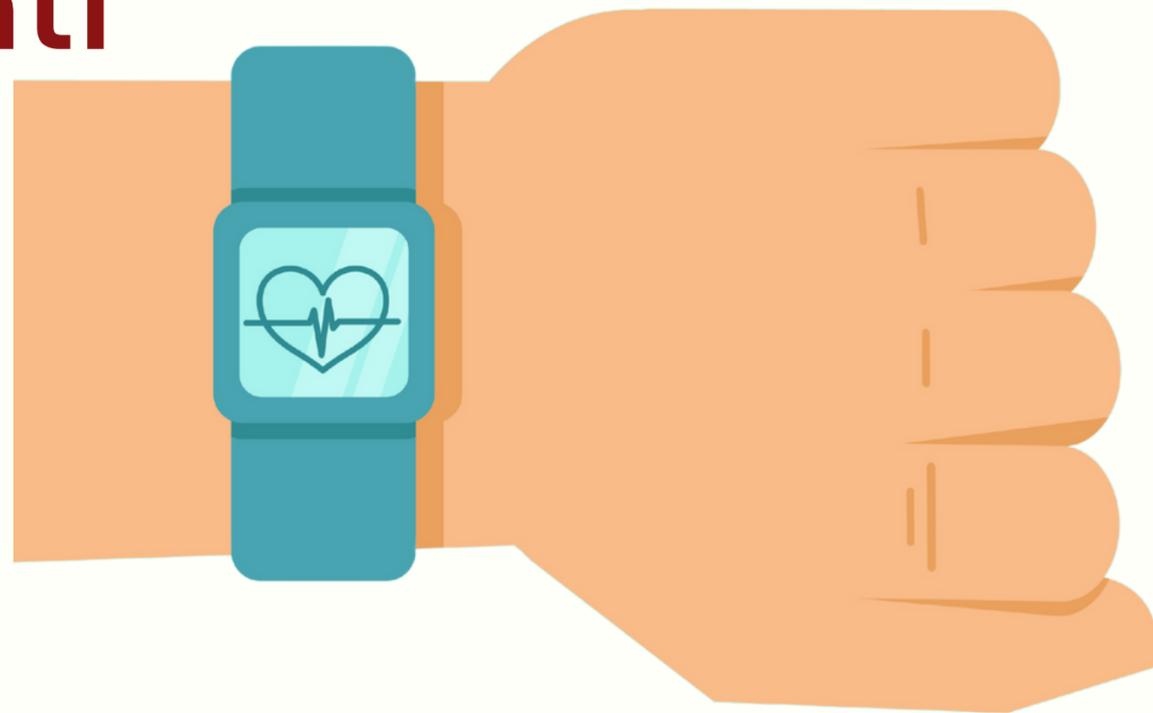


# App e dispositivi fitness tracker e protezione dei dati personali

## I suggerimenti del Garante



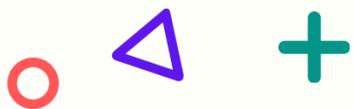
La scheda ha finalità meramente divulgative e sarà aggiornata  
in base agli sviluppi tecnologici e normativi

Le app e i dispositivi di tipo “fitness tracker” misurano le prestazioni sportive (rilevando ad esempio i passi fatti, la distanza percorsa in bicicletta o di corsa, le calorie consumate durante una determinata attività fisica, ecc.) e monitorano e registrano alcuni parametri di stato psicofisico (ad esempio, il battito cardiaco, la pressione sanguigna, il livello di stress, le ore dormite, la quantità di acqua bevuta, il peso, le calorie e le tipologie di cibo mangiate).

**Si tratta di ausili utili per tentare di mantenere un buono stato di forma o per migliorare le performance sportive. Tuttavia occorre sempre ricordare che tali strumenti:**

- ✓ **sono in grado di raccogliere moltissimi dati, anche di natura sensibile**, cioè riferiti al nostro stato psicofisico e di salute, che potrebbero anche essere trasmessi a terzi per finalità non sempre conosciute. Inoltre, app e dispositivi fitness tracker hanno funzioni di geolocalizzazione che possono tracciare la nostra posizione e i nostri spostamenti in un preciso momento e nel tempo.
- ✓ **sono integrati nell’Internet delle cose (IoT)**, sono cioè capaci di dialogare e scambiare dati con altre app e altri dispositivi come il pc lo smartphone. Ciò aumenta le possibilità di trattamento e diffusione dei dati personali raccolti da tali strumenti, per finalità e con modalità di cui non sempre siamo consapevoli. Potrebbe anche accadere che il fitness tracker raccolga a sua volta dati da altri dispositivi (computer, smartphone, ecc.) e app con cui è interconnesso.
- ✓ **Hanno una spiccata “vocazione social”**, cioè possiedono funzionalità che consentono di condividere obiettivi, sfide e risultati con altri utenti, spesso sconosciuti.

**E’ quindi bene utilizzare questi supporti con consapevolezza e adottando possibilmente alcune importanti accortezze.**



# Leggi bene l'informativa

**Cerca di capire quanti e quali dati verranno raccolti e come verranno utilizzati, consultando l'informativa sul trattamento di dati personali.**

**In particolare verifica:**

- chi tratterà i tuoi dati personali e con quali finalità
- per quanto tempo verranno conservati i dati personali che ti riguardano
- se possono essere condivisi con terze parti per finalità commerciali o di altro tipo.

**L'informativa dovrebbe essere sempre disponibile:**

- nella confezione del dispositivo
- sul sito web del produttore del dispositivo
- sul sito web della app o nel market da cui viene scaricata



# Minimizza il trattamento dei dati

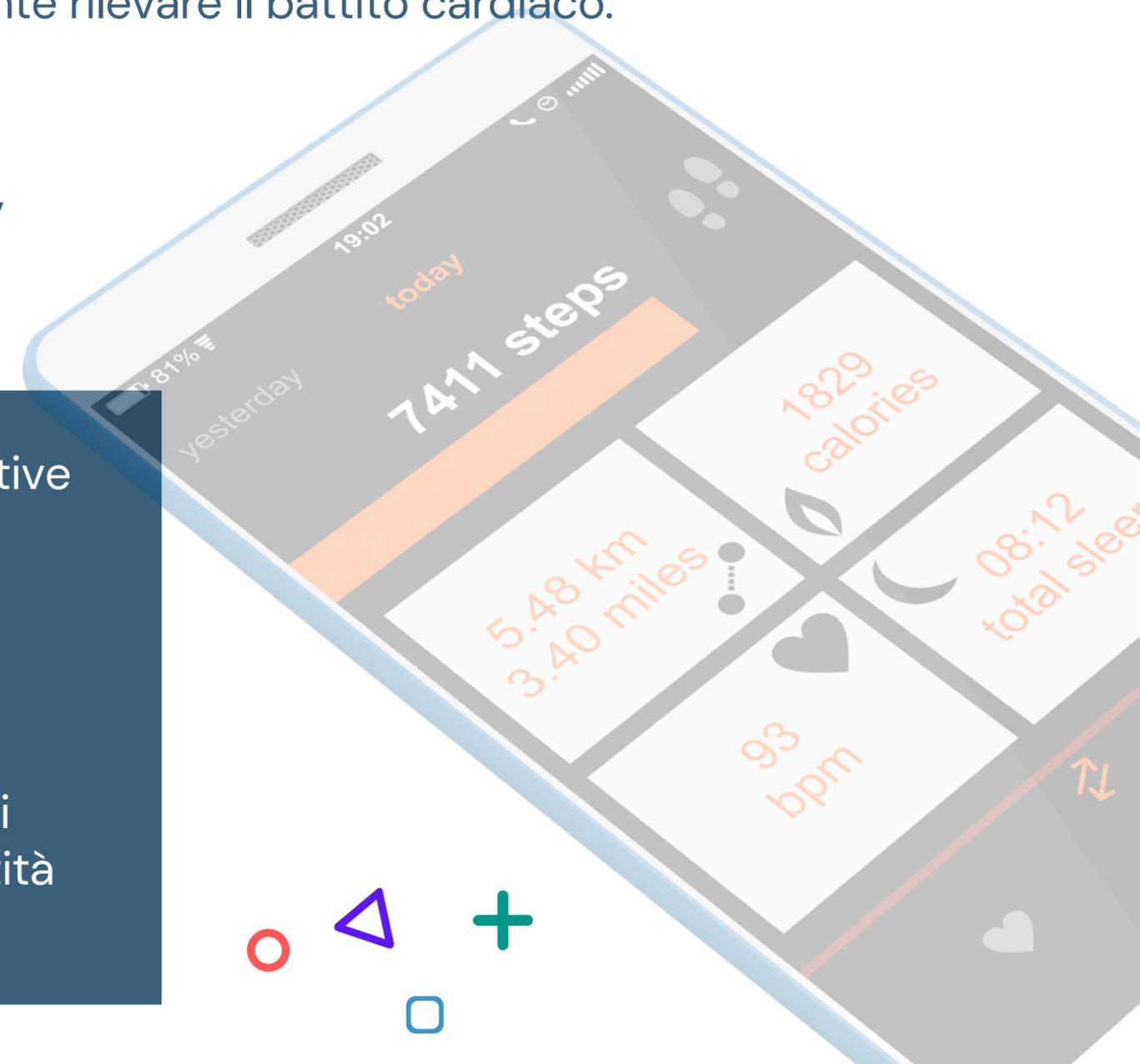
Verifica quali e quanti dati siano assolutamente **indispensabili** per il normale funzionamento della app o del dispositivo di monitoraggio.

Ad esempio, puoi scegliere di tenere traccia della durata seduta di corsa o bicicletta e la distanza percorsa, anche senza necessariamente rilevare il battito cardiaco.

Inoltre, potresti **disattivare** alcune funzioni non essenziali in una comune attività di fitness (vale a dire, non professionistica): come, ad esempio le funzioni per monitorare il sonno, i pasti, ecc.

Se per il **download** dell'app di monitoraggio delle prestazioni sportive e/o per la sua installazione è prevista la creazione di un profilo personale, prova a fornire solo i dati **strettamente** necessari all'attivazione del servizio.

**Se possibile usa uno pseudonimo:** in questo modo, nel caso di condivisione social dei tuoi dati, puoi limitare la possibilità che altri utenti, o in genere soggetti terzi, associno facilmente alla tua identità reale le informazioni sulle tue prestazioni o sulla forma fisica.



# Prudenza con le connessioni

Il dispositivo e/o la app fitness tracker possono richiedere la connessione con altri **device** (ad esempio, lo smartphone) o altre **app** (ad esempio, quelle per il monitoraggio di base dell'attività fisica a volte installate di *default* negli smartphone). Ciò può comportare una ulteriore potenziale diffusione e un trattamento di dati personali, che è invece sempre bene evitare o almeno limitare.

Se la connessione ad altri dispositivi **non è indispensabile** al funzionamento del dispositivo o della app, **non concedere l'autorizzazione**. In caso contrario:

- ✓ limita in ogni caso al minimo la condivisione di dati;
- ✓ cerca di leggere bene l'informativa nella parte relativa alla condivisione di dati.

Se possibile, **non** permettere l'accesso di app e dispositivi fitness tracker ad alcuni dati presenti sullo smartphone, sul computer o in altre app che non sono strettamente necessari al tracciamento dell'attività sportiva (come i contatti in rubrica, le foto, l'agenda o il microfono).

In generale, **limita** il più possibile le condivisioni di dati: anche perché eventuali malintenzionati potrebbero usare vulnerabilità nelle connessioni per cercare di veicolare **virus** e **malware**, sottrarre dati personali o prendere il controllo di alcuni dispositivi (compresi quelli domotici).



# Non dire tutto a tutti

Se decidi di attivare le funzioni di condivisione social di obiettivi, risultati e, in generale, di dati sul tuo stato di forma psico-fisica, valuta sempre con attenzione quali informazioni stai rendendo accessibili e a chi.

Se possibile, limita il numero di informazioni condivise e seleziona gli utenti che potranno visualizzarle (ad esempio, solo amici e conoscenti).

Soprattutto fai attenzione a non diffondere in modalità social, volontariamente o involontariamente, dati delicati, come quelli da cui si può desumere lo stato di salute o sulla geolocalizzazione.

Immagina ad esempio i rischi insiti nel diffondere pubblicamente informazioni da cui si possono desumere eventuali problemi fisici, oppure sui percorsi che si è soliti fare di corsa o in bicicletta, rendendo quindi noto il tragitto e gli orari e i giorni in cui si è lontani da casa.



# Attenzione alla sicurezza

Per utilizzare dispositivi ed app con maggiore sicurezza, puoi adottare alcune semplici accortezze di base, sempre valide nell'utilizzo di strumenti tecnologici, come:

- ✓ impostare **password** di accesso complesse e sicure;
- ✓ **aggiornare** periodicamente la app alle nuove versioni, che contengono di solito anche miglioramenti sul fronte della sicurezza;
- ✓ impostare una **autenticazione** di accesso a più fattori;
- ✓ installare sul dispositivo dove sono collocate le app un **software antivirus** in grado di proteggere anche i dati personali da eventuali violazioni;
- ✓ scaricare le app tramite **siti web e market ufficiali**.

Se **connetti app e dispositivi tramite Bluetooth o wi-fi**, ricorda che eventuali malintenzionati potrebbero sfruttare eventuali falle di sicurezza per accedere alle tue informazioni o addirittura prendere il controllo dei dispositivi. Quindi, ad esempio:

- ✓ **disconnetti** il dispositivo e, in generale, **spegni** il Bluetooth quando non li usi;
- ✓ **connetti** il tuo dispositivo a una rete wi-fi **solo** se sei certo degli standard di sicurezza adottati contro virus e rischi di intrusione. Evita dunque connessioni pubbliche che non puoi verificare, come quelle di palestre, centri sportivi, spiagge, bar, ristoranti, ecc..

# Cancella i dati

Se possibile, **cancella periodicamente i dati raccolti dal dispositivo e dalla app**, considerando anche quelli eventualmente trasmessi ad un altro dispositivo (ad esempio lo smartphone).

Laddove previsto, accedi al sito web cui fanno riferimento ed **elimina** i dati relativi al tuo **profilo utente**.

# Se non lo usi, spegnilo

Chiediti se per te è assolutamente indispensabile indossare e tenere acceso il dispositivo fitness tracker 24 ore su 24.

Se non lo vuoi spegnere, come nel caso dei braccialetti utilizzabili anche come orologi da polso, puoi almeno decidere di disattivare alcuni sensori e/o alcune funzioni di rilevamento.

# Tutela i minori

In generale, è meglio **evitare** che i minori possano utilizzare dispositivi e app per il monitoraggio delle prestazioni sportive: almeno non da soli. I più piccoli, infatti, sono meno consapevoli e più esposti al rischio di una raccolta e diffusione incontrollata di dati personali.



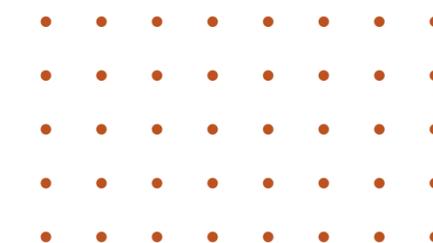
# Non dare via i tuoi dati

Nel caso in cui decidessi di vendere o regalare il tuo dispositivo fitness tracker, o comunque di liberartene, ricorda di disattivare l'account personale creato per l'utilizzo e di provvedere alla **cancellazione** di tutti i dati eventualmente registrati nel dispositivo e sulla app.

Se non usi più una app sportiva, **disinstallala** dallo smartphone e verifica che contemporaneamente siano **cancellati** tutti i dati che ha raccolto, **sia in locale** (cioè nel dispositivo o nella app) **che sulla piattaforma** del fornitore della app e dei servizi collegati.

Informati anche se i tuoi dati siano eventualmente conservati sui server dell'azienda che produce il dispositivo o l'app fitness tracker ed eventualmente chiedi la **cancellazione**.





# Impara a difenderti

Il Regolamento UE/2016/679 in materia di protezione dati prevede che i sistemi elettronici siano prodotti e configurati per ridurre al minimo la raccolta e il trattamento di dati personali (**privacy by design e privacy by default**).

I dati devono inoltre essere trattati in modo trasparente nei confronti dell'interessato (**principio di trasparenza**) e adeguati, pertinenti e limitati a quanto previsto dalla finalità (**principio di minimizzazione**).

Tali principi debbono essere conosciuti e rispettati dai produttori di dispositivi digitali e dai fornitori di servizi di comunicazione ed eventualmente certificati.

E' però sempre importante ricordare che le prime e più importanti linee di difesa da possibili violazioni della nostra privacy sono la **consapevolezza** nell'uso delle tecnologie e l'**accortezza** nel diffondere i nostri dati personali.

Per maggiori informazioni, è possibile consultare anche la sezione **Diritti** del sito web [www.gpdp.it](http://www.gpdp.it) e le **pagine tematiche** del Garante. È inoltre possibile rivolgersi per informazioni, chiarimenti o segnalazioni all'**Ufficio Relazioni con il Pubblico (URP) del Garante**.

