→ Direttiva sulla protezione dei dati

Ambito di validità

La presente direttiva regola il trattamento delle informazioni conforme alla protezione dei dati e le relative responsabilità di PluSport Sport Andicap Svizzera. Tutti i collaboratori, compresi gli esterni, i responsabili dei club sportivi e altre persone autorizzate con accesso ai sistemi informativi di PluSport (tramite app, interfacce web, ecc.), sono tenuti a rispettare la presente direttiva.

Responsabile della protezione dei dati

Il responsabile della protezione dei dati è nominato dalla Direzione, che può anche nominare un consulente per la protezione dei dati.

Raccolta, trattamento e uso dei dati personali

PluSport Sport Andicap Svizzera si impegna a proteggere tutti i dati personali e aziendali da un trattamento non autorizzato mediante misure tecniche e organizzative adeguate. Poiché PluSport è un'associazione sportiva per persone con disabilità, tutti i dipendenti e le persone che hanno accesso alla nostra banca dati (in particolare l'amministrazione dei membri) e ai documenti fisici sono in una posizione di fiducia e sono tenuti a mantenere particolare discrezione e a trattare con riservatezza le questioni affidate loro.

I collaboratori sono consapevoli che, nello svolgimento del lavoro per PluSport, possono avere accesso a dati, documenti e informazioni relative a membri, responsabili e monitori dei club sportivi, partecipanti e monitori di campi sportivi, allenamenti, eventi e corsi di formazione, membri del Comitato e delle commissioni, collaboratori, persone coinvolte nella raccolta di fondi ecc., che sono soggetti a particolari obblighi del segreto e che, nel caso di informazioni relative a persone fisiche o giuridiche, sono anche soggetti a una protezione speciale (ai sensi della legge federale sulla protezione dei dati; https://www.admin.ch/opc/it/classified-compilation/19920153/index.html). Questo vale anche per le persone esterne con accesso ai sistemi informativi di PluSport.

Le seguenti informazioni devono essere trattate in modo strettamente confidenziale:

- **Dati personali, in alcuni casi dati personali particolarmente sensibili (di collaboratori, clienti, membri, partecipanti, ecc.):** circostanze personali (familiari, finanziarie, ecc.), tipologia di disabilità, salute/malattia, privacy, dati sull'occupazione (ad es. stipendio), ecc.
- **Dati aziendali:** segreti commerciali (ad es. situazione di reddito, libri contabili, strategie, documenti di calcolo dei costi, dati relativi al budget), direttive di pianificazione e strategia, password dei computer, regolamenti di accesso, misure di sicurezza (ad es. codici delle porte), dati dalle banche dati, luoghi di conservazione delle chiavi di porte o armadi, ecc.

Impegno volontario di persone autorizzate esterne

I collaboratori esterni che lavorano sotto contratto, mandato o per conto di PluSport, responsabili e monitori di club sportivi, campi sportivi o formazione e altre persone autorizzate

che hanno accesso ai dati di PluSport sono tenuti a rispettare la presente direttiva sulla protezione dei dati. PluSport informa le persone interessate tramite lettera informativa, nei contratti, ordini, ecc.

Impegno volontario dei collaboratori di PluSport

Tutti i collaboratori di PluSport Sport Andicap Svizzera accettano la presente direttiva sulla protezione dei dati. I collaboratori confermano quindi di trattare i suddetti dati personali e aziendali in modo confidenziale, di utilizzare le informazioni e i documenti solo per l'esecuzione degli ordini a loro trasmessi e di non renderli accessibili a persone non autorizzate in nessun modo o forma, né in tutto né in parte. Le informazioni non possono nemmeno essere trasmesse al di fuori dell'ambiente di lavoro, e cioè privatamente a partner, parenti o conoscenti.
I collaboratori informeranno spontaneamente i loro superiori in merito a eventuali criticità o lacune nella protezione dei dati e nella sicurezza delle informazioni all'interno di PluSport, constatate nell'ambito del loro rapporto di lavoro.

I collaboratori sono consapevoli che l'utilizzo non autorizzato e la divulgazione di documenti e informazioni che devono essere tenuti segreti o trattati in modo confidenziale e a cui ottengono accesso presso PluSport nel corso del loro mandato o impiego sono punibili secondo le disposizioni delle leggi svizzere e possono eventualmente comportare sanzioni secondo il diritto del lavoro, fino alla risoluzione del rapporto di lavoro senza preavviso. La violazione del dovere di discrezione è regolata dall'articolo 35 della DPA*. L'obbligo del segreto si applica anche dopo la fine del mandato o dell'impiego. I dati dei sistemi informativi di PluSport non possono essere memorizzati e conservati su supporti dati privati. Qualsiasi uso improprio delle risorse informatiche è proibito. L'abuso può essere qualitativo o quantitativo. L'uso privato di strumenti informatici (comprese fotocopiatrici, stampanti, computer portatili, ecc.) è consentito previa consultazione e, se necessario, dietro pagamento. Tuttavia, questo non cambia la possibilità di accesso ai dati da parte di PluSport.

*Art. 35 Violazione dell'obbligo di discrezione

[1] Chiunque intenzionalmente rivela in modo illecito dati personali segreti e degni di particolare protezione o profili della personalità, dei quali è venuto a conoscenza nell'esercizio di una professione che richiede la conoscenza di tali dati, è punito, a querela di parte, con la multa.

[2] È passibile della stessa pena chiunque intenzionalmente rivela in modo illecito dati personali segreti e degni di particolare protezione o profili della personalità, dei quali è venuto a conoscenza nell'ambito dell'attività svolta per conto della persona astretta all'obbligo del segreto o in occasione della sua formazione presso tale persona.

[3] La rivelazione illecita di dati personali segreti e degni di particolare protezione o di profili della personalità è punibile anche dopo la cessazione dei rapporti di lavoro o di formazione.

Accesso alla casella di posta elettronica in caso di uscita o malattia/incidente del collaboratore

Oltre a proteggere i dati personali e aziendali, proteggere la privacy e l'uso degli account di posta elettronica dei dipendenti di PluSport è altrettanto importante. I seguenti punti regolano la gestione delle caselle di posta dei collaboratori in caso di cessazione del rapporto di lavoro o di assenza per malattia o incidente.

- Prima dell'uscita programmata del dipendente, questo dovrebbe consegnare internamente le attività ancora in corso e le e-mail alla persona responsabile (superiore, vice o successore).
- I collaboratori confermano che tutti i documenti aziendali sono stati consegnati alla persona responsabile al più tardi durante il regolare colloquio di uscita.

- I collaboratori in uscita hanno la possibilità di salvare le loro e-mail private, i dati e i documenti su supporti dati privati (ad esempio una chiavetta USB o un disco rigido esterno) e di cancellarli dai server del datore di lavoro. Se questo non viene fatto, il datore di lavoro cancella questi dati dopo l'uscita del dipendente al più tardi dopo tre mesi.
- Immediatamente dopo l'ultimo giorno di lavoro, gli account di posta elettronica dei collaboratori uscenti, così come tutti gli altri account IT e le loro caselle di posta vengono bloccati (la password viene cambiata dal datore di lavoro). Dopo circa due o tre mesi, questi account vengono disattivati o cancellati.
- In caso di licenziamento senza preavviso, sospensione o decesso, l'account e-mail del collaboratore interessato sarà bloccato immediatamente. Successivamente, se necessario, le e-mail private e altri dati privati (in caso di decesso con il coinvolgimento dei parenti del defunto) possono essere eliminati secondo il principio del doppio controllo.
- I mittenti che inviano e-mail all'indirizzo e-mail bloccato dopo che il collaboratore ha lasciato PluSport sono automaticamente informati che l'indirizzo del destinatario non è più valido (messaggio di assenza Outlook). Nella risposta automatica viene fornito un indirizzo di posta elettronica sostitutivo adeguato o viene effettuato un inoltro automatico a un altro indirizzo di posta elettronica del settore.
- La Direzione è eccezionalmente autorizzata, se necessario da un punto di vista operativo, ad accedere alla casella di posta elettronica aziendale di una persona assente per malattia o incidente e a far elaborare le e-mail da persone da essa autorizzate. Le e-mail/I dati designati come privati non saranno visualizzati o elaborati a meno che la persona assente non dia il permesso.

Sicurezza informatica e dei dati

La sicurezza informatica e dei dati perseguono l'obiettivo di proteggere, nel processo di elaborazione dei dati, da perdita, distruzione, falsificazione, presa di conoscenza non autorizzata ed elaborazione infondata dei dati.
PluSport assicura in particolare che

- l'accesso ai dati e quindi la loro presa di conoscenza sono limitati agli utenti autorizzati (protezione con password, gestione dei diritti degli utenti, salvaschermo protetti sui computer, ecc.). Nessuna password PluSport può essere memorizzata su dispositivi privati, a meno che non si crei una sessione di lavoro dedicata esclusivamente al lavoro da casa o si acceda ai dati tramite l'app PluSport. Lo stesso vale per la modifica (cambio e cancellazione) dei dati;
- i dati sensibili non possono essere cambiati senza segnalare la modifica, ma i cambiamenti sono tracciabili;
- l'accesso ai dati è garantito entro un determinato periodo di tempo per gli utenti debitamente autorizzati e la funzionalità dei sistemi informatici non è compromessa.

I collaboratori hanno l'obbligo di segnalare immediatamente osservazioni o constatazioni sospette. Pagine Web, e-mail ecc. sospette non devono essere aperte. I collaboratori sono istruiti a utilizzare solo le risorse IT designate o fornite da PluSport (servizi cloud, applicazioni, ecc). Al fine di proteggere la sicurezza dei dati e dell'elaborazione elettronica dei dati o su ordine delle autorità, la Direzione può disporre la registrazione e l'analisi dei dati. In tal senso, le registrazioni di dati personali sono trattate come dati sensibili. I collaboratori sono consapevoli che anche i dati privati possono esserne interessati se, in particolare, i computer vengono utilizzati per scopi privati.
I dati elettronici sono gestiti e protetti in modo professionale presso PluSport da un fornitore di servizi esterno (Dynawell, Bassersdorf). La gestione della nostra struttura di server comprende:

- Archiviazione dei dati garantita in Svizzera
- Data center protetto e con aria condizionata
- Fornitura, installazione e messa in funzione dei server
- Manutenzione sostenibile di software e hardware
- Servizi di sicurezza, aggiornamento e patching
- Monitoraggio e allerta dell'infrastruttura server sette giorni su sette, 24 ore su 24

- Protezione multilivello contro lo spam e i virus
- Sicurezza di rete (LAN, WAN, WLAN, DMZ)
- Servizi di firewall e backup
- ecc.

Il presente regolamento è stato approvato dal Comitato ed entrerà in vigore il 31 gennaio 2021. La Direzione si riserva il diritto di modificare singole disposizioni o l’intero regolamento in qualsiasi momento. Le modifiche sono notificate alle persone interessate.

31.3.2022