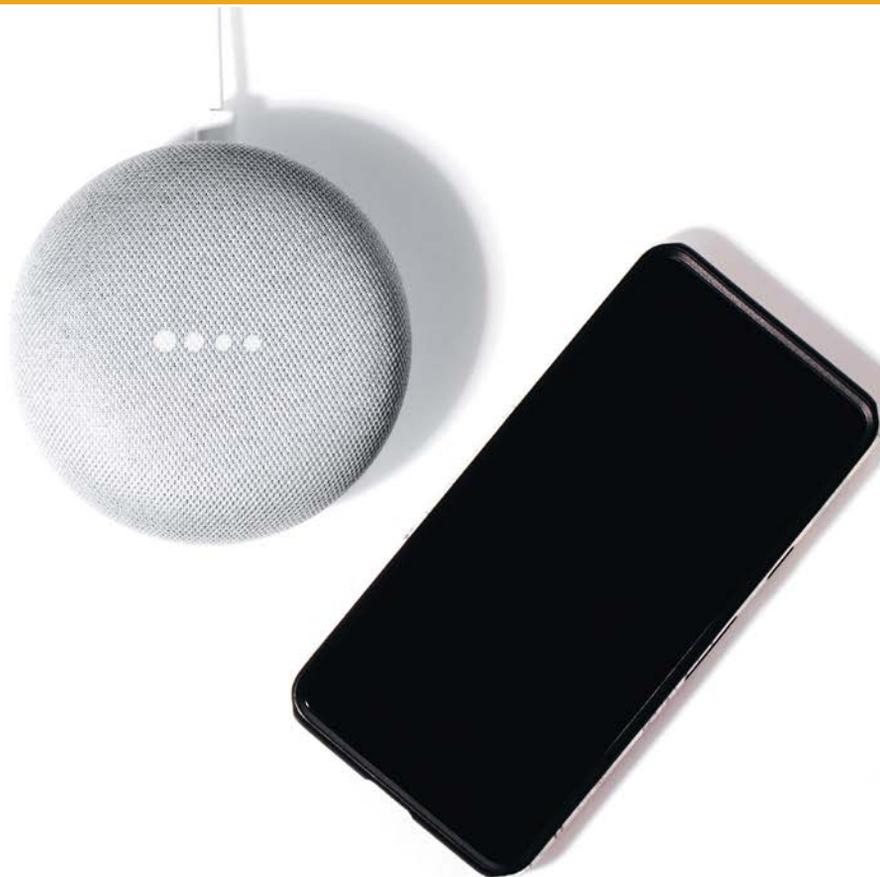


**GPDP****GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Assistenti digitali (smart assistant) I consigli del Garante per un uso a prova di privacy

L'assistente digitale (o smart assistant) è un programma che interpreta il linguaggio naturale tramite **algoritmi di intelligenza artificiale** ed è in grado di dialogare con gli esseri umani al fine di soddisfare diversi tipi di richieste (ad esempio: rispondere direttamente a richieste di informazioni, fare ricerche su Internet, ricercare e indicare percorsi stradali, ecc.) o compiere determinate azioni (ad esempio: fare un acquisto online, regolare la temperatura o l'illuminazione di un'abitazione, chiudere o aprire serrature di case o automobili intelligenti, attivare elettrodomestici come la lavatrice, ecc.).

Questa tecnologia è ormai molto diffusa e viene installata su vari dispositivi (la troviamo nei nostri smartphone, nelle auto, nelle case sotto forma di «altoparlanti intelligenti»).



Gli assistenti digitali possono raccogliere e memorizzare una grande quantità di dati personali - non solo relativi all'utente diretto, ma a chiunque si trovi nello stesso ambiente - riguardanti, ad esempio:

- **scelte, preferenze e abitudini** relative a stili di vita, consumi, interessi, ecc.;
- **caratteristiche biometriche**, come ad esempio quelle della voce e del volto, se dotati di videocamera;
- **geolocalizzazione** (posizione, percorsi abituali o frequenti, domicilio, indirizzo del posto di lavoro, ecc);
- **numero e caratteristiche** (età, sesso, ecc.) delle persone che si trovano nell'ambiente in cui operano;
- **stati emotivi**.

E' quindi opportuno cercare di fare un uso informato e consapevole di questi strumenti, per tutelare in modo adeguato i nostri dati personali e quelli di tutte le persone che entrano, volontariamente o meno, nel campo di azione degli assistenti digitali.

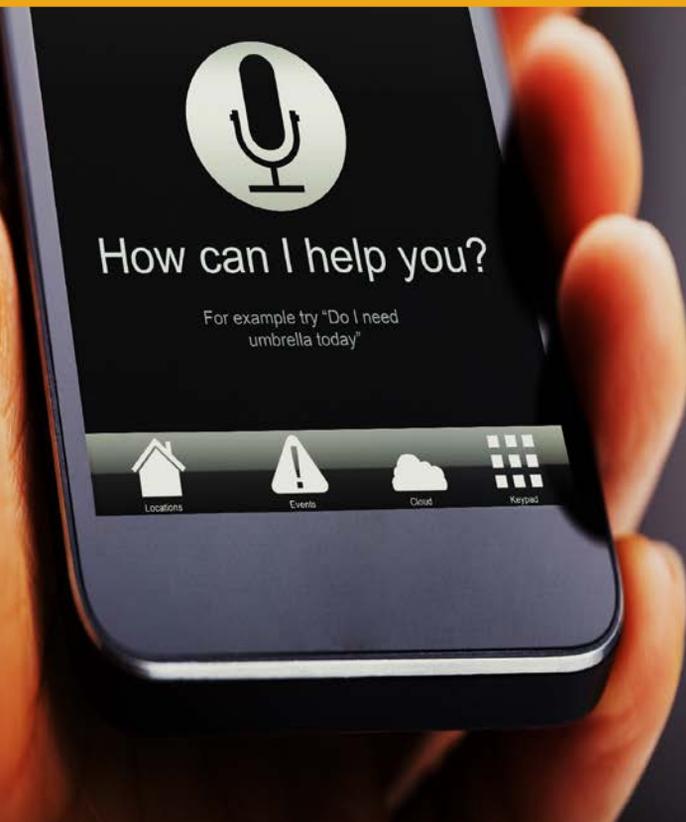


**Informati
sempre su
come
vengono
trattati
i tuoi dati**

Se per **attivare l'assistente digitale o le eventuali app di gestione** è necessario registrarsi fornendo dati personali, è **bene leggere con attenzione l'informativa sul trattamento dei dati personali**, che deve sempre essere disponibile, ad esempio sul sito dell'azienda che offre il servizio o nella confezione del dispositivo in cui è installato lo smart assistant (smartphone, altoparlante intelligente, ecc.).

In particolare, è importante cercare di comprendere

- **quali e quante informazioni** saranno acquisite direttamente dall'assistente digitale (ad esempio, tramite microfono e/o videocamera);
- **come potrebbero essere utilizzati o trasferiti a terzi i dati raccolti** (solo per far funzionare lo strumento o anche per altre finalità);
- **chi e come potrebbe ricevere i dati raccolti** e se sono previsti, per qualsiasi ragione, **accessi «in diretta» al microfono** e alla videocamera dello smart assistant da parte di addetti della società che lo ha prodotto o della società che gestisce i servizi offerti dallo smart assistant;
- **dove** sono conservati questi dati e per quanto tempo.



Non dire troppe cose al tuo smart assistant

Nel momento in cui si attiva per la prima volta lo smart assistant è meglio fornire solo le informazioni specificamente necessarie per la registrazione e attivazione dei servizi ed eventualmente utilizzare pseudonimi per gli account, soprattutto se riferiti a minori. In generale, si potrebbe decidere di evitare che questi ultimi possano utilizzare lo smart assistant, impostando password o impronte vocali che limitano l'accesso al servizio solo a specifici utenti adulti.

Meglio evitare di utilizzare l'assistente digitale per memorizzare informazioni delicate come quelle relative alla propria salute, le password, i numeri delle carte di credito, ecc..

Occorre valutare anche **rischi e benefici** dell'eventuale accesso da parte dello smart assistant ai **dati conservati sul dispositivo** in cui è installato, come ad esempio l'archivio fotografico, la rubrica, il calendario dello smartphone, ecc..

Disattiva l'assistente digitale quando non lo usi



Quando è acceso ma non viene utilizzato, l'assistente digitale è in uno stato detto di «**passive listening**», una sorta di «dormiveglia» da cui esce non appena sente la parola di attivazione che abbiamo scelto. Ecco allora alcune precauzioni:

- (se è consentito) scegliere con cura la parola di attivazione, **evitare parole di uso frequente** (nomi di persona o di oggetti di uso quotidiano) che possono causare, qualora captate, attivazioni involontarie dello smart assistant;
- **ricordare che durante il passive listening l'assistente digitale è potenzialmente in grado di «sentire»** (tramite il microfono del dispositivo su cui è installato) ed eventualmente anche di «vedere» (tramite la videocamera del dispositivo su cui è installato) tutto quello che diciamo e facciamo. Questi dati possono anche essere memorizzati e inviati a terzi, o comunque possono essere conservati non sul dispositivo, ma su server esterni.

Per evitare ogni possibile acquisizione e trasmissione non desiderata di dati, **quando non si usa l'assistente digitale** (ad esempio la notte, quando non si è in casa, ecc.), si può:

- (se è consentito) decidere di **disattivare il microfono o la videocamera o entrambi gli strumenti**, a seconda dei casi, attraverso appositi tasti presenti sul dispositivo che ospita l'assistente digitale (ad esempio: smartphone, altoparlante intelligente, ecc.) o utilizzando le impostazioni sulle app di gestione; oppure:
- **disattivare del tutto l'assistente digitale** tramite le impostazioni del dispositivo su cui è installato, oppure spegnere direttamente il dispositivo che lo ospita. E' una scelta forse un po' scomoda, perché comporta il dover riattivare il dispositivo quando necessario; ma può servire a garantire una maggiore protezione della propria riservatezza.

Decidi quali funzioni mantenere attive

Se l'assistente digitale è in grado di svolgere particolari azioni, come inviare messaggi ad altre persone (tramite sms o sistemi di messaggistica), pubblicare contenuti sui social o effettuare acquisti online, si può decidere di:

- **disattivare** tali funzioni;
- inserire, laddove possibile, una **password** per autorizzare l'uso solo su specifica richiesta dell'utente.

Gli assistenti digitali, come tutti i dispositivi e servizi che sono parte dell'Internet delle cose (IoT), non si limitano ad essere in connessione con la rete, ma **sono anche in grado di «dialogare» con altri dispositivi IoT**. Questa capacità amplifica la possibilità di raccolta, incrocio dei dati e diffusione di informazioni personali. Ad esempio, gli assistenti digitali con **funzioni domotiche** possono essere connessi con oggetti e servizi presenti nelle nostre case, dagli elettrodomestici alle smart TV, dalle luci ai sistemi di sicurezza e videosorveglianza. Si tratta di funzioni che semplificano la vita, perché in questo modo molti oggetti diventano controllabili a distanza con il solo utilizzo della voce.

Tuttavia è sempre bene:

- **informarsi** con attenzione su come e da chi vengono raccolti, elaborati, conservati ed eventualmente a chi vengono resi accessibili i dati personali;
- considerare il possibile impatto sulla privacy domestica.

Occorre inoltre valutare se **disattivare** alcune funzioni di controllo domotico e inserire apposite **password** per controllare l'attivazione o disattivazione dei sistemi, in modo da poter utilizzare lo smart assistant con maggiore sicurezza. Si pensi, ad esempio, al rischio eventuale che la voce dell'utente venga in qualche modo captata e clonata da malintenzionati e utilizzata per controllare elettrodomestici o ingressi o sistemi di protezione della casa, oppure per "spiare" l'interno dell'abitazione utilizzando microfoni e videocamere.



Cancella periodicamente la cronologia delle informazioni

Per limitare il trattamento dei dati personali raccolti dall'assistente digitale, si può **periodicamente cancellare la cronologia delle informazioni in esso registrate, o quantomeno eliminare dalla cronologia alcune tipologie di dati** (ad esempio, quelli ritenuti più delicati).

Questa operazione si può effettuare di solito **utilizzando il sito web o l'app dedicati alla gestione dello smart assistant, oppure utilizzando le funzioni di impostazione del dispositivo su cui è installato** (smartphone, smart speaker, automobili intelligenti, ecc.).



Attenzione alla sicurezza

Come per tutti i servizi digitali, una buona regola di base è **impostare password di accesso complesse**, sia per l'uso dello smart assistant che per la sua connessione a Internet.

Sono precauzioni importanti:

- verificare che la **crittografia** della rete Wi-Fi sia impostata preferibilmente sul protocollo di sicurezza WPA 2;
- **cambiare periodicamente la password**;
- verificare se sul dispositivo in cui è installato lo smart assistant siano presenti **sistemi di protezione anti-virus** e tenerli costantemente aggiornati.

Se il **sistema operativo** dell'assistente digitale o della app di gestione prevedono delle impostazioni privacy, è opportuno controllarle e regolarle sui livelli di protezione desiderati.

Se dai via il tuo smart assistant non dare via i tuoi dati



Nel caso in cui il dispositivo (smartphone, smart speaker, automobili intelligenti, ecc.) su cui è installato lo smart assistant venga eventualmente **venduto, regalato o dismesso**, è bene disattivare gli eventuali account personali creati - ad esempio per attivarlo e connetterlo online - e provvedere alla cancellazione di tutti i dati eventualmente registrati al suo interno o sulla app di gestione.

Se i dati raccolti sono stati trasmessi e conservati nei database dell'azienda produttrice o di altri soggetti è opportuno **chiederne la cancellazione**.

Nei casi in cui ci siano dubbi sull'effettivo rispetto delle norme o sul corretto uso dei propri dati personali, ci si può rivolgere al Garante per la protezione dei dati personali.