

INFORMATIVA GLOBALE SULLA PRIVACY DEI DIPENDENTI

Ultimo aggiornamento: [30 giugno 2023]

Johnson Controls International plc e le sue affiliate (collettivamente **Johnson Controls**) garantiscono la tutela della privacy e si impegnano a trattare i dati personali in conformità alle pratiche di gestione corretta delle informazioni e alle leggi vigenti in materia di riservatezza dei dati.

A riprova del nostro impegno in materia di privacy, abbiamo adottato una serie di Norme vincolanti d'impresa ("BCR" – Binding Corporate Rules) che contengono i nostri impegni globali in materia di privacy, tra cui la nostra politica sul trasferimento dei dati personali e dei diritti relativi alla privacy dei soggetti associati. L'obiettivo è garantire che i dati personali siano protetti durante il trattamento da parte di qualsiasi nostra consociata in tutto il mondo. Le suddette BCR sono state approvate dalle Autorità europee per la protezione dei dati e possono essere consultate nel [portale della privacy](#).

1. Ambito di applicazione

La presente informativa globale spiega in che modo, nel corso delle sue attività, Johnson Controls tratta i dati personali di dipendenti, candidati, personale interno, ex-dipendenti, persone a carico, beneficiari, appaltatori, consulenti e lavoratori temporanei.

Con "dato personale" si intende una qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Per categorie particolari di dati personali (dette anche dati personali sensibili) si intendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale e i dati relativi alla salute o alla vita sessuale, i dati genetici o biometrici.

2. Identità del titolare del trattamento dei dati

In genere, l'entità di Johnson Controls responsabile del trattamento dei dati personali (spesso definita "titolare del trattamento dei dati") è l'entità di Johnson Controls con cui si intrattiene un rapporto di lavoro (o, per i non dipendenti, l'entità di Johnson Controls responsabile del lavoro del soggetto interessato). In caso di dubbi è possibile rivolgersi al reparto Risorse Umane o all'Ufficio per la privacy (privacy@jci.com).

3. Categorie di dati personali

Nel corso delle normali attività aziendali e di gestione delle risorse umane vengono trattate le seguenti categorie di dati personali:

- dati di identificazione personale quali nome, luogo di nascita, indirizzo privato, data di nascita, genere, fotografie scattate nell'ambito delle attività professionali e numero di telefono privato;
- numeri di identificazione rilasciati dal governo, quali il numero di previdenza sociale e l'ID nazionale, per esigenze di contabilità dell'ufficio paghe;
- situazione riguardante il permesso di soggiorno, il permesso di lavoro e la residenza;
- dati per contattare la famiglia in caso di emergenza;
- informazioni inerenti il lavoro quali anni di servizio, sede di lavoro, numero di matricola, stato di servizio, assenze per ferie e dati contrattuali;

- informazioni riguardanti il livello di istruzione e il grado di formazione quali borse di studio, certificati e licenze, esperienze professionali e partecipazione a corsi di formazione in azienda;
- dati riguardanti l'assunzione e le prestazioni lavorative quali obiettivi, valutazioni, commenti, feedback, curriculum professionale, attrezzature di lavoro, carriera e pianificazione dell'avvicendamento, capacità e competenze, altre qualifiche professionali e informazioni sui precedenti personali;
- informazioni riguardanti l'uso delle risorse messe a disposizione da Johnson Controls, in particolare i computer, i dispositivi mobili, i sistemi di telecomunicazione e il traffico generato in Internet;
- informazioni raccolte da software di gestione di dispositivi mobili, tra cui nome, numero di cellulare, indirizzo e-mail aziendale, Paese del provider di telefonia mobile e informazioni contenute nelle applicazioni aziendali installate sul dispositivo;
- informazioni necessarie per le attività riguardanti la compliance e di gestione dei rischi quali provvedimenti disciplinari, esiti di controlli dei precedenti personali e dati sulla sicurezza;
- informazioni riguardanti busta paga, pagamenti o benefit, ad esempio stato civile, informazioni su salario e assicurazione, codice identificativo o codice fiscale rilasciato dal governo, dettagli riguardanti il conto bancario, informazioni sui benefit previsti dal contratto di lavoro e informazioni su famiglia e persone a carico;
- informazioni relative alla localizzazione e alla gestione delle presenze;
- informazioni su viaggi e passaporto;
- registrazioni vocali/video relative all'azienda e
- fotografie.

Possono essere trattate inoltre categorie particolari di dati personali, ad esempio:

- informazioni su stato di salute e malattie, come sintomi, diagnosi, cure e farmaci, se necessario, certificati medici e informazioni su infortuni e malattie sul posto di lavoro;
- informazioni relative alla salute e alla sicurezza sul lavoro;
- razza e nazionalità, se richiesto o consentito dalla legge;
- informazioni biometriche, comprese quelle relative al riconoscimento facciale, nel caso in cui le nostre sedi utilizzino tali sistemi, in conformità alle leggi vigenti;
- dati precisi sulla posizione geografica, nei casi previsti dall'incarico ricoperto, ove consentito dalla legge, compreso il caso in cui venga utilizzato uno dei nostri veicoli;
- appartenenza sindacale;
- condanne penali e procedimenti giudiziari e altre informazioni sui precedenti personali (se consentito dalla legge in alcuni paesi); e
- in alcune giurisdizioni, il numero di passaporto, il numero di previdenza sociale o il numero di identificazione nazionale.
- In India, le password e le informazioni finanziarie (come il conto bancario, la carta di credito o di debito o altri strumenti di pagamento) sono considerate informazioni personali sensibili.

Oltre a raccogliere i dati personali direttamente dall'interessato, possiamo raccogliere i suoi dati personali anche da altre fonti, tra cui:

- organizzazioni governative, fornitori di servizi sanitari e di prestazioni sociali;
- fornitori di servizi, ad esempio società che eseguono controlli dei precedenti personali;
- supervisor, colleghi o referenti nominati; e
- informazioni disponibili al pubblico.

4. Finalità del trattamento

I dati personali sono trattati per le seguenti finalità:

- risorse umane e occupazione, comprese la pianificazione della forza lavoro, la ricerca e l'assunzione di personale; gestione della forza lavoro, buste paga, programmi retributivi e benefit, gestione delle prestazioni, formazione e sviluppo, avanzamento di carriera e pianificazione dell'avvicendamento;
- fusioni, acquisizioni e dimissioni;
- rispetto delle prescrizioni di legge, ivi comprese gestione aziendale, ottemperanza a richieste di informazioni da parte delle autorità governative, pignoramenti e intimazioni, nonché adempimento degli obblighi fiscali;
- gestione dei posti di lavoro, ad esempio programmi di viaggi e spese e programmi interni di salute e sicurezza;
- reportistica interna;
- audit;
- per proteggere Johnson Controls, la sua forza lavoro e il pubblico da danni, furti, responsabilità legale, frodi o abusi o altri danni; e
- formazione e dimostrazioni dei prodotti;
- sviluppo di prodotti che coinvolgono o riguardano i dipendenti; e
- altre finalità di legge e collegate alle abituali attività dell'azienda.

Inoltre Johnson Controls monitora e filtra l'uso delle apparecchiature, della rete e il traffico internet assicurandosi che avvenga per scopi aziendali legittimi, e in particolare per:

- assicurare l'adeguata integrità dei sistemi informativi e rilevare nonché prevenire potenziali attività criminali, inclusi i crimini informatici;
- proteggere da distruzione, perdita, alterazione, accesso da parte di persone non autorizzate, diffusione o pirateria le informazioni di cui l'azienda è in possesso, ivi compresi, tra gli altri, i dati personali, le informazioni confidenziali e le informazioni commerciali di alto valore;
- garantire il buon funzionamento dei propri sistemi informativi;
- garantire la conformità con gli obblighi normativi e di autoregolamentazione applicabili; e
- rilevare eventuali casi di mancato rispetto delle norme di Johnson Controls riguardanti l'uso di Internet e del Codice etico.

Nel caso in cui sul dispositivo personale sia stato installato un software di gestione dei dispositivi mobili (per consentire l'accesso alla posta elettronica, ai servizi di rete e ai dati di Johnson Controls), Johnson Controls potrebbe dover apportare modifiche alla configurazione di sicurezza del dispositivo per conformarsi ai requisiti di sicurezza dei dispositivi mobili di Johnson Controls. Qualsiasi monitoraggio e/o filtraggio dell'uso di questo dispositivo, per gli scopi sopra menzionati, è limitato alle applicazioni aziendali. Per ulteriori informazioni, consultare la sezione "Come contattarci".

5. Basi giuridiche del trattamento

Trattiamo i dati personali in virtù delle seguenti basi:

- quando il trattamento è necessario per l'esecuzione del contratto con l'interessato, ad esempio per assumerlo, pagarlo e gestire il suo rapporto di lavoro con noi;
- laddove il trattamento sia necessario ai fini dei nostri legittimi interessi, ad esempio per la rendicontazione interna e la revisione contabile; per proteggere Johnson Controls, il suo personale e il pubblico da infortuni, furti, responsabilità legali, frodi o abusi o altri danni; per garantire l'integrità dei sistemi informativi; per assicurare la conformità con gli obblighi normativi e disciplinari applicabili; in relazione a fusioni, acquisizioni e dismissioni; per lo sviluppo di prodotti; per la formazione e dimostrazioni dei prodotti; per riunioni e telefonate di carattere commerciale;
- se il trattamento è necessario per adempiere a un obbligo di legge, ad esempio per scopi fiscali e previdenziali, per verificare il diritto al lavoro, per soddisfare le richieste delle autorità governative, per pignoramenti e adempimenti fiscali; e
- se l'interessato ha dato il proprio consenso.

Trattiamo le categorie particolari di dati personali in virtù delle seguenti basi:

- qualora il soggetto interessato abbia dato il proprio esplicito consenso;
- quando il trattamento è necessario ai fini dell'adempimento di obblighi e dell'esercizio di diritti in materia di diritto del lavoro;
- qualora il trattamento riguardi dati personali palesemente resi pubblici dall'interessato; e
- quando il trattamento è necessario per l'accertamento, l'esercizio o la difesa di diritti in sede giudiziaria.

6. Destinatari dei dati personali

I dati personali potranno essere divulgati nelle seguenti circostanze a:

- altre entità di Johnson Controls, joint venture, subappaltatori o fornitori che forniscono servizi per conto dell'azienda per le finalità precedentemente citate;
- un'organizzazione acquirente o di nuova costituzione, qualora Johnson Controls sia interessata da una fusione, una vendita o dal trasferimento di tutte o parte delle sue attività;
- fornitori di servizi terzi (che ci aiutano a svolgere le nostre attività aziendali), quali fornitori di servizi informatici, fornitori di benefit, fornitori di servizi di buste paga e consulenti (ad esempio avvocati, commercialisti e revisori dei conti);
- ogni altro destinatario, qualora ci venga imposto ad esempio dalla legge o in virtù di un'ordinanza di una corte competente;
- ogni altro destinatario, previo consenso dell'interessato, ad esempio per una verifica della situazione lavorativa o un prestito bancario; o
- ogni altro destinatario, se ragionevolmente necessario, ad esempio nel caso di una situazione di emergenza potenzialmente pericolosa per la vita di una o più persone.

7. Trasferimenti internazionali

Le terze parti, le consociate e le affiliate a cui i dati personali potrebbero dover essere comunicati possono trovarsi in altri paesi, tra cui gli Stati Uniti, l'India, la Slovacchia e il Messico; di conseguenza, è possibile che i dati personali vengano trasmessi in paesi in cui le leggi sulla privacy sono diverse da quelle del paese di residenza. In questi casi, l'azienda adotterà opportune misure per far sì che i dati personali ricevano un adeguato livello di protezione; queste misure includono le Norme vincolanti d'impresa, che stabiliscono disposizioni rigorose per il trattamento dei dati personali nonché termini contrattuali tipo. Se richiesto dalle leggi in vigore a livello locale, l'azienda potrebbe richiedere il consenso dell'interessato.

Sistema di norme transfrontaliere in materia di privacy (CBPR) dell'APEC: le pratiche di Johnson Controls in materia di privacy descritte nella presente Informativa sono conformi al sistema di norme transfrontaliere in materia di privacy dell'APEC. Il sistema CBPR dell'APEC prevede un quadro normativo applicabile alle organizzazioni per garantire la protezione dei dati personali trasferiti tra i paesi delle economie APEC. Maggiori informazioni sulle norme APEC sono disponibili [qui](#). Fare clic [qui](#) per visionare il nostro stato di certificazione in relazione al sistema CBPR dell'APEC.

Se non si ritiene di aver ricevuto una risposta soddisfacente a un dubbio relativo alla privacy o all'uso dei dati, invitiamo a contattare la terza parte responsabile per la risoluzione delle controversie negli Stati Uniti (gratuitamente) al link: <https://feedback-form.truste.com/watchdog/request>.

8. Conservazione dei dati

I dati personali saranno conservati per la durata necessaria al conseguimento dello scopo per il quale erano stati raccolti, solitamente per la durata della relazione contrattuale e, successivamente, per la durata prescritta o consentita dalle leggi vigenti. I piani di conservazione dei documenti in Johnson Controls sono consultabili su: <https://my.jci.com/Ethics/Pages/RIM.aspx>.

9. Protezione e sicurezza

Johnson Controls adotta tutte le precauzioni necessarie per proteggere i dati personali e prevenirne la perdita, l'uso illecito, l'accesso da parte di persone non autorizzate, la diffusione, l'alterazione e la distruzione. L'azienda ha adottato le opportune misure tecniche e organizzative per proteggere i sistemi informativi in cui sono conservati i dati personali e impone per contratto ai propri fornitori di beni e servizi l'obbligo di garantire analoga protezione dei medesimi.

10. Diritti dell'interessato

I diritti del soggetto interessato possono dipendere dalle leggi in vigore a livello locale. Nel rispondere alle richieste sui diritti di riservatezza come quelle elencate qui sotto, Johnson Controls si atterrà alla legislazione locale.

- Informazione e accesso: è possibile chiedere di avere accesso ai propri dati personali, di ricevere informazioni supplementari e di ottenere una copia dei propri dati personali. Il diritto all'informazione e all'accesso è soggetto ad alcune restrizioni. Ad esempio, l'accesso ai dati può essere negato (i) in caso di richieste di accesso frequenti nell'arco di poco tempo o (ii) nel caso in cui concedere tale accesso o correzione potrebbe compromettere la riservatezza di un'altra persona o rivelare informazioni sensibili riguardanti l'azienda senza che ve ne sia valido motivo.
- Rettifica: è possibile chiedere che i propri dati personali, se inesatti o non più validi, vengano rettificati e/o aggiornati.
- Cancellazione: l'interessato ha il diritto di chiedere la cancellazione dei suoi dati personali. Questo diritto è soggetto a restrizioni.
- Restrizione: l'interessato ha il diritto di chiedere la restrizione dei suoi dati personali. Restrizione significa che Johnson Controls si limita a conservare i dati personali, senza farli oggetto di trattamento, finché il ricorso dell'interessato non arriva a definizione.
- Obiezione al trattamento: l'interessato ha il diritto di sollevare obiezioni al riguardo di specifiche tipologie di trattamento, quali il marketing diretto, il trattamento per finalità statistiche o di ricerca e il trattamento basato su interessi legittimi. Il diritto di obiezione al trattamento sulla base di interessi legittimi può essere soggetto a dimostrazione da parte di Johnson Controls di motivi prioritari rispetto al diritto dell'interessato.
- Portabilità dei dati: l'interessato ha il diritto di richiedere la portabilità dei dati. Con portabilità dei dati si intende la fornitura dei dati personali in un formato strutturato, comunemente usato e leggibile

automaticamente così che possano essere facilmente trasferiti dall'interessato o da Johnson Controls a un'altra società. Il diritto alla portabilità dei dati è soggetto a restrizioni. Ad esempio, la portabilità dei dati non è applicabile ai documenti cartacei, e non deve pregiudicare né i diritti di altri né le informazioni sensibili dell'azienda.

- Diritto di non essere soggetto a decisioni basate unicamente su processi decisionali automatizzati: l'interessato ha il diritto di non essere soggetto a decisioni basate unicamente sul trattamento automatizzato (ossia senza alcun intervento dell'uomo) se tali decisioni producono effetti giuridici o si ripercuotono su di lui in maniera significativa. Con trattamento automatizzato si intende il trattamento dei dati personali con mezzi automatici. Se attuiamo un trattamento che utilizza un processo decisionale automatizzato che produce effetti legali o che riguarda in modo significativo l'interessato, quest'ultimo ha il diritto di non essere sottoposto a una decisione basata esclusivamente sul trattamento automatizzato.

Potrebbe inoltre avere diritto a sporgere un reclamo presso le autorità di controllo.

Per esercitare uno qualsiasi dei diritti sopra descritti è possibile rivolgersi al referente locale presso il reparto Risorse Umane o all'Ufficio per la privacy scrivendo all'indirizzo privacy@jci.com.

11. Consenso e revoca del consenso

Se il consenso è la base giuridica del trattamento dei dati personali o di categorie particolari di dati personali, l'interessato ha facoltà di revocare, a titolo gratuito, un consenso precedentemente concesso per una finalità specifica contattando l'Ufficio per la privacy all'indirizzo privacy@jci.com.

12. Modifiche alla nostra Informativa sulla privacy

L'azienda si riserva di modificare la presente informativa ogni qualvolta ne ravvede la necessità. Se dovessimo proporre cambiamenti significativi, provvederemo a comunicarli mediante una notifica su questa pagina. La presente informativa può anche essere integrata con altre dichiarazioni eventualmente necessarie per garantire la conformità con la giurisdizione del paese in cui si vive, o laddove esistano degli accordi con i rappresentanti del personale.

13. Problemi di privacy e come contattare l'azienda

Per qualsiasi domanda riguardante la presente informativa o se si ritiene che i propri dati personali non siano gestiti in maniera conforme a quanto previsto dalle leggi applicabili o dalla presente informativa, è possibile scegliere di:

- contattare l'Ufficio per la privacy all'indirizzo privacy@jci.com;
- discutere del problema con il proprio supervisore o con un altro supervisore o responsabile;
- contattare il reparto Risorse Umane o
- È inoltre possibile contattare la Integrity Helpline di Johnson Controls, attiva 24 ore su 24, all'indirizzo: www.johnsoncontrolsintegrityhelpline.com.