|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ***Valutazione d’impatto sulla protezione dei dati*** | | | |
| Documento N.: | Data emissione: | Stato: | | Revisione: |
| GW\_DPIA\_001 | 17/05/2019 |  | | Rev\_001 |
| Proprietario del Documento: | Redatto da: | | Approvato da: | |
| Gowen s.r.l. | Gowen s.r.l. | |  | |

**Valutazione d’impatto**

**sulla protezione dei dati**

[art. 35 Reg. EU 679/2016]

* *adeguamento Regolamento EU 2016/679 -*

Sommario

[a) DESCRIZIONE SISTEMATICA DEL TRATTAMENTO 3](#_Toc16083282)

[*1.* *natura, ambito di applicazione, contesto del trattamento* 3](#_Toc16083283)

[*2.* *descrizione del sistema degli strumenti informatici e telematici* 3](#_Toc16083284)

[*3.* *descrizione del sistema di gestione di documentazione materiale / cartacea e del sistema archiviazione cartacea* 4](#_Toc16083285)

[*4.* *finalità del trattamento* 4](#_Toc16083286)

[*5.* *descrizione funzionale del trattamento* 7](#_Toc16083287)

[*6.* *dati personali trattati, destinatari e periodo di conservazione dei dati personali trattati* 8](#_Toc16083288)

[6.1. dati personali trattati 8](#_Toc16083289)

[6.2. destinatari interni, esterni o terzi dei dati trattati 9](#_Toc16083290)

[6.3 periodo di conservazione dei dati personali trattati 11](#_Toc16083291)

[*7.* *liceità del trattamento* 12](#_Toc16083292)

[b) VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO 13](#_Toc16083293)

[1. *finalità determinate, esplicite e legittime* 13](#_Toc16083294)

[*2.* *liceità del trattamento* 13](#_Toc16083295)

[*3.* *dati personali adeguati, pertinenti e limitati a quanto necessario* 14](#_Toc16083296)

[*4.* *limitazione della conservazione dei dati* 16](#_Toc16083297)

[*5.* *Informazioni e diritti dell’interessato* 17](#_Toc16083298)

[*6.* *Contitolarità del trattamento* 17](#_Toc16083299)

[c) VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI E MISURE PREVISTE PER AFFRONTARE I RISCHI E GARANTIRE LA PROTEZIONE DEI DATI; VALUTAZIONE PROCEDURA INCIDENT RESPONSE PLAN 18](#_Toc16083300)

[*1.* *rischio di accesso illegittimo ai dati* 18](#_Toc16083301)

[*2.* *rischio di modifiche indesiderate dei dati* 18](#_Toc16083302)

[*3.* *rischio di perdita/scomparsa dei dati* 19](#_Toc16083303)

[*4.* *procedura di IRP - notifica violazione dei dati personali (data breach)* 20](#_Toc16083304)

[*5.* *procedura di riscontro delle richieste degli interessati* 20](#_Toc16083305)

[d) CONCLUSIONI 20](#_Toc16083306)

[*1.* *analisi dei rischi – valutazione dei rischi* 20](#_Toc16083307)

[*2.* *consultazione preventiva* 21](#_Toc16083308)

[Storico del Documento 21](#_Toc16083309)

La Società **Gowen s.r.l.**, con sede in Roma (RM) 00135 Via Salomone Morpurgo n. 8 – p.iva e c.f. 03563891005 (d’ora in avanti anche “la Società”), con il presente documento e quale titolare del trattamento, procede alla presente valutazione di impatto sulla protezione dei dati relativi al trattamento effettuato mediante sistemi telematici, informatici e manuali/cartacei (di seguito anche solo “cartacei”), dunque per trattamenti simili e/o analoghi.

La presente, nel rispetto dell’art. 35 Reg.Eu 679/2016, analizza in particolare le attività concernenti la gestione dei servizi erogati e la gestione dei dati clientie fornitori, dipendenti, collaboratori, consulenti e professionisti, utenti, che implicano un trattamento di dati personali con modalità telematiche e informatiche mediante server e software gestionali ovvero con modalità manuali/cartacee (ad es. fascicoli e documenti cartacei).

# **a) DESCRIZIONE SISTEMATICA DEL TRATTAMENTO**

*[art. 35, paragrafo 7, lettera a)]*

1. ***natura, ambito di applicazione, contesto del trattamento***

Il trattamento dei dati personali è effettuato attraverso strumenti telematici, informatici e cartacei al fine di gestione dell’attività della Società. Inoltre, presso la sede della società sita in via Salomone Morpugno n. 8 – Roma, sono presenti le sedi operative delle società GHP s.r.l. e Mifin s.r.l. con le quali, pertanto sono condivise strumentazioni telematiche e informatiche. Tale rapporto è regolato da un accordo di contitolarità del trattamento dei dati personali ai sensi dell’art. 26 Reg. UE 679/2016.

Categorie di dati trattati:

* dati relativi ai clienti diretti (trattati in qualità di Titolare);
* dati relativi ai fornitori;
* dati relativi ai dipendenti, collaboratori, consulenti e professionisti;
* dati relativi agli utenti del sito.

1. ***descrizione del sistema degli strumenti informatici e telematici***

La Società è dotata di un sistema di strumenti informatici e telematici per mezzo dei quali svolge le attività relative al proprio business. Pertanto, attraverso tali sistemi e mediante gli stessi, avviene parte del trattamento dei dati personali nonché parte del sistema di archiviazione.

La Società ha implementato e modificato parte del sistema al fine di rendere idoneo il trattamento a quanto richiesto dal Regolamento EU 679/2016 procedendo quindi ad una revisione dell’ambito e del contesto di trattamento.

Il dettaglio tecnico della struttura informatica e tecnica della Società è evincibile come da misure di sicurezza di cui all’allegato **A)** della presente (v. in particolare par. 2.3).

In particolare, sono adottate le seguenti policies (inserite nelle misure di sicurezza di cui all’allegato A): 1) *Password policy*; 2) *Record Retention Policy* (*RRP*); 3) *Incident responce plan* (*IRP*); 3) *Subject access reques* (*SAR*).

1. ***descrizione del sistema di gestione di documentazione materiale / cartacea e del sistema archiviazione cartacea***

La Società svolge le attività relative al proprio business anche per il tramite di documenti cartacei. Pertanto, attraverso tali documenti cartacei e per mezzo l’archiviazione cartacea degli stessi, avviene parte del trattamento dei dati personali.

La Società ha implementato e modificato parte del sistema al fine di rendere idoneo il trattamento a quanto richiesto dal Regolamento EU 679/2016 procedendo quindi ad una revisione dell’ambito e del contesto di trattamento. Il sistema è descritto nelle misure di sicurezza di cui all’allegato **A)** della presente (v. in particolare par. 3).

Inoltre, si rappresenta che, come da misure di sicurezza (v. all. A) par. 3.2) «l’accesso agli archivi contenenti dati dei dipendenti ovvero ancora dati particolari o giudiziari è consentito solo al Titolare ovvero alle persone autorizzate attraverso specifica autorizzazione scritta da parte del titolare del trattamento contenuta nell’incarico».

Ancora, per quanto di interesse relativamente al trattamento dei dati mediante strumenti cartacei la società adotta le seguenti policies: 2) *Record Retention Policy* (*RRP*); 3) *Incident responce plan* (*IRP*); 3) *Subject access reques* (*SAR*).

1. ***finalità del trattamento***

I dati personali, i dati particolari raccolti ai sensi dell’art. 9 Reg. UE 2016/679 e dati di cui all’art. 10 Reg. UE 2016/679 sono trattati, rispettivamente, per le seguenti finalità:

* 1. dati clienti

*finalità relative alla prestazione contrattuale*

* + dare corso al rapporto contrattuale e negoziale, pertanto in esecuzione della gestione dello stesso;
  + gestione commesse, ordini e spedizioni, ricezione, gestione dei servizi oggetto delle prestazioni richieste alla società;
  + gestione appalti e bandi di gara pubblici (pubblici e/o privati);
  + amministrazione contabile, emissione fatture e gestione fatture, gestione contratti, gestione pagamenti e incassi;
  + quotazioni clienti;
  + due diligence e/o gestione del credito;

*finalità di legge*

* + dare esecuzione ad obblighi di legge, regolamenti, normative nazionali, comunitarie ed internazionali o derivanti da disposizioni impartite da Autorità a ciò legittimate dalla legge;
  + perseguire accertare e/o difendere, eventualmente, un diritto o legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali;
  + adempiere agli obblighi previsti in ambito fiscale e contabile;
  + adempiere ad obblighi legati alla normativa sulla sicurezza e salute;
  + adempiere ad obblighi legati alla normativa del trasporto, in particolare, di merci ovvero scarti e rifiuti;
  + amministrazione contabile, emissione e gestione fatture, gestione contratti, gestione pagamenti, incassi;
  + dare esecuzione ad obblighi impartiti dall’autorità giudiziaria;
  + perseguire, eventualmente, un legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali.

*altre finalità*

* + attività di promozione commerciale della società relativamente ai servizi offerti, comunicazioni di varia natura ai clienti;
  1. dati fornitori

*finalità relative alla prestazione contrattuale*

* + dare corso al rapporto contrattuale e negoziale, pertanto in esecuzione della gestione dello stesso;
  + gestione commesse, ordini e spedizioni, ricezione, gestione dei servizi oggetto delle prestazioni richieste alla società;
  + gestione appalti e bandi di gara pubblici (pubblici e/o privati);
  + amministrazione contabile, emissione fatture e gestione fatture, gestione contratti, gestione pagamenti, incassi;
  + quotazione fornitori;
  + due diligence e/o gestione del credito;

*finalità di legge*

* + dare esecuzione ad obblighi di legge, regolamenti, normative nazionali, comunitarie ed internazionali o derivanti da disposizioni impartite da Autorità a ciò legittimate dalla legge;
  + perseguire accertare e/o difendere, eventualmente, un diritto o legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali;
  + adempiere agli obblighi previsti in ambito fiscale e contabile;
  + adempiere ad obblighi legati alla normativa sulla sicurezza e salute;
  + adempiere ad obblighi legati alla normativa del trasporto, in particolare, di merci ovvero scarti e rifiuti;
  + amministrazione contabile, emissione e gestione fatture, gestione contratti, gestione pagamenti, incassi;
  + dare esecuzione ad obblighi impartiti dall’autorità giudiziaria;
  + perseguire, eventualmente, un legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali.

*altre finalità*

* + attività di promozione commerciale della società relativamente ai servizi offerti, comunicazioni di varia natura ai fornitori;
  1. dati dipendenti, collaboratori, consulenti e professionisti
  + dare corso al rapporto contrattuale e/o di lavoro, pertanto in esecuzione della gestione dello stesso;
  + gestione degli obblighi di legge relativi al rapporto di lavoro/collaborazione/agenzia/mandato (buste paga, fatture, pagamento degli stipendi e dei compensi, pagamento dei contributi previdenziali e assistenziali e delle imposte) e gestione della qualità del rapporto di lavoro/collaborazione/agenzia (valutazioni, monitoraggio delle attività, ecc.);
  + comunicazioni con dipendenti, collaboratori, consulenti e professionisti.
  + con riferimento ai dati personali dei dipendenti, il trattamento è effettuato allo specifico fine di dare corso al rapporto contrattuale e pertanto in esecuzione della gestione dello stesso;
  + dare esecuzione ad obblighi di legge, regolamenti, normative nazionali, comunitarie ed internazionali o derivanti da disposizioni impartite da Autorità a ciò legittimate dalla legge;
  + dare esecuzione ad obblighi impartiti dall’autorità giudiziaria;
  + perseguire, eventualmente, un legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali;
  + applicazione alle normative in tema di rapporto di lavoro per la gestione dei dati assicurativi, previdenziali, fiscali, per la gestione delle cause di sospensione dal contratto (malattia, maternità e infortunio) o per richieste di permessi o aspettativa ovvero ancora per la fruizione di ogni altro diritto previsto dalle disposizioni in materia di diritto del lavoro o da altre disposizioni di legge nonché per gli adempimenti in materia di sicurezza sul lavoro e prevenzione degli infortuni e malattie professionali;
  1. dati utente
  + dati raccolti mediante strumenti telematici/informatici tramite sito internet a seguito di compilazione di richiesta di informazioni ai fini di gestione della richiesta di informazioni, contatto dell’utente e invio del relativo riscontro, sulla base del consenso espresso dall’utente medesimo e mendiate accettazione delle condizioni privacy esposte in informativa;
  + dati raccolti mediante strumenti telematici/informatici tramite cookies del sito internet per consentire all’utente di usufruire dei servizi presenti sul sito e per rendere più semplice e veloce la navigazione sul sito e meglio adattarlo agli interessi e bisogni dell’utente, soprattutto per le visite successive oltre che per garantire la normale navigazione e la gestione del sito e dei relativi applicativi; saranno presenti cookies di terze parti.

1. ***descrizione funzionale del trattamento***

Il trattamento dei dati personali, dei dati particolari raccolti ai sensi dell’art. 9 Reg. UE 2016/679 e dei dati di cui all’art. 10 Reg. UE 2016/679 per le finalità sopra indicate è costituito da – e definibile come – quanto previsto dall’art. 4 paragrafo 1, n.2 Reg. UE 679/2016.

Pertanto, la società pone in essere operazioni con dati trattati – mediante strumenti telematici, informatici o cartacei – di raccolta, registrazione, organizzazione, struttu­razione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione a mezzo mail/telefono/internet, raffronto o interconnessione, limitazione, cancellazione o distruzione.

1. ***dati personali trattati, destinatari e periodo di conservazione dei dati personali trattati***

6.1. dati personali trattati

* 1. dati clienti
  + dati personali identificativi diretti e indiretti della persona e solo eventualmente dati particolari ex art. 9 Reg. UE 2016/679 e dati di cui all’art. 10 Reg. UE 2016/679;
  + dati necessari per l’esecuzione dei servizi effettuati, delle commesse, dei servizi, dei contratti o di ogni altro rapporto giuridico in essere o in via di esecuzione o ancora in via di terminazione;
  + dati relativi al pagamento dei corrispettivi, delle fatture e necessari ai fini degli adempimenti fiscali e di legge;
  1. dati fornitori
  + dati personali identificativi diretti e indiretti della persona e solo eventualmente dati particolari ex art. 9 Reg. UE 2016/679 e dati di cui all’art. 10 Reg. UE 2016/679.
  + dati necessari per l’esecuzione dei servizi di fornitura effettuati, delle commesse, dei servizi, dei contratti o di ogni altro rapporto giuridico in essere o in via di esecuzione o ancora in via di terminazione;
  + dati relativi al pagamento dei corrispettivi, delle fatture e necessari ai fini degli adempimenti fiscali e di legge.
  1. dati di dipendenti, collaboratori, consulenti e professionisti
  + dati personali identificativi diretti e indiretti della persona ed eventualmente dati particolari ex art. 9 Reg. UE 2016/679 e dati di cui all’art. 10 Reg. UE 2016/679;
  + dati relativi al rapporto di lavoro/collaborazione/agenzia/consulenza necessari ai fini degli adempimenti contrattuali e degli adempimenti di legge;
  + dati contenuti nelle buste paga o nelle fatture;
  + dati relativi al pagamento delle retribuzioni dei dipendenti, delle fatture per compensi, anche necessari per l’esecuzione degli obblighi previdenziali assistenziali e fiscali;
  + in particolare, con riferimento ai dati dei dipendenti, dal trattamento dei dati personali anche particolari ai sensi degli artt. 9 e giudiziari di cui all’art. 10 Reg. EU 679/2016, può discendere il trattamento di dati personali sanitari relativi alla salute e alla vita sessuale, etnici, adesione a sindacati, adesione a partiti politici, adesione confessioni religiose, adesione ad enti o associazioni.
  1. dati utente
  + a seguito di richiesta di informazioni, verranno trattati dati personali identificativi diretti e indiretti della persona forniti dall’utente, tra i quali possibili: dati anagrafici, nome e cognome, indirizzi di domicilio/residenza, codice fiscale/p. iva, indirizzo e-mail, numeri di telefono, oltre alle informazioni inoltrate nel messaggio.
  + conseguentemente all’accesso al sito e all’accettazione del relativo avviso privacy, sono raccolti cookies di identificazione della sessione dell’utente. Potrebbero essere trattati dati relativi gli indirizzi IP o i nomi a dominio dei computer utilizzati dall’Utente per connettersi e navigare sul sito, gli indirizzi in notazione URI (Uniform Resource Identifier), l’orario della richiesta, il metodo utilizzato nell’inoltrare la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta dal server (buon fine, errore, ecc.), il paese di provenienza, le caratteristiche del browser e del sistema operativo utilizzati dal visitatore, le varie connotazioni temporali della visita (ad esempio il tempo di permanenza su ciascuna pagina) e i dettagli relativi all’itinerario seguito all’interno del sito, con riferimento alla sequenza delle pagine consultate, ai parametri relativi al sistema operativo e all’ambiente informatico dell’Utente. Sono cookies di terze parti e pertanto, per tali dati trattati, si rimanda alle relative privacy policies.

6.2. destinatari interni, esterni o terzi dei dati trattati

1. dei dati clienti
   * i destinatari preventivamente individuabili sono, per area/ufficio interni: amministrazione, ufficio appalti, ufficio contabilità;
   * i destinatari, preventivamente individuabili, di dati particolari nell’esercizio delle mansioni svolte risultano essere, in particolare, gli autorizzati impiegati nell’area amministrazione, ufficio appalti, ufficio contabilità;
   * fornitori della società;
   * consulenti esterni e professionisti in materia di lavoro, fiscale e legale; autorità competenti in materia lavoristica, previdenziale, fiscale e finanziaria e autorità statali in generale; autorità giudiziaria e consulenti che assisteranno la Società in eventuali procedimenti giudiziari;
   * consulenti e tecnici informatici esterni;
   * fornitori di servizi tecnici terzi, corrieri postali, servizi telematici e informatici, hosting provider, software gestionali;
   * i dati non più soggetti a trattamento finalizzato all’esecuzione del rapporto giuridico ma comunque di cui è necessaria l’archiviazione – e dunque la conservazione – per finalità fiscali, tributarie o finanziarie ovvero per legittimo interesse della società ovvero ancora per finalità relative ad obblighi di legge potrebbero essere oggetto di trasferimento a società specializzate nell’archiviazione esterna ovvero a professionisti a cui la Società si affida per tali servizi.
2. dai dati fornitori
   * i destinatari preventivamente individuabili sono, per area/ufficio interni: amministrazione, ufficio appalti, ufficio contabilità;
   * i destinatari, preventivamente individuabili, di dati particolari nell’esercizio delle mansioni svolte risultano essere, in particolare, gli autorizzati impiegati nell’area amministrazione, ufficio appalti, ufficio contabilità;
   * clienti della società;
   * consulenti esterni e professionisti in materia di lavoro, fiscale e legale; autorità competenti in materia lavoristica, previdenziale, fiscale e finanziaria e autorità statali in generale; autorità giudiziaria e consulenti che assisteranno la Società in eventuali procedimenti giudiziari;
   * consulenti e tecnici informatici esterni;
   * fornitori di servizi tecnici terzi, corrieri postali, servizi telematici e informatici, hosting provider, software gestionali;
   * i dati non più soggetti a trattamento finalizzato all’esecuzione del rapporto giuridico ma comunque di cui è necessaria l’archiviazione – e dunque la conservazione – per finalità fiscali, tributarie o finanziarie ovvero per legittimo interesse della società ovvero ancora per finalità relative ad obblighi di legge potrebbero essere oggetto di trasferimento a società specializzate nell’archiviazione esterna ovvero a professionisti a cui la Società si affida per tali servizi.
3. dei dati dipendenti, collaboratori, consulenti e professionisti
   * i destinatari preventivamente individuabili sono, per area/ufficio interni: Legale rappresentate/Titolare; amministrazione;
   * consulenti esterni e professionisti in materia di lavoro, fiscale e legale ovvero, in via generale, a liberi professionisti di cui la società si avvale quali medici, avvocati, commercialisti e consulenti tributari, fiscali o societari, anche in forma associata, nonché a Banche, Assicurazioni o Istituti di Credito, organizzazioni sindacali, fondi integrativi, organizzazioni imprenditoriali cui aderisce la Società; autorità competenti in materia lavoristica, previdenziale, fiscale e finanziaria e autorità statali in generale; autorità giudiziaria e consulenti che assistono la Società in eventuali procedimenti giudiziari;
   * consulenti e tecnici informatici esterni;
   * fornitori di servizi tecnici terzi, corrieri postali, servizi telematici e informatici, hosting provider, software gestionali;
4. dei dati utente
   * i destinatari preventivamente individuabili sono, per area/ufficio interni: amministrazione;
   * fornitori di servizi tecnici terzi, corrieri postali, servizi telematici e informatici, hosting provider, software gestionali, agenzie di comunicazione
   * in particolare, la gestione e manutenzione del sito internet è interamente affidata alla società Walter Marketing s.n.c. (p. iva 11091001005) con sede in via Francesco Carletti n. 18, 00154 – Roma

6.3 periodo di conservazione dei dati personali trattati

I dati personali trattati, con riferimento a clienti, fornitori, dipendenti, collaboratori, consulenti e professionisti, sono conservati durante la persistenza ed esecuzione del contratto in essere, contratto di lavoro, contratto di appalto, servizi o fornitura, consulenza ovvero qualsiasi altro rapporto giuridico o negoziale posto alla base del trattamento con la Società.

Inoltre, al termine del rapporto di qualsiasi genere o natura con la Società, i dati saranno conservati per il tempo necessario ai fini dell’adempimento degli obblighi di legge, specie in materia contributiva, fiscale, tributaria e comunque ai fini degli adempimenti di legge previsti per la singola tipologia di rapporto giuridico o negoziale sussistente.

Da ultimo, quanto alla policy relativa alla conservazione dei dati, la Società applica una *Record Retention Policy* (v. all. **2**).

Tale policy prevede limiti di conservazione – spirati i quali il documento è soggetto a eliminazione / distruzione – diversificati a seconda della tipologia di documento e dunque dei dati presenti all’interno del documento stesso prevedendo una ripartizione così suddivisa:

* + documenti conservabili fino 30 giorni;
  + documenti conservabili da 30 giorni fino ad un massimo di 12 mesi;
  + documenti conservabili da 1 a 5 anni;
  + documenti conservabili fino a 10 anni;
  + documenti conservabili senza previsione di un termine definito.

1. ***liceità del trattamento***

Il trattamento è svolto a seguito della verificazione delle sottoelencate condizioni o ragioni.

1. dati clienti

- gli interessati esprimono il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precon­trattuali adottate su richiesta dello stesso; il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

1. dati fornitori

gli interessati esprimono il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precon­trattuali adottate su richiesta dello stesso; il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

1. dati dipendenti, collaboratori, consulenti e professionisti

gli interessati esprimono il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precon­trattuali adottate su richiesta dello stesso; il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi.

1. dati utente

gli interessati esprimono il consenso al trattamento dei propri dati personali; il trattamento è necessario all'esecuzione del servizio – sia esso di richiesta informazioni ovvero di fruizione del sito internet – richiesto dall’utente.

# **b) VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO**

*[articolo 35, paragrafo 7, lettera b)]*

1. ***finalità determinate, esplicite e legittime***

*[articolo 5, paragrafo 1,* lettera b)]

* **valutazione:** accettabile

Quanto indicato al **punto a.4)** della presente risulta essere conforme alle previsioni del Reg. UE 679/2016 e in particolare a quanto previsto dall’art. 5, par. 1, lett. b) del Regolamento.

Le sopra esplicitate finalità [v**. punto a.4**]si ritengono determinate, esplicite e legittime in quanto:

* + necessarie all'esecuzione di un contratto (o comunque rapporto negoziale) di cui l'interessato è parte o all'esecuzione di misure precon­trattuali adottate su richiesta dello stesso.
  + necessarie a dare esecuzione ad obblighi di legge, regolamenti, normative nazionali, comunitarie ed internazionali o derivanti da disposizioni impartite da Autorità a ciò legittimate dalla legge;
  + necessarie al perseguimento del legittimo interesse del titolare del trattamento o di terzi;
  + è effettuato a fronte dell’espresso rilascio da parte degli interessati del consenso al trattamento dei dati personali per mezzo di informative recanti, tra le altre, le precise indicazioni delle specifiche finalità.

1. ***liceità del trattamento***

*[articolo 6]*

* **valutazione:** accettabile

La liceità del trattamento dei dati così come descritto nel paragrafo **a.7)** della presente PIA risulta essere conforme a quanto previsto dal GDPR e in particolare da quanto previsto dall’art. 5 del Reg. UE 679/2016. Nel dettaglio:

* con riferimento all’art. 6, par. 1, lett. a) Reg. EU 679/2016, gli interessati esprimono il consenso al trattamento dei propri dati personali per una o più specifiche finalità.
* con riferimento all’art. 6, par. 1, lett. b) Reg. EU 679/2016, il trattamento è svolto per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precon­trattuali adottate su richiesta dello stesso. Inoltre, la società si dotata di ogni misura necessaria al fine di mantenere il trattamento limitato alle finalità previste, a limitare il trattamento alla specifica esecuzione contrattuale. Inoltre, la Società si è dotata delle misure necessarie a trattare i dati particolari o dati giudiziari con particolare riguardo, tenendo conto – invero anche per i dati personali non particolari o giudiziari – delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati.
* con riferimento all’art. 6, par. 1, lett. c) Reg. EU 679/2016, il trattamento di una parte dei dati è altresì svolto per adempiere un obbligo legale. Tali obblighi discendono dal diritto nazionale italiano – precisamente ma non esclusivamente dalle normative giuslavoristiche, fiscali e tributarie – nonché dal diritto dell’Unione Europea – precisamente ma non esclusivamente dalle disposizioni in materia commerciale.
* con riferimento all’art. 6, par. 1, lett. f) Reg. EU 679/2016, il trattamento in alcuni casi – invero per la maggior parte eventuali – potrebbe essere necessario per il perseguimento del legittimo interesse della Società o di terzi. Ci si riferisce, in particolare, ai casi in cui i dati sono trattati al fine di dare esecuzione ad obblighi impartiti dall’autorità giudiziaria ovvero perseguire, eventualmente, proprio un legittimo interesse della Società nella gestione di eventuali contenziosi anche giudiziali;
* anche con riferimento al trattamento basato sul perseguimento di un legittimo interesse, i trattamenti svolti non ledono o prevalgono sugli interessi o i diritti e le libertà fondamentali dell'interessato. Infatti, anche per la natura dell’attività della Società risultano minimamente critici solo i trattamenti inerenti i dipendenti i quali però sono altresì fondati sulle ragioni di liceità di cui ai punti che precedono. Ad ogni modo, come già sopra specificato, la Società si è dotata delle misure necessarie a trattare i dati particolari o dati giudiziari con particolare riguardo, tenendo conto – invero anche per i dati personali non particolari o giudiziari – delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati.

1. ***dati personali adeguati, pertinenti e limitati a quanto necessario***

*[articolo 5, paragrafo 1, lettera c)]*

* **valutazione**: accettabile

Il trattamento dei dati, anche alla luce delle descrizioni di cui al **punto a)** della presente PIA, segue il criterio della minimizzazione come previsto dalla norma di cui all’art. 5, paragrafo 1, lett. c), per i dati di:

1. clienti
   * i dati trattati riguardano quelli strettamente necessari per la gestione organizzativa del contratto o del negozio in essere;
   * i dati trattati riguardano quelli strettamente necessari per la gestione contabile e amministrativa dei clienti e dei rispettivi contratti o commesse. In particolare, ci si riferisce ai dati necessari per l’esecuzione dei servizi effettuati, delle commesse e dei contratti o di ogni altro rapporto giuridico in essere o in via di esecuzione o ancora in via di terminazione; dati relativi al pagamento dei corrispettivi, delle fatture e necessari ai fini degli adempimenti fiscali e di legge;
   * il trattamento svolto – e dunque i dati raccolti – risulta minimizzato nei limiti di quanto strettamente necessario.
2. fornitori
   * i dati trattati riguardano quelli strettamente necessari per la gestione contabile e amministrativa dei fornitori e dei rispettivi contratti o commesse. In particolare, ci si riferisce ai dati necessari per l’esecuzione dei servizi di fornitura effettuati, delle commesse, dei servizi, dei contratti o di ogni altro rapporto giuridico in essere o in via di esecuzione o ancora in via di terminazione; dati relativi al pagamento dei corrispettivi, delle fatture e necessari ai fini degli adempimenti fiscali e di legge;
   * il trattamento svolto – e dunque i dati raccolti – risulta minimizzato nei limiti di quanto strettamente necessario.
3. dipendenti, collaboratori, consulenti e professionisti
   * i dati trattatati riguardano quelli strettamente necessari per la formulazione delle fatture e/o delle buste paga, ivi compresi eventuali dati particolari relativi alla salute e alla appartenenza a gruppi sindacali e per gli adempimenti previdenziali, assistenziali e fiscali;
   * con particolare riferimento ai dipendenti, come già più compiutamente indicato, il trattamento dei dati personali anche particolari ai sensi degli artt. 9 e giudiziari di cui all’art. 10 Reg. EU 679/2016 si rende necessario per l’applicazione alle normative in tema di rapporto di lavoro o ancora materia fiscale, assicurativa e previdenziale, ecc. Ad esempio, taluni dei dati sono trattati in via eventuale in caso di malattia ovvero ancora nei casi in cui il dipendente eserciti i suoi diritti in materia di diritto del lavoro o altre disposizioni di legge;
   * inoltre, anche l’accesso ai dati da parte di altri dipendenti è limitato in quanto tali dati sono trattati solo – e direttamente – dal Titolare e, solo eventualmente e su specifica delega ma comunque solo parzialmente, dall’ufficio amministrazione;
   * lo stesso dicasi per i professionisti esterni i quali sono autorizzati di volta in volta all’accesso ai dati strettamente necessari all’esecuzione del mandato/contratto/consulenza.
   * il trattamento svolto – e dunque i dati raccolti – risulta minimizzato nei limiti di quanto strettamente necessario.
4. Utenti
   * i dati trattati riguardano quelli strettamente necessari per la gestione ai fini di gestione della richiesta di informazioni, contatto dell’utente e invio del relativo riscontro nonché per consentire all’utente di usufruire dei servizi presenti sul sito e per rendere più semplice e veloce la navigazione sul sito e meglio adattarlo agli interessi e bisogni dell’utente;
   * Il trattamento svolto – e dunque i dati raccolti – risulta minimizzato nei limiti di quanto strettamente necessario.
5. ***limitazione della conservazione dei dati***

*[articolo 5, paragrafo 1, lettera e)]*

* **valutazione:** accettabile

Così come previsto dall’articolo 5, paragrafo 1, lettera e) i dati personali sono «*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*».

Inoltre, la società applica le procedure indicate e previste nella *Record Retention Policy* (RRP) adottata la quali risultano idonee ed in linea con quanto previsto dalle disposizioni normative relative ai limiti alla conservazione dei dati.

Infatti, al fine di garantire un limite di conservazione, la Società tratta i dati acquisiti mediante conservazione esclusivamente effettuata durante la persistenza ed esecuzione del contratto di service/lavoro/fornitura ovvero qualsiasi altro rapporto giuridico o negoziale posto alla base del trattamento con la Società.

Al termine del rapporto con la Società, di qualsiasi genere o natura, i dati saranno conservati per il tempo necessario al fine di adempimento degli obblighi in materia contributiva, fiscale, tributaria e comunque ai fini degli adempimenti di legge previsti per la singola tipologia di rapporto giuridico o negoziale sussistente.

Per quanto concerne i dati degli utenti del sito nonché degli utenti richiedenti informazioni commerciali a mezzo del form presente sul medesimo sito, i dati utenti trattati – v. punti 4.d), 6.1.d), 6.2.d) – saranno conservati, commisurando il grado di indispensabilità, per il solo tempo necessario a raggiungere lo scopo dell’attività in oggetto e dunque per il tempo necessario a gestire la richiesta dell’utente e a fornire il relativo riscontro. In ogni caso, i dati degli utenti non vengono conservati dalla Società per un periodo superiore a 365 giorni.

Quanto a cookies di terze parti, la durata del trattamento è evincibile dalle relative privacy policies.

1. ***Informazioni e diritti dell’interessato***

*[informazioni fornite all'interessato (articoli 12, 13 e 14); diritto di accesso e portabilità dei dati (articoli 15 e 20); diritto di rettifica e alla cancellazione (articoli 16, 17 e 19); diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21); rapporti con i responsabili del trattamento (articolo 28)]*

* **valutazione:** accettabile

La Società quando acquisisce dati personali, siano essi di clienti, fornitori, dipendenti, collaboratori, consulenti o professionisti, informa l’interessato di tutto quanto previsto dal Reg. EU 679/2016.

Le informative risultano idonee. Gli interessati vengono edotti di tutte le informazioni necessarie a norma di legge, viene loro riconosciuto il diritto di accesso, di portabilità, di rettifica, di cancellazione dei dati, di opposizione e di limitazione del trattamento, vengono indicati i nominativi del titolare e del responsabile nonché i recapiti della società e gli indirizzi di posta elettronica ai quali rivolgersi per l’esercizio dei predetti diritti.

Inoltre, gli interessati sono informati dell’esistenza di accordi di contitolarità ai sensi dell’art. 26 Reg. UE 679/2016 e sono informati della facoltà di richiedere che venga messo a disposizione il contenuto essenziale dell'accordo di contitolarità nel trattamento dei dati personali stipulato dalla società con altri contitolari del trattamento.

1. ***Contitolarità del trattamento***

*[articolo 26]*

Presso la sede della società sita in via Salomone Morpugno n. 8 – Roma, sono presenti le sedi operative delle società GHP s.r.l. e Mifin s.r.l. con le quali, pertanto sono condivise strumentazioni telematiche e informatiche. Tale rapporto è regolato da un accordo di contitolarità del trattamento dei dati personali ai sensi dell’art. 26 Reg. UE 679/2016.

Infatti, l’art. 26 Reg. EU 679/2016 stabilisce che «*allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14* […]».

* **valutazione:** accettabile

Nell’accordo sono stabilite responsabilità e obblighi relativi ai singoli contitolari e le modalità di collaborazione e assistenza in caso di esercizio dei diritti degli interessati e in caso di potenziale data breach.

# **c) VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI E MISURE PREVISTE PER AFFRONTARE I RISCHI E GARANTIRE LA PROTEZIONE DEI DATI; VALUTAZIONE *PROCEDURA INCIDENT RESPONSE PLAN***

*[articolo 35, paragrafo 7 lettere c) e d; articoli 33 e 34]*

1. ***rischio di accesso illegittimo ai dati***
   * **impatto sui soggetti interessati se tale rischio si dovesse realizzare**: perdita di riservatezza;
   * **principali minacce che potrebbero concretizzare il rischio**: accesso ai supporti informatici o cartacei;
   * **fonti di rischio:** esterne; dipendenti e non autorizzati;
   * **misure previste per gestire il rischio:** quanto al sistema tecnico e di sicurezza e alle modalità di trattamento si veda il **punto a)** della presente PIA; quanto alle misure di sicurezza adottate dalla società, si vedano punti 2), 3) e 6) delle misure di sicurezza tecniche e organizzative di cui all’all. **A)** alla presente.
   * **valutazione della gravità del rischio riguardo i potenziali impatti e misure previste:** medio;
   * **valutazione della probabilità del rischio in relazione alle minacce, alle fonti di rischio ed alle misure previste**: bassa;

* **valutazione di impatto:** accettabile

I sistemi tecnici e di sicurezza oltre che le modalità di trattamento indicate al punto a) della presente PIA nonché le misure di sicurezza adeguate adottate dalla società (v. **allegato A**), rendono il rischio di perdita di riservatezza degli interessati limitato e dunque la valutazione del rischio risulta accettabile.

1. ***rischio di modifiche indesiderate dei dati***
   * **impatto sui soggetti interessati se tale rischio si dovesse realizzare:** perdita di integrità dei dati;
   * **principali minacce che potrebbero concretizzare il rischio: errore umano,** comportamento doloso, errore non umano;
   * **fonti di rischio:** errore umano, accesso illegittimo e malfunzionamento impianto;
   * **misure previste per gestire il rischio:** quanto al sistema tecnico e di sicurezza e alle modalità di trattamento si veda il **punto a)** della presente PIA; quanto alle misure di sicurezza adottate dalla società, si vedano punti 2), 3) e 6) delle misure di sicurezza tecniche e organizzative di cui all’all. **A)** alla presente;
   * **valutazione della gravità del rischio riguardo i potenziali impatti e misure previste:** medio/basso;
   * **valutazione della probabilità del rischio in relazione alle minacce, alle fonti di rischio ed alle misure previste**: bassa;

* **valutazione di impatto:** accettabile

I sistemi tecnici e di sicurezza oltre che le modalità di trattamento indicate al punto a) della presente PIA nonché le misure di sicurezza adeguate adottate dalla società (v. **allegato A**), rendono il rischio di perdita di integrità dei dati degli interessati limitato e dunque la valutazione del rischio risulta accettabile.

1. ***rischio di perdita/scomparsa dei dati***
   * **impatto sui soggetti interessati se tale rischio si dovesse realizzare:** perdita di disponibilità dei dati;
   * **principali minacce che potrebbero concretizzare il rischio:** errore umano, comportamento doloso, errore non umano
   * **fonti di rischio:** errore umano, accesso illegittimo e malfunzionamento impianto
   * **misure previste per gestire il rischio:** quanto al sistema tecnico e di sicurezza e alle modalità di trattamento si veda il **punto a)** della presente PIA; quanto alle misure di sicurezza adottate dalla società, si veda si vedano punti 2), 3) e 6) delle misure di sicurezza tecniche e organizzative di cui all’all. **A)** alla presente.
   * **valutazione della gravità del rischio riguardo i potenziali impatti e misure previste:** medio/basso;
   * **valutazione della probabilità del rischio in relazione alle minacce, alle fonti di rischio ed alle misure previste**: bassa;

* **valutazione di impatto:** accettabile

I sistemi tecnici e di sicurezza oltre che le modalità di trattamento indicate al punto a) della presente PIA nonché le misure di sicurezza adeguate adottate dalla società (v. **allegato A**), rendono il rischio di perdita di disponibilità dei dati degli interessati limitato e dunque la valutazione del rischio risulta accettabile.

1. ***procedura di IRP - notifica violazione dei dati personali (data breach)***

La Società adotta la procedura di gestione delle eventuali violazioni della riservatezza dell’interessato nonché dell'integrità e della disponibilità dei dati.

Le procedure sono rese disponibili agli autorizzati e ai referenti all’atto di nomina.

Le modalità di azione, i controlli periodici e la revisione delle procedure da attivare in caso di allarme/verificazione della violazione dei dati personali sono demandata al Titolare con ausilio dei referenti privacy nominati.

* **valutazione di idoneità:** accettabile

1. ***procedura di riscontro delle richieste degli interessati***

La Società adotta una dettagliata procedura di gestione delle richieste degli interessati denominata *Subject Access Request* (SAR).

Le procedure sono rese disponibili agli autorizzati e ai referenti all’atto di nomina.

I protocolli previsti e programmati, i controlli periodici e la revisione delle procedure da attivare in caso di richieste ai sensi dell’art. 15 e ss. del Regolamento UE 2016/679 sono demandata al Titolare con ausilio dei referenti privacy nominati.

* **valutazione di idoneità:** accettabile

# **d) CONCLUSIONI**

1. ***analisi dei rischi – valutazione dei rischi***

Alla luce delle misure adottate l’analisi dei rischi restituisce un parametro generale di livello di impatto medio e livello di probabilità del rischio basso.

Il sistema di trattamento dei dati appare dunque idoneo e implementato secondo i limiti e le regole previste dal Reg. EU 679/2016 e della normativa in materia di protezione dei dati personali.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Molto**  **alto** |  |  |  |  |
| **Alto** |  |  |  |  |
| **Medio** | **c.1; c.2; c.3** |  |  |  |
| **Basso** |  |  |  |  |
|  | **Basso** | **Medio** | **Alto** | **Molto Alto** |

**Livello di impatto**

**Livello di probabilità del rischio**

1. ***consultazione preventiva***

*[art. 36]*

L’art. 36 paragrafo 1 del Reg. EU 679/2016 prevede che «*il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità̀ di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*».

Alla luce dei risultati della presente valutazione di impatto espletata ai sensi dell’art. 35 Reg. EU 679/2016, si deve ritenere non necessaria la procedura di consultazione preventiva prevista dall’art. 36 del medesimo Regolamento.

Pertanto, alla luce dei risultati della valutazione d’impatto ai sensi dell’art. 35 Reg. EU 679/2016 non si ritiene essere sussistente alcuna necessità di comunicazione ovvero interpello ovvero ancora procedura di consultazione preventiva di cui all’art. 36 Reg. EU 679/20126 all’Autorità Garante per la Protezione dei Dati Personali con riferimento ai trattamenti qui analizzati.

\*\*\*

In allegato:

1. Valutazione dei rischi e misure di sicurezza adeguate
2. *Password policy;*
3. *Record Retention Policy (RRP);*
4. *Incident responce plan* (*IRP*);
5. *Subject access reques* (*SAR*);

Roma, \_\_ / \_\_ / \_\_\_\_\_ Il Titolare del trattamento

## 

## **Storico del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Creato da** | **Data** | **Approvato da:** | **Data** |
| Gowen s.r.l. | 17/05/2019 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rev.** | **Modificato da** | **Data** | **Approvato da:** | **Data** |
| 01 |  |  |  |  |
| 02 |  |  |  |  |
| 03 |  |  |  |  |