheimhaltungspflichten unterstehen und betreffend Angaben mit einem Bezug auf natürliche oder juristische Personen darüber hinaus besonders geschützt sind (durch das Bundesgesetz über den Datenschutz; https://www.admin.ch/opc/de/classified-compilation/19920153/index.html). Dies gilt auch für externe Personen mit Zugang zu den Informations-Systemen von PluSport.

Streng vertraulich zu behandeln sind folgende Informationen:

- **Personendaten, teilweise besonders schützenswerte Personendaten (von Mitarbeitenden, Kund:innen, Mitgliedern, Teilnehmenden etc.):** Persönliche Lebensverhältnisse (familiär, finanziell, etc.), Behinderungsart, Gesundheit/Krankheit, Intimsphäre, arbeitsvertragliche Daten (z.B. Gehalt), usw.
- **Firmendaten:** Geschäftsgeheimnisse (z.B. Ertragslage, Geschäftsbücher, Strategien, Kalkulationsunterlagen, Budgetdaten), Planungs- und Strategievorgaben, Computer-Passwörter, Zugriffsregelungen, Sicherheitsmassnahmen (z.B. Türcodes), Daten aus Datenbanken, Aufbewahrungsort von Tür- oder Schrankschlüsseln, usw.

## Selbstverpflichtung von externen autorisierten Personen

Externe Mitarbeitende, die mit Verträgen, im Mandat oder im Auftrag von PluSport arbeiten, Verantwortliche und Leitende in Sportclubs, Sportcamps oder Ausbildung und weitere autorisierte Personen, die Zugang zu Daten von PluSport haben, sind verpflichtet, sich an diese Datenschutzrichtlinie zu halten. PluSport informiert die entsprechenden Personen per Informationsschreiben, in Verträgen, Aufträgen etc.

## Selbstverpflichtung der Mitarbeitenden von PluSport

Alle Mitarbeitenden von PluSport Behindertensport Schweiz akzeptieren diese Datenschutzrichtlinie. Sie bestätigen damit, die oben erwähnten Personen- und Firmendaten vertraulich zu behandeln, Informationen und Unterlagen nur zur Ausführung der ihnen erteilten Aufträge zu verwenden und nicht berechtigten Personen in keiner Art und Form, weder ganz noch auszugsweise, zugänglich zu machen. Auch ausserhalb des Arbeitsumfeldes – also privat an Partner:in, Angehörige oder Bekannte – dürfen keine Informationen weitergegeben werden.
Die Mitarbeitenden werden ihre Vorgesetzten unaufgefordert auf Schwachstellen oder Lücken bzgl. Datenschutz und Informationssicherheit innerhalb von PluSport hinweisen, welche sie im Rahmen des Arbeitsverhältnisses feststellen.

Die Mitarbeitenden wissen, dass die unbefugte Verwendung und Bekanntgabe von geheim zu haltenden oder vertraulich zu behandelnden Unterlagen und Informationen, die ihnen bei PluSport zugänglich werden während des ihnen erteilten Auftrages bzw. ihrer Anstellung, nach den Bestimmungen des schweizerischen Gesetzes mit Strafe bedroht sind und u.U. eine arbeitsrechtliche Sanktion bis hin zur fristlosen Kündigung des Arbeitsverhältnisses zur Folge haben können. Die Verletzung der beruflichen Schweigepflicht ist in Art. 35 DSG geregelt.* Die Geheimhaltungspflicht gilt auch nach Beendigung des Auftrags bzw. der Anstellung. Daten aus Informationssystemen von PluSport dürfen nicht auf private Datenträger gespeichert und behalten werden. Jeder Missbrauch der IT-Mittel ist untersagt. Ein Missbrauch kann dabei in qualitativer oder quantitativer Hinsicht erfolgen. Der Privatgebrauch von IT-Mitteln (auch Kopierern, Druckern, Laptops etc.) ist nach Rücksprache und allenfalls gegen Entschädigung erlaubt. Dies ändert jedoch nichts an der Zugriffsmöglichkeit auf die Daten durch PluSport.

*Art. 35 DSG (Verletzung der beruflichen Schweigepflicht)

1 Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, wird auf Antrag mit Busse bestraft.

2 Gleich wird bestraft, wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

3 Das unbefugte Bekanntgeben geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

## Zugriff auf Mailbox bei Austritt oder Krankheit/Unfall von Mitarbeitenden

Zusätzlich zum Schutz der Personen- und Firmendaten ist der Schutz der Privatsphäre sowie die Verwendung des E-Mail-Accounts der Angestellten von PluSport genauso wichtig. Nachfolgende Punkte regeln die Verwaltung der Mailbox von Mitarbeitenden bei der Beendigung des Arbeitsverhältnisses oder bei Abwesenheit in Folge von Krankheit oder Unfall.

- Vor dem geplanten Austritt der Angestellten sollen diese die noch laufenden Geschäfte und E-Mails intern an die zuständige Person übergeben (Vorgesetzte, Stellvertretung oder Nachfolger:in).

- Die Mitarbeitenden bestätigen die Übergabe sämtlicher Geschäftsdokumente an die zuständige Person spätestens beim ordentlichen Austrittsgespräch.
- Die austretenden Mitarbeitenden haben die Möglichkeit, ihre privaten E-Mails, Daten und Dokumente auf private Datenträger (z.B. USB-Stick oder externe Festplatte) zu speichern und von den Servern der Arbeitgeberin zu löschen. Wird dies nicht gemacht, löscht die Arbeitgeberin diese Daten nach Austritt der Angestellten nach spätestens 3 Monaten.
- Umgehend nach dem letzten Arbeitstag werden die E-Mail-Accounts der austretenden Mitarbeitenden sowie auch alle anderen IT-Accounts und deren Mailbox gesperrt (Passwort wird seitens Arbeitgeberin geändert). Nach rund 2 bis 3 Monaten werden diese Accounts deaktiviert oder gelöscht.
- Bei einer fristlosen Kündigung, Freistellung oder im Todesfall wird der E-Mail-Account der betroffenen Mitarbeitenden sofort gesperrt. Anschliessend können nötigenfalls die privaten E-Mails und sonstigen privaten Daten (im Todesfall unter Beizug der Angehörigen des/der Verstorbenen) nach dem 4-Augen-Prinzip ausgesondert werden.
- Absender, die E-Mails an die gesperrte E-Mail-Adresse senden, nachdem der/die Mitarbeitende PluSport verlassen hat, werden automatisch informiert, dass die Empfängeradresse hinfällig geworden ist (Outlook-Abwesenheitsmeldung). In der automatischen Antwort wird eine geeignete Ersatz-E-Mail-Adresse angegeben, oder es erfolgt eine automatische Weiterleitung auf eine andere E-Mail-Adresse des Bereichs.
- Die Geschäftsleitung ist ausnahmsweise und – wenn aus betrieblicher Sicht nötig – autorisiert, auf die Geschäfts-Mailbox einer wegen Krankheit oder Unfall abwesenden Person zuzugreifen und die E-Mails durch von ihr autorisierte Personen bearbeiten zu lassen. Als privat bezeichnete E-Mails/Daten werden dabei nicht gesichtet oder bearbeitet, es sei denn, die abwesende Person gibt dazu ihre Erlaubnis.

## EDV- und Datensicherheit

Die EDV- und Datensicherheit verfolgt das Ziel, im Prozess der Datenverarbeitung vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung der Daten zu schützen.
PluSport gewährleistet, dass insbesondere

- der Zugriff auf die Daten und somit deren Kenntnisnahme ausschliesslich durch autorisierte Benutzer:innen erfolgt (Passwortschutz, Benutzerrechteverwaltung, geschützte Bildschirmschoner auf Computern etc.). Es darf kein PluSport-Passwort auf privaten Geräten gespeichert werden, es sei denn, dass eine Arbeitssitzung erstellt wird, die ausschliesslich der Arbeit zuhause gewidmet ist oder der Zugriff auf die Daten via PluSport-App erfolgt; das Gleiche gilt für die Modifikation (Ändern und Löschen) von Daten,
- sensible Daten nicht unbemerkt verändert werden können, sondern Änderungen nachvollziehbar sind,
- der Zugriff auf Daten innerhalb eines festgelegten Zeitraums für entsprechend autorisierte Nutzer:innen gewährleistet ist und die Funktionalität der IT-Systeme nicht beeinträchtigt ist.

Die Mitarbeitenden haben die Pflicht, verdächtige Beobachtungen oder Feststellungen unverzüglich mitzuteilen. Verdächtige Webseiten, E-Mails etc. dürfen nicht geöffnet werden. Die Mitarbeitenden sind angewiesen, ausschliesslich nur von PluSport bezeichnete oder zur Verfügung gestellte IT-Mittel (Cloud-Dienste, Anwendungen etc.) zu nutzen. Zum Schutz der Daten- und EDV-Sicherheit oder auf behördliche Anordnung kann die Geschäftsleitung Datenaufzeichnung und -auswertung anordnen. Dabei werden personenbezogene Datenaufzeichnungen als sensitive Daten behandelt. Die Mitarbeitenden sind sich bewusst, dass auch private Daten davon betroffen sein können, falls insbesondere Computer zu privaten Zwecken verwendet werden.
Die elektronischen Daten werden bei PluSport durch einen externen Dienstleister (Dynawell, Bassersdorf) professionell verwaltet und gesichert. Die Verwaltung unserer Serverstruktur beinhaltet:

- Garantierte Datenhaltung in der Schweiz
- Gesichertes, klimatisiertes Datacenter
- Beschaffung, Installation und Inbetriebnahme der Server

- Nachhaltige Software und Hardware Maintenance
- Security-, Update- und Patching Services
- 7x24h Monitoring und Alerting der Server-Infrastruktur
- Multilayer Spam- und Virenschutz
- Network Security (LAN, WAN, WLAN, DMZ)
- Firewall & Backup Services
- etc.

Dieses Reglement wurde vom Vorstand genehmigt und tritt per 31. Januar 2021 in Kraft. Die Geschäftsleitung behält sich vor, einzelne Bestimmungen oder das ganze Reglement jederzeit zu ändern. Änderungen werden den betroffenen Personen zur Kenntnis gebracht.

31.3.2022