**Informativa sulla privacy delle risorse di soggetti esterni globali**

|  |  |
| --- | --- |
| **Contatto policy sulla privacy:**  Responsabile globale della protezione dei dati | **Data: 1 gennaio 2023**   |
|  (pgprivacyofficer.im@pg.com) **Regione:** Globale | **Ambito di applicazione:**  Tutte le risorse di soggetti esterni |

# **In****tento**

La presente Informativa illustra a tutte le risorse di soggetti esterni (“RSE”) (definite di seguito) le modalità con cui The Procter & Gamble Company e le sue consociate e/o affiliate (“P&G” o la “Società”) raccoglieranno e gestiranno le Sue Informazioni personali.

# **Stato dell’appaltatore indipendente**

La presente Informativa non instaura un rapporto di lavoro tra P&G e una RSE. Le RSE forniscono servizi a P&G come imprenditori indipendenti, a prescindere dal fatto che tali servizi siano forniti direttamente a P&G o in virtù di un accordo tra P&G e il datore di lavoro dell’RSE.

1. **Definizioni**

**Risorsa di soggetti esterni:** Qualsiasi individuo che fornisca a P&G prestazioni di lavoro o servizi per i quali P&G non sia il datore di lavoro di riferimento al momento della fornitura del lavoro o dei servizi, come ad esempio gli appaltatori.

**Informazioni personali:** Qualsiasi informazione relativa a un individuo identificato o identificabile, come il nome, altri identificatori, dettagli di contatto, informazioni professionali e caratteristiche personali.

**La Società o P&G:** ai fini della presente informativa, con “Società” o “P&G” si intendono The Procter & Gamble Company e le sue consociate e/o affiliate.

1. **Principi**

I principi fondamentali seguiti da P&G in materia di trattamento dei dati sono i seguenti:

* Raccogliere e gestire la quantità minima di Informazioni personali dell’RSE.
* Rispettare la privacy individuale.
* Rispettare i nostri Scopi, Valori e Principi (SVP), la presente Informativa e le leggi in materia.
* Seguire gli standard e le procedure appropriati nella raccolta e/o gestione delle Informazioni personali relative all’RSE.
1. **Informativa**

P&G rispetta la privacy di tutti. La presente informativa descrive le modalità di trattamento delle Informazioni personali dell’RSE, i tipi di informazioni che raccogliamo direttamente dall’utente e/o dal suo datore di lavoro, gli scopi per cui le utilizziamo, le categorie di destinatari con cui le condividiamo e le scelte che l’utente può fare in merito al loro utilizzo. Descriviamo inoltre le misure che adottiamo a tutela della sicurezza delle Informazioni personali relative all’RSE e i modi per contattarci in merito alle nostre pratiche in materia di protezione dei dati.

* 1. **Per quali scopi raccogliamo e utilizziamo le informazioni personali delle RSE?**

P&G raccoglie le Informazioni Personali riguardanti le EPR nel contesto del contratto di servizi e del rapporto con l’imprenditore indipendente che P&G ha con l’utente e/o con il suo datore di lavoro. In linea generale, raccogliamo e utilizziamo i dati personali dell’RSE e/o del suo datore di lavoro per i seguenti servizi e/o attività:

* Salute/sicurezza sul lavoro, compresi gli screening sanitari e i programmi medici relativi alla COVID-19 o a emergenze sanitarie simili
* Gestione degli accessi al sito
* Gestione dell’identità e delle credenziali, compresa la verifica e l’autenticazione dell’identità, l’emissione di documenti d’identità e badge, l’amministrazione del sistema, la registrazione dei log in/out e la gestione delle credenziali di accesso, la sicurezza delle informazioni e la cybersecurity
* Pianificazione degli imprevisti, compresa la continuità operativa, il personale, la gestione dei turni e i protocolli di emergenza/sicurezza
* Assegnazione e gestione dei dispositivi elettronici e ottimizzazione dell’utilizzo di rete e dispositivi
* Controlli per la sicurezza fisica e informatica, incluso il monitoraggio di dispositivi elettronici e reti e la registrazione di video di sicurezza come le telecamere a circuito chiuso
* Contenziosi e indagini interne/esterne, audit e risoluzione delle controversie
* Operazioni finalizzate allo svolgimento ordinario del lavoro (ad es., autenticazione e accesso ai nostri sistemi)
* Partecipazione a riunioni, corsi di formazione ed eventi
* Ottemperanza a leggi, regolamenti e politiche aziendali in materia di anticorruzione, lavoro minorile, anticorruzione, embargo, controlli sulle esportazioni, diritti umani e altri requisiti di governance e gestione aziendale
* Indagini condotte da P&G e/o dal datore di lavoro in merito a comportamenti scorretti sul posto di lavoro o a violazioni di procedure
* Applicazione e verifica dei nostri accordi di servizio con l’utente e/o il suo datore di lavoro, compresa la valutazione delle prestazioni dei servizi,
* Conformità con tutti i requisiti legali, normativi, giudiziari o governativi e risposta e conformità con le ordinanze del tribunale, le citazioni in giudizio, le richieste di documentazione o altre richieste di dati governativi
	+ Sicurezza e gestione del rischio, compresa la sicurezza e il monitoraggio del personale e dei locali e la protezione di P&G, dei nostri lavoratori e dei nostri clienti da furti, responsabilità legali, frodi o abusi.
	1. **Quali tipi di Informazioni personali relative all’RSE raccogliamo?**

Il tipo e la quantità di Informazioni personali relative all’RSE che la Società raccoglie saranno sempre mantenuti al minimo indispensabile. Il grafico seguente descrive più dettagliatamente le categorie di Informazioni personali relative alle RSE che P&G raccoglie nell’ambito dei propri processi aziendali.

La raccolta di informazioni e l’accesso alle informazioni potranno variare a seconda degli obblighi legali e/o aziendali specifici di ogni Paese.

La base giuridica o aziendale per la raccolta e il trattamento delle Informazioni personali delle RSE varierà in base al tipo di dati e all’uso previsto, come descritto nella Sezione 5.3 di seguito riportata.

|  |  |
| --- | --- |
| **Quali tipi di dati delle RSE raccogliamo e trattiamo?** | **Perché raccogliamo e trattiamo questo tipo di Informazioni personali delle RSE?***Raccogliamo e trattiamo questi tipi di dati per una serie di processi organizzativi e aziendali come descritto in dettaglio nella Sezione 5.1, e come ulteriormente spiegato di seguito:* |
| *Informazioni di contatto e caratteristiche personali* * Nome completo o eventuali cognomi precedenti (come il cognome da nubile)
* Altri identificatori univoci, come i numeri di identificazione o le credenziali rilasciate da P&G (ad esempio, l’accesso all’e-mail) o qualsiasi numero di identificazione rilasciato dal vostro datore di lavoro.
* Indirizzo postale
* Indirizzo e-mail
* Numero di telefono
 | * Accesso al sito e alla rete informatica
* Comunicazioni con il cliente relative alla pianificazione degli imprevisti aziendali, compresa la gestione dei turni
* Partecipazione a riunioni, corsi di formazione ed eventi
* Operazioni finalizzate allo svolgimento ordinario del lavoro (ad es., autenticazione e accesso ai nostri sistemi)
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
	+ Sicurezza e gestione del rischio, compresa la sicurezza e il monitoraggio del personale e dei locali e la protezione di P&G, dei nostri lavoratori e dei nostri clienti da furti, responsabilità legali, frodi o abusi
* Salute/sicurezza sul lavoro, compresi gli screening sanitari e i programmi medici relativi alla COVID-19 o a emergenze sanitarie simili
* Applicazione e verifica dei nostri accordi di servizio con l’utente e/o il suo datore di lavoro, compresa la valutazione delle prestazioni dei servizi
* Conformità con tutti i requisiti legali, normativi, giudiziari o governativi e risposta e conformità con le ordinanze del tribunale, le citazioni in giudizio, le richieste di documentazione o altre richieste di dati governativi
 |
| *Documento di identità/Idoneità all’impiego/Documento datore di lavoro** Documento d’identità (come passaporto, visto, codice fiscale, patente di guida, altri documenti d’identità rilasciati da istituzioni governative)
* Cittadinanza
* Residenza
* Nazionalità
* Paese di nascita
* Status di militare e/o veterano
* ID univoco come dipendente dell’azienda con cui P&G ha stipulato il contratto
 | * Identificazione del dipendente e mantenimento dell’integrità dei nostri registri
* Rispetto degli obblighi in materia di immigrazione e di lavoro
* Gestione della sicurezza e dei rischi, come nel caso della raccolta dei dati della patente di guida per le RSE che utilizzano automobili aziendali, la verifica di licenze professionali, la prevenzione delle frodi e scopi simili
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Pianificazione della sicurezza e degli imprevisti
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
 |
| *Informazioni finanziarie* * Numero e dettagli del conto bancario
* Informazioni sulla carta di pagamento personale, se fornite per i rimborsi
 | * Facilitare i rimborsi spese
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Pianificazione della sicurezza e degli imprevisti
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
 |
| *Informazioni sanitarie* * Informazioni relative alle condizioni di salute fisica o psicologica di un individuo, comprese eventuali disabilità o limitazioni nello svolgimento di mansioni o funzioni lavorative
* Esami tossicologici e altri tipi di accertamenti sanitari
 | * Rispettare gli obblighi in materia di salute e sicurezza sul posto di lavoro e di segnalazione alle istituzioni
* Gestire la sicurezza delle RSE e i rischi aziendali associati alla pandemia COVID-19 o simili emergenze sanitarie
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Pianificazione della sicurezza e degli imprevisti
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
 |
| *Dati di identificazione elettronica/Identificatori univoci/Immagine e voce** Identificatori associati ai sistemi P&G (ad es. nomi utente o credenziali online)
* Firma digitale
* Dati di identificazione elettronica, registri e registrazioni riguardanti l’accesso e l’utilizzo di dispositivi, sistemi, applicazioni, licenze, database e della rete P&G (come l’utilizzo di e-mail, internet e social media).
* Informazioni raccolte dai sistemi di sicurezza P&G, tra cui il sistema di telecamere a circuito chiuso (“CCTV”), i sistemi di accesso al sito, le telecamere utilizzate in concomitanza con processi o operazioni di produzione
* Dati di identificazione elettronica, registri e registrazioni relativi all’accesso ai siti fisici di P&G e alle aree ad accesso limitato, compreso il numero di badge/badge identificativo con foto
* Video, fotografie e altre registrazioni audio o video nel contesto di riunioni/corsi di formazione
* Dati di identificazione elettronica relativi alle registrazioni del call center
 | * Amministrazione di sistema, accesso e gestione delle risorse tecnologiche e IT
* Difendere la nostra sicurezza fisica, nonchè la sicurezza delle informazioni e la sicurezza informatica dalle minacce interne e/o esterne
* Gestire la prevenzione della perdita di informazioni e il recupero delle stesse nei nostri uffici e nelle sedi di produzione
* Raccolta dati e rendicontazione interna, comprese le attività di analisi statistica e confronto dei dati
* Consentire l’accesso ai siti, alla rete, agli strumenti, alle applicazioni e ad altri sistemi e risorse aziendali di P&G
* Favorire la visibilità sull’utilizzo e sui costi associati al consumo di strumenti, licenze, servizi e applicazioni P&G, a fini di ottimizzazione, controllo di qualità audit e analisi dei costi
* Documentare corsi di formazione e riunioni
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Pianificazione della sicurezza e degli imprevisti
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
 |
| *Cookie -* I cookie sono piccoli file inviati al computer dell’utente durante la navigazione sul web. Memorizzano informazioni utili sul modo in cui l’utente interagisce con i siti web che visita. I cookie non raccolgono alcuna informazione memorizzata sul computer o sul dispositivo dell’utente o nei file dell’utente. I cookie non contengono alcuna informazione che possa identificarlo direttamente come persona. I cookie associano il computer e il dispositivo dell’utente solo ad una stringa di numeri e lettere assegnati casualmente (ad es. ID cookie ABC12345) e mai, ad esempio, a John E. Smith. Questi sono i tipi di cookie che utilizziamo: * *Cookie di sessione*.I cookie di sessione si ricordano di te (utilizzando un ID generato casualmente) mentre navighi da una pagina all’altra del sito, in modo che non ti venga chiesto di fornire nuovamente le stesse informazioni già fornite. Questi cookie vengono eliminati non appena l’utente lascia il nostro sito o chiude il browser.
* *Cookie persistenti*. I cookie persistenti consentono ai siti di ricordare le preferenze dell’utente quando torna nuovamente sul sito. Ad esempio, se si sceglie di leggere il sito in francese durante la prima visita, nella visita successiva il sito apparirà automaticamente in francese.
* *Cookie analitici*. Questi cookie ci dicono come funzionano i nostri siti web. In alcuni casi, utilizziamo i cookie di Google Analytics per monitorare le prestazioni dei nostri siti. La nostra capacità di utilizzare e condividere le informazioni raccolte da Google Analytics sulle visite dell’utente ai nostri siti è delimitata dai [Termini di utilizzo di Google Analytics](https://www.google.com/analytics/terms/us.html) e dall’[Informativa sulla privacy di Google](https://policies.google.com/privacy).
 | Utilizziamo i cookie nei siti web rivolti alle RSE P&G per una serie di motivi, tra cui: * conoscere meglio il modo in cui l’utente interagisce con i nostri siti web e i contenuti di P&G
* cercare di migliorare l’esperienza dell’utente quando visita i nostri siti web
* personalizzare il sito web in base alle preferenze dell’utente
* identificare gli errori e risolverli
* analizzare le prestazioni dei nostri siti web
 |
| *Altre caratteristiche personali** Dati biometrici, come impronte digitali o scansioni facciali
* Verifica dei precedenti penali
 | * Agevolare l’accesso ai siti e ai sistemi aziendali tramite l’utilizzo di dati biometrici
* Conformità alle norme e ai regolamenti
* Governance e gestione aziendale
* Pianificazione della sicurezza e degli imprevisti
* Segnalazioni esterne obbligatorie
* Indagini e gestione degli incidenti
 |

* 1. **Su quale base giuridica e/o commerciale trattiamo le informazioni personali delle RSE?**

Raccogliamo e gestiamo la quantità minima di Informazioni personali relative all’RSE necessaria per ottemperare ai nostri obblighi contrattuali e/o giuridici relativi al rapporto del nostro imprenditore indipendente con l’utente e/o il suo datore di lavoro; per promuovere i legittimi interessi commerciali della Società in modo proporzionale agli interessi della privacy dell’utente; e per trattare le Informazioni personali fornite con il consenso dell’utente, ove applicabile, per gli scopi previsti.

Le basi giuridiche e/o aziendali per il trattamento delle Informazioni personali dell’RSE possono essere rappresentate di volta in volta: dall’ottemperanza di P&G alle leggi e ai regolamenti applicabili; dall’ottemperanza ai propri obblighi contrattuali; dai legittimi interessi aziendali della Società; dagli interessi collegati alla salute pubblica; e/o dal consenso dell’utente.

La base giuridica e/o aziendale per il trattamento delle Informazioni personali delle RSE può variare in base alla giurisdizione, alla categoria/tipo di dati e alle ragioni per cui raccogliamo e utilizziamo tali informazioni.

Queste sono le basi giuridiche sulle quali ci baseremo generalmente per il trattamento di tali categorie di dati:

|  |  |
| --- | --- |
| **Tipo di dati personali** | **Base giuridica per il trattamento** |
| Informazioni di contatto, Documento di identità, Informazioni finanziare, Informazioni sanitarie | Ottemperanza di P&G agli obblighi contrattuali e legali  |
| Documento di identità/idoneità all’impiego | Ottemperanza di P&G alle leggi applicabili |
| Informazioni professionali, Informazioni di contatto | Legittimi interessi aziendali di P&G |

* 1. **In che modo condividiamo le Informazioni personali relative alle RSE?**

P&G condividerà le Informazioni personali relative alle RSE esclusivamente con coloro che hanno una legittima esigenza aziendale di venirne a conoscenza.

P&G può condividere le informazioni dell’utente con il suo datore di lavoro (e con altre entità se incaricate dal suo datore di lavoro), con gli appaltatori, i fornitori, le agenzie, i lavoratori temporanei o qualsiasi altra parte che agisca per conto di P&G (“Parti esterne”).

Le Informazioni personali delle RSE possono essere condivise con la nostra sede centrale e le nostre affiliate a livello globale, se necessario, per raggiungere gli scopi di trattamento indicati nella sezione 5.2 di cui sopra.

Possiamo inoltre condividere le Informazioni personali relative alle RSE qualora ci venga richiesto di farlo per legge o in base a procedimenti legali; per far rispettare o proteggere i diritti e le politiche aziendali di P&G; per fornire assistenza in relazione a indagini su casi sospetti o accertati di attività illecite o di condotta impropria.

* 1. **Quali sono i diritti in materia di protezione dei dati personali dei Dipendenti?**

La RSE ha il diritto di contattarci e richiedere l’accesso alle proprie Informazioni personali da noi trattate. Laddove consentito dalla legge applicabile, l’utente può richiedere la correzione, la cancellazione o la limitazione di informazioni inaccurate, obsolete o non necessarie, così come chiedere a P&G di fornire i dati in un formato che ne consenta il trasferimento da parte loro a un fornitore di servizi, a seconda dei casi. Laddove il trattamento delle Informazioni personali delle RSE si basi sul consenso, l’utente ha il diritto di revocare il proprio consenso in qualsiasi momento. Laddove il trattamento delle Informazioni personali delle RSE si basi su un interesse legittimo, l’utente ha in determinate circostanze il diritto di opporsi al trattamento dei dati.

Nell’esercizio di tali diritti, invitiamo l’utente a discutere innanzitutto con il dipendente P&G che svolge il ruolo di sponsor del sito. In alternativa, è possibile contattare il nostro Responsabile della Protezione dei Dati all’indirizzo indicato di seguito. Se l’utente non è soddisfatto della nostra risposta alla sua richiesta o del trattamento dei suoi dati personali, può presentare un reclamo all’autorità garante per la protezione dei dati personali nel proprio Paese.

* 1. **In che modo trasferiamo le Informazioni personali relative all’RSE?**

P&G è un’azienda globale e ha RSE in molti Paesi. Se legalmente consentito, e in base a requisiti e/o limitazioni specifiche per ogni paese, le Informazioni personali delle RSE possono essere trasferite in Paesi diversi da quello in cui sono state raccolte. Le Informazioni personali delle RSE possono essere archiviate in sistemi situati negli Stati Uniti, a cui hanno accesso altre affiliate di P&G di tutto il mondo, compresi fornitori di servizi, oppure possono venire trasferite in altri Paesi, se necessario per lo svolgimento delle operazioni pertinenti. Tali Paesi potrebbero non avere le stesse leggi in materia di protezione dei dati del Paese di residenza del Dipendente. In caso di trasferimento delle Informazioni personali ad altri Paesi o accesso alle informazioni da altri Paesi al di fuori del Paese di residenza dell’utente, poniamo in essere salvaguardie appropriate e implementiamo le misure amministrative, tecniche e/o contrattuali legalmente richieste per la protezione delle informazioni personali. Effettuiamo trasferimenti al di fuori dello Spazio Economico Europeo (SEE), del Regno Unito (UK) e della Svizzera, sia tra le entità P&G sia verso i nostri fornitori di servizi, in base alle Clausole Contrattuali Tipo. Se si desidera una copia di queste clausole, contattare corporateprivacy.im@pg.com. P&G si atterrà inoltre ai requisiti nazionali specifici che limitano i trasferimenti di dati al di fuori del Paese di raccolta.

* 1. **In che modo proteggiamo le Informazioni personali relative alle RSE?**

Poniamo in essere misure fisiche, amministrative e tecniche appropriate, quali pseudonimizzazione, crittografia e controlli d’accesso, volti a tutelare le Informazioni personali relative alle RSE da distruzione, perdita, alterazione, divulgazione, oppure accesso o utilizzo, accidentali, illeciti o non autorizzati, e da tutte le altre forme illecite di trattamento. Nel caso in cui le Parti esterne trattino le Informazioni personali delle RSE per conto di P&G, stipuliamo anche contratti con tali Parti esterne per garantire che implementino le misure fisiche, amministrative e tecniche appropriate nella gestione di tali dati.

**5.8 Per quanto tempo vengono conservate le Informazioni personali delle RSE**?

Conserviamo le Informazioni personali delle RSE per il tempo necessario a soddisfare le finalità aziendali, a meno che non sia richiesto o consentito dalla legge applicabile un periodo di conservazione più lungo. In genere si tratta del periodo di utilizzo dei servizi da parte dell’utente. In alcuni casi, potremmo dover conservare le Informazioni personali delle RSE per un periodo di tempo successivo alla cessazione del rapporto con P&G al fine di rispettare gli obblighi legali o contrattuali.

* 1. **P&G monitora l’utilizzo della rete e dei dispositivi?**

La Società monitora l’utilizzo della rete P&G e dei dispositivi P&G. P&G ha l’obbligo di proteggere i propri dipendenti, beni e strutture. P&G controlla le sue reti e i suoi dispositivi aziendali per tre finalità: i) proteggere la sicurezza (intendendo con questo anche la riservatezza, l’integrità e la disponibilità) delle persone, dei dati, della rete, delle risorse, delle strutture, della reputazione e degli interessi competitivi di P&G; ii) indagare su condotte illecite o violazioni di legge sospette o confermate (anche a supporto di eventuali contenziosi legali); iii) garantire l’integrità dei processi aziendali e della rendicontazione finanziaria.

P&G non monitora la rete e i dispositivi di P&G di soggetti specifici, a meno che non vi sia un valido motivo per farlo, ovvero nel caso in cui ci venga imposto dalla legge, ad esempio su richiesta delle forze dell’ordine. Ci riserviamo il diritto, nel rispetto delle leggi vigenti, di accedere, ispezionare, divulgare e smaltire qualsiasi file, dato e messaggio elettronico creato, memorizzato, inviato o ricevuto attraverso le nostre reti e i nostri dispositivi, come necessario per gli scopi sopra menzionati. Tale monitoraggio è sempre conforme alle leggi e alle normative vigenti. P&G implementerà procedure, standard, politiche e/o misure attive aggiuntive, laddove necessario, per soddisfare i requisiti legali locali.

In particolare, P&G condurrà un monitoraggio passivo e attivo delle reti P&G e dei dispositivi di proprietà P&G assegnati alle RSE per segnalare potenziali minacce agli interessi di P&G. Il “monitoraggio passivo” non analizzerà attivamente il comportamento di un soggetto, ma piuttosto ricerca indicatori di rischio. Tali indicatori di rischio sono predefiniti da P&G e da fornitori specializzati in soluzioni di sicurezza, e sono calibrati per soddisfare le esigenze di P&G in fatto di sicurezza. Quando scatta un indicatore di rischio (un “Evento”), i sistemi registrano i relativi dati e li conservano per la successiva analisi e/o indagine. In particolare, le seguenti tecniche di monitoraggio passivo saranno utilizzate nelle reti P&G e nei dispositivi di proprietà P&G assegnati alle RSE:

1. **Il Monitoraggio del Comportamento di Utilizzo** è una tecnica di monitoraggio per cui software o hardware controllano la rete anonimizzata e i dati Web di P&G per verificare la presenza di una serie predefinita di indicatori di rischio. Questa tecnica cerca schemi sospetti nelle modalità di *utilizzo* della rete di P&G e/o dei dispositivi di proprietà di P&G assegnati all’RSE. Ad esempio, P&G può impostare lo strumento di Monitoraggio del Comportamento di Utilizzo in modo da ricercare indicatori di rischio in base alla sede P&G da cui è stato effettuato l’accesso. La Sicurezza di P&G può calibrare lo strumento in modo da emettere un avviso qualora le credenziali di accesso vengano inserite in due sedi diverse di P&G più rapidamente di quanto potrebbe ragionevolmente fare una persona che si spostasse tra i due luoghi.
2. **L’Analisi del Traffico in Entrata** è uno strumento di monitoraggio che esamina le comunicazioni in entrata basate su Web (compresa la posta elettronica) per verificare la presenza di indicatori di rischio all’ingresso nella rete di P&G. Antivirus e firewall sono gli esempi più tipici di questo strumento, in quanto analizzano costantemente il traffico in entrata per verificare la presenza di indicatori di malware in allegati, link, siti Web, etc...
3. **L’Analisi Periodica** è uno strumento di monitoraggio che effettua analisi a livello di rete P&G e di dispositivo P&G, in modo da rilevare specifici indicatori di rischio che potrebbero aver superato i controlli del perimetro effettuati dall’Analisi del Traffico in Entrata. Questo strumento è utile perché a volte gli Eventi sono più facilmente identificabili se visualizzati in un contesto più ampio. Esempio tipico di questa funzionalità è la scansione di tutto il disco mediante antivirus.
4. **Analisi del Traffico in Uscita** P&G dispone della funzione di analisi del traffico Web in uscita per verificare la presenza di indicatori di rischio specifici e predefiniti. Lo strumento analizza il traffico in uscita per verificare se è scattato un Evento secondo le regole specificate relativamente agli indicatori di rischio. Ad esempio, P&G può stabilire una regola in base alla quale verranno segnalati upload di file di grandi dimensioni al di fuori della rete di P&G che contengano dati Altamente Riservati o determinate parole chiave, come uno specifico componente chimico nella formula di un nuovo prodotto

P&G valuta, in base alla natura di un rischio segnalato dagli strumenti di monitoraggio passivo o portato in altro modo all’attenzione di P&G (ad es. causa legale, sospetta condotta impropria, forze dell’ordine, etc...), se è necessario svolgere ulteriori indagini/analisi sul rischio. In tale valutazione, P&G prende in esame i potenziali danni che verrebbero arrecati a dipendenti, consumatori e altre parti interessate, e/o alla Società, nonché gli aspetti legali e in materia di privacy dei soggetti coinvolti. P&G può anche stabilire se sono necessarie ulteriori analisi in base a requisiti legali o di politica per salvaguardare le risorse e garantire l’integrità dei processi aziendali. In base a tale analisi, P&G deciderà di non svolgere ulteriori indagini, oppure di procedere con un’indagine proporzionata mediante strumenti di monitoraggio attivo.

P&G si avvale di cinque tipi fondamentali di strumenti di Monitoraggio Attivo: (1) Analisi Dispositivi, (2) Analisi Internet, (3) Monitoraggio Soft, (4) Monitoraggio Hardware e (5) Prevenzione Perdita Dati.

1. **Analisi dei Dispositivi:** questi strumenti consentono a P&G, talvolta tramite terzi, di estrarre *tutto* il contenuto in un preciso momento da un computer di proprietà di P&G o di un altro dispositivo P&G per usarlo in un’indagine. Gli strumenti di Analisi dei Dispositivi non solo estraggono file e applicazioni salvati e archiviati sugli stessi, ma possono anche ottenere la memoria presente sul dispositivo P&G al momento dell’acquisizione. A seconda dello strumento, P&G può decidere di estrarre esclusivamente i file fisici (vale a dire, non la memoria) oppure un’immagine parziale del dispositivo, permettendo così all’indagine di focalizzarsi unicamente su specifici tipi di file o applicazioni in linea con i principi di proporzionalità.
2. **Analisi Internet:** P&G implementa uno strumento proxy Web basato su cloud fornito da terzi che ha tre funzioni principali. Innanzitutto, esso ha la capacità di monitorare l’utilizzo pubblico che le RSE fanno di Internet a livello di URL (vale a dire, i nomi dei siti Web visitati) quando usano un dispositivo di proprietà di P&G. Questa funzione monitora e registra l’attività su Internet mediante identificatori hash personali (anonimizzando in tal modo l’utente) per il potenziale impiego durante un’indagine autorizzata. Secondariamente, esso ha la capacità di fornire la visibilità dei dati inseriti in un sito Web non crittografato e dei file caricati o scaricati durante la visita di siti Web non crittografati. In terzo luogo, è in grado di decriptare un sottoinsieme limitato di traffico web predefinito come ad alto rischio (ad esempio, connessioni in uscita a pagine web note come dannose, pagine web note per fornire malware ai dispositivi o siti di condivisione di file non approvati). Questa soluzione è configurata in modo da non decriptare il traffico diretto a siti web che possono trattare informazioni personali sensibili dell’utente finale (ad esempio, siti bancari e sanitari).
3. **Monitoraggio Soft:** si tratta di tecniche implementate nel contesto di un’indagine che coinvolge individui identificabili quando (a) gli individui vengono messi a conoscenza dell’indagine, e (b) gli individui non sono l’oggetto dell’indagine. Ad esempio, uno strumento di Monitoraggio Soft potrebbe essere rappresentato da una telefonata o da un’e-mail volte a stabilire dove si trova in quel momento/dove ha effettuato l’accesso una RSE *identificata*, al fine di determinare la natura legittima di un Evento geografico che è scattato.
4. **Monitoraggio Hardware e delle Applicazioni**: gli strumenti di Monitoraggio Hardware e delle Applicazioni sono funzioni di registrazione e monitoraggio che i fabbricanti integrano nell’hardware e/o nelle applicazioni stesse che, se collegati a una RSE identificabile, costituiscono Monitoraggio Attivo. Esempi tipici ne sono log di server, accessi SAP, report di utilizzo di badge identificativi, autenticazioni di rete, etc...
5. **Prevenzione Perdita Dati:** P&G o un fornitore di servizi approvato analizza le e-mail destinate a indirizzi non-P&G alla ricerca di indicatori di perdita di dati. Ad esempio, se un’RSE invia un’e-mail non crittografata con un allegato altamente riservato a un indirizzo e-mail non-P&G, la soluzione di prevenzione della perdita di dati segnalerà l’e-mail come un rischio per la sicurezza delle informazioni e l’utente potrà essere informato della necessità di utilizzare una soluzione di crittografia approvata per le comunicazioni future. Allo stesso modo, se un’e-mail in uscita classificata come altamente riservata o segreta (comprese le parole chiave specificamente designate) fosse contrassegnata, tale e-mail verrebbe esaminata per verificare il rischio di sicurezza. Se opportuno, può essere avviata un’indagine. P&G non scansiona i messaggi classificati come “Personali” o “Privati” o che sono contrassegnati come “Personali” o “Privati” nell’oggetto.
6. **Modifiche future**

P&G si riserva il diritto di modificare la presente Informativa come necessario, ad esempio per rispettare eventuali modifiche delle leggi, normative, prassi e procedure aziendali, o al fine di rispondere a nuove minacce o a nuovi obblighi imposti dalle autorità per la protezione dei dati. Laddove tali modifiche influiscano sostanzialmente sul nostro trattamento delle Informazioni personali dell’RSE, lo comunicheremo di conseguenza.

1. **Informazioni di contatto**

In caso di domande o dubbi in merito al trattamento da parte nostra dei dati personali/delle informazioni personali dell’EPR o se si desidera esercitare i propri diritti in materia di privacy, è possibile contattare il nostro Responsabile globale della protezione dei dati – E-mail: pgprivacyofficer.im@pg.com, Telefono: +1 (513) 622-0103, Indirizzo postale: 1 Procter & Gamble Plaza, Cincinnati, OH 45202, Stati Uniti

In caso di dubbi circa una presunta violazione dei dati che riguardi le informazioni personali dell’RSE o di qualsiasi altra informazione personale trattata da P&G, inviare un’e-mail a securityincident.im@pg.com.