MODELLO ORGANIZZATIVO *PRIVACY* DI EUDAIMON S.P.A.

Sommario

1. Premessa

1.1. Il Contesto normativo

Con il Regolamento Europeo in materia di protezione dei dati personali (UE) n. 2016/679 ("*General Data Protection Regulation*" nel seguito anche "Regolamento" o "GDPR") la Commissione Europea ha inteso rafforzare ed unificare la protezione dei dati personali entro i confini dell'Unione Europea (UE), enucleando il principio di *"accountability"* ossia di responsabilizzazione dei soggetti che pongono in essere attività di trattamento di Dati personali A tale riguardo, l'art. 24 GDPR prevede che il Titolare del trattamento adotti misure tecniche ed organizzative adeguate ed efficaci al fine di garantire che il trattamento dei Dati personali abbia luogo in conformità alle Leggi sulla protezione dei dati applicabili

1.2 La Società

Eudaimon S.p.A. (di seguito anche la "Società" o l'"Azienda") è una società specializzata nella fornitura e nella messa a disposizione di una vasta gamma di servizi di carattere sociale, ricreativo e assistenziale, a favore di persone fisiche e giuridiche, anche tramite la consulenza, la progettazione e l'organizzazione dei servizi offerti per conto dei propri clienti.

Nell'ambito della propria attività e per l'esecuzione della medesima, Eudaimon tratta sistematicamente Dati Personali sia internamente (Dipendenti) che esternamente (Clienti, Fornitori, Utenti).

1.3 Il Modello

I. Scopo e Finalità

In considerazione di quanto sopra esposto, Eudaimon S.p.A., ha ritenuto necessario adottare il presente Modello Organizzativo Privacy (nel seguito, anche "Modello Organizzativo" o "Modello" o "MOP") al fine di specificare i presidi organizzativi e di processo di cui si è dotata per garantire una tutela effettiva ed efficace dei Dati personali dalla stessa trattati in qualità di Titolare e/ o di Responsabile del Trattamento, anche ai fini dell'adempimento alle obbligazioni di cui all'art. 24 GDPR.

II. Ambito di applicazione e Destinatari

Il presente Modello Organizzativo si applica a tutti i trattamenti effettuati dalla Società ed è rivolto agli amministratori, dirigenti, dipendenti, collaboratori, Responsabili del trattamento dei dati, fornitori, consulenti e, in generale, a qualunque soggetto che opera per Eudaimon effettuando attività che implicano il trattamento di dati personali.

2. Definizioni

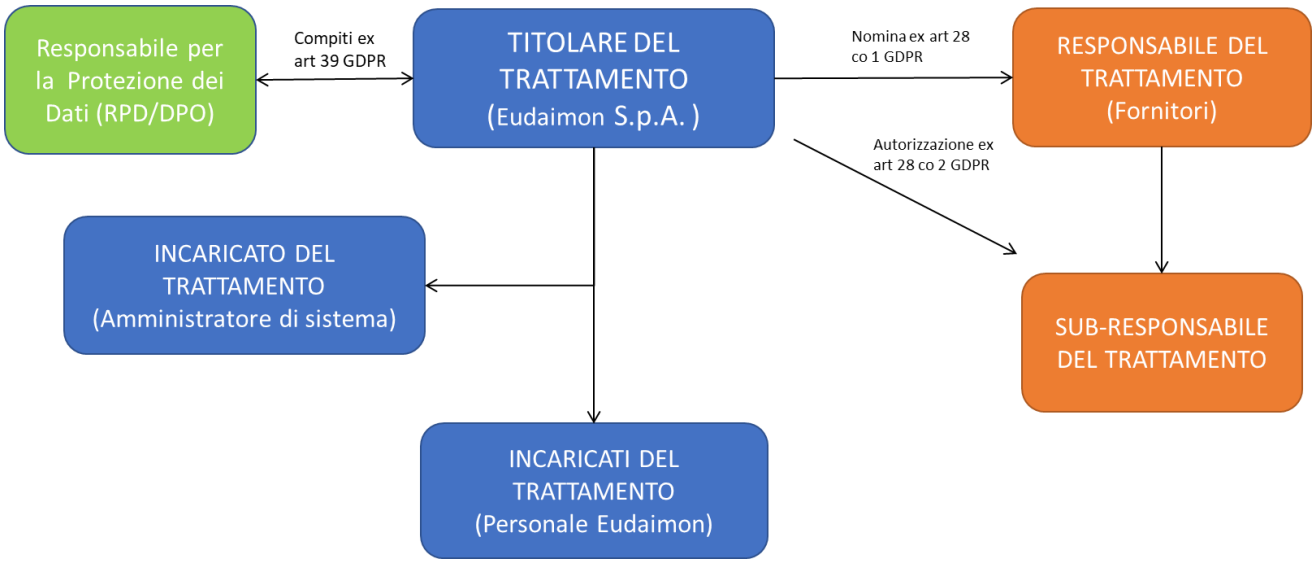
Ai fini del presente Modello Organizzativo, tutti i concetti specificamente coinvolti dalle attività di trattamento effettuate, direttamente ed indirettamente da Eudaimon S.p.A., hanno il significato loro riconosciuto ai sensi dal GDPR e dalle normative ad esso complementari o, in difetto, quello che verrà loro espressamente assegnato dal modello stesso. I termini al singolare manterranno lo stesso significato al plurale ove il contesto lo richieda e salvo diversa precisazione.
Si riportano di seguito alcune delle definizioni più rilevanti:

Dato Personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"); 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
Interessato	persona fisica a cui si riferiscono i Dati personali oggetto

	di trattamento
Trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare del trattamento	L'entità che determina le finalità e i mezzi del trattamento. Nello specifico la società **Eudaimon S.p.a.** (P.I./C.F. 03269680967) con sede legale in P.zza Pajetta n. 2, 13100 Vercelli (VC) - di seguito indicato, per brevità, anche ***"Eudaimon"***, ***"Società"*** o ***"Azienda"*** - nella persona dell'Amministratore Delegato **Dott. Cesare Concina.**
Responsabile della Protezione Dati (RPD) / Data Protection Officer (DPO)	Figura nominata dal Titolare chiamata ad informare e consigliare in merito agli obblighi imposti dal GDPR; Sorvegliare l'osservanza del GDPR e delle policy adottate; Collaborare con l'Autorità di controllo e gli interessati. Nello specifico l'**Avv. Giuliano Greppi**, nominato con Verbale del Consiglio di Amministrazione del 29/11/2022 (nomina comunicata all'Autorità Garante - prot. 20220008189).
Incaricato/Autorizzato al trattamento	soggetto che effettua operazioni di trattamento a qualsiasi titolo sotto la diretta autorità e secondo le istruzioni impartite dal Titolare.
Responsabile del Trattamento dei Dati	L'entità esterna che tratta Dati personali per conto del Titolare o di altro Responsabile (Sub-Responsabile)
Amministratore di sistema	figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Nello specifico il **Dott. Alessandro Brullo** – nominato con atto dell'Amministratore Delegato *pro tempore* del 07/03/2019.
Garante per la Protezione dei Dati Personali (c.d. *Garante per la Privacy*)	Indica l'Autorità di controllo Italiana designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51).

3. Ruoli e responsabilità

Il Modello Organizzativo Privacy di cui si è dotata la Società si articola su diversi livelli secondo lo schema riportato di seguito



4. I principi fondamentali del trattamento

Ogni trattamento di dati personali deve essere effettuato nel rispetto dei principi generali di cui all'articolo 5 GDPR:

a) **Principio di liceità, correttezza e trasparenza** che prescrive al soggetto che agisce sui dati personali la conformità alla legge del trattamento posto in essere e la trasparenza per l'interessato della raccolta e delle altre operazioni, vietando artifizi e raggiri. I dati personali trattati in violazione della normativa in materia protezione dei dati personali non possono essere utilizzati.

b) **Principio di limitazione della finalità:** secondo cui la raccolta dei dati deve essere collegata e funzionale alla finalità perseguita, che deve essere legittima, determinata e non incompatibile con l'impiego dei dati.

c) **Principio di minimizzazione dei dati**: che impone che, i dati personali trattati debbano essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento (laddove le stesse finalità possano essere perseguite anche senza l'uso di dati personali, il trattamento deve riguardare solo dati anonimi oppure deve essere posto in essere adottando opportune modalità che permettano di identificare l'interessato solo in caso di necessità).

d) **Principio di esattezza**: prevede che i dati trattati debbano essere non solo corretti e rispondenti a quanto raccolto, ma anche aggiornati, ed eventualmente rettificati, a richiesta dell'interessato, se sbagliati.

e) **Principio di limitazione della conservazione**: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento.

f) **Principio di integrità e riservatezza**: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Detti principi debbono permeare l'attività di chi effettua il trattamento, il quale deve ispirare la propria operatività ai criteri di:

- *Privacy-by-default*: che implica la necessità di prevedere, già in fase di progettazione del trattamento dati e dei sistemi informatici e applicativi, l'adozione di logiche di minimizzazione del trattamento e di disegno dello stesso sin dall'origine in linea coi principi in esame;
- *Privacy-by-design* (articolo 25): che implica l'implementazione da parte dell'organizzazione di un processo che preveda e disciplini le modalità di acquisizione, trattamento, protezione e modalità di diffusione dei dati personali, limitando la raccolta dei dati esclusivamente a quei dati personali realmente necessari per la realizzazione delle finalità perseguite, in

ottemperanza al principio di minimizzazione dei dati, e determinando sin dall'origine il periodo per il quale i dati personali raccolti dovranno essere conservati.

Tutti i dati devono essere trattati in modo responsabilizzato ed il Titolare, in ottemperanza al c.d. **Principio di Responsabilizzazione** (o "*accountability*"), è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che ciò avvenga.

4.1. Liceità

I Trattamenti effettuati dalle Società avvengono esclusivamente nel rispetto dei criteri di liceità individuati ai sensi dell'art. 6 del GDPR.

In particolare, il trattamento è lecito solo e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) L'Interessato ha espresso il **consenso** al trattamento dei propri Dati personali per una o più specifiche finalità;
b) 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;
c) Il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il Titolare;
d) Il trattamento è necessario alla **salvaguardia degli interessi vitali** dell'Interessato o di un'altra persona fisica;
e) Il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;
f) Il trattamento è necessario per il **perseguimento del legittimo interesse** del Titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei Dati personali, in particolare se l'Interessato è un minore.

Il Titolare ha provveduto ad individuare preventivamente il criterio per la legittimità dei trattamenti più comuni legati alla normale operatività aziendale.

I Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di Trattamento di Dati Personali, la sussistenza dei requisiti predeterminati o di almeno uno dei requisiti di liceità sopra indicati. In caso di dubbi relativi alla liceità del trattamento o in merito alla base giuridica da utilizzare in relazione allo specifico trattamento i Destinatari possono rivolgersi al Titolare e/o al RPD aziendale.

FOCUS: il Consenso

In base al GDPR (art. 4) si intende per "consenso" qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso esprime il proprio assenso al trattamento dei dati personali che lo riguardano.

Il consenso deve consistere in un atto positivo (Considerando 32) e non può, pertanto, configurare consenso il silenzio, l'inattività o la preselezione di caselle. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste e, nel caso in cui sia fornito nel quadro di una dichiarazione scritta riguardante anche altre tematiche, la richiesta di consenso dovrà essere presentata in maniera chiaramente distinguibile dagli altri temi.

Nel caso in cui il consenso al trattamento dei dati personali riguardi i minori, il consenso deve essere prestato da parte di un genitore o da chi esercita la responsabilità genitoriale.

I Titolari del trattamento dei dati devono essere in grado di dimostrare che l'interessato abbia effettivamente prestato il consenso e che lo stesso possa essere efficacemente ritirato o modificato.

Per approfondimento sulle caratteristiche del consenso e sulle modalità di acquisizione dello stesso, si rimanda alla **Procedura Privacy 1 – "*Trattamento Dati Personali*".**

4.2. Trasparenza

Il GDPR pone a carico del Titolare un obbligo di trasparenza nei confronti degli Interessati.

In particolare, ogni volta che vengono raccolti dati personali oggetto di trattamento, deve essere resa agli Interessati un'apposita informativa, la quale deve essere concisa, trasparente, intellegibile e facilmente accessibile, con linguaggio semplice e chiaro.
Ai sensi dell'art. 13 GDPR, le Informative rese agli Interessati devono contenere almeno le seguenti informazioni:

- Identità e dati di recapito del Titolare e, ove applicabile, del rappresentante del Titolare e del RPD;
- Le categorie di Dati personali raccolti e trattati, nonché la fonte da cui sono stati raccolti;
- Le finalità del Trattamento, nonché la base giuridica del Trattamento;
- Gli eventuali destinatari o le eventuali categorie di destinatari dei Dati personali;
- L'eventuale intenzione del Titolare di trasferire i Dati personali a paesi o organizzazioni internazionali terzi e l'esistenza o l'assenza di una decisione di adeguatezza da parte della Commissione Europea, ovvero il riferimento ad adeguate o idonee tutele, nonché i mezzi per ottenere una copia di tali dati o il luogo ove sono stati resi disponibili.
- Il periodo di conservazione dei Dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- L'esistenza dei seguenti diritti in capo all'Interessato:
  - *Diritto di accesso*
  - *Diritto di rettifica*
  - *Diritto di cancellazione*
  - *Diritto alla limitazione del trattamento*
  - *Diritto di opporsi al trattamento*
  - *Diritto alla portabilità dei dati*
  - *Diritto di proporre reclami all'Autorità Garante* (**GPDP – Garante per la Protezione dei Dati Personali**)
- Nel caso in cui il Trattamento si fondi sul Consenso dell'Interessato, è necessario informare quest'ultimo della possibilità di revocare il consenso precedentemente prestato in qualsiasi momento, senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca;
- Se la comunicazione di Dati personali è un obbligo legale o contrattuale ovvero un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i Dati personali, nonché le possibili conseguenze della mancata comunicazione dei Dati personali;
- L'esistenza di un processo decisionale automatizzato tra cui la profilazione e, (almeno) in tal caso, informazioni significative sulla logica adottata e la rilevanza e le conseguenze di tale trattamento per l'Interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, il Titolare, ai sensi dell'art. 14 GDPR, è comunque tenuto a fornire a quest'ultimo apposita informativa.
Eudaimon ha redatto e messo a disposizione degli Interessati le Informative relative ai trattamenti operati per tramite del proprio sito istituzionale (www.eudaimon.it).
Inoltre ha redatto e messo a disposizione dei Destinatari del presente modello le informative da utilizzare e fornire in relazione ai trattamenti più comuni legati alla normale operatività aziendale. I Destinatari sono tenuti a veicolare le Informative in favore degli interessati.
In caso di operazioni di Trattamento nuove e/o diverse, i Destinatari sono tenuti a coinvolgere il Titolare e/o il RPD al fine di verificare che l'Informativa precedentemente resa sia coerente con il nuovo trattamento che si intende effettuare e se vi sia o meno la necessità di informare nuovamente l'Interessato.

4.3. Proporzionalità, minimizzazione dei dati e limitazione della conservazione

Il Titolare può trattare i Dati personali solo ed esclusivamente per le finalità indicate al momento della raccolta degli stessi. In questo contesto, dovranno essere raccolti solo ed esclusivamente i dati "rilevanti", utili e funzionali al raggiungimento delle suddette finalità. Nel

caso in cui le finalità del trattamento fossero oggetto di modifica è necessario ottenere, ove necessario, il consenso da parte dell'Interessato per il perseguimento delle nuove finalità ovvero verificare se il perseguimento delle nuove finalità sia ammesso dalla normativa applicabile.
I Destinatari, in ogni caso di raccolta di dati e di trattamento degli stessi sono tenuti a verificare se la raccolta di tali dati è necessaria al conseguimento della finalità (ovvero se la finalità può comunque essere conseguita senza di loro) e/o se per raggiungere il risultato è necessario trattare quei dati (*posso raggiungere lo stesso la finalità indicata inviando meno dati o altri dati?*).
Il Titolare ha provveduto ad individuare i nuclei di dati necessari all'esecuzione delle attività connesse all'ordinaria operatività.
In caso di attività nuove o diverse e/o di dati ulteriori rispetto a quelli individuati, i Destinatari sono tenuti a coinvolgere il Titolare e/o il RPD al fine di ottenere maggiori informazioni e supporto nello stabilire la necessità e la pertinenza e/o, su come integrare le condizioni di legittimità del trattamento.

Fermo quanto precede, i Destinatari trattano i Dati personali per il tempo strettamente necessario a conseguire gli scopi per cui i Dati personali sono stati raccolti, a meno che obblighi legali prevalenti impongano periodi di conservazione più lunghi o più brevi. I Dati personali non più utilizzati devono essere distrutti o anonimizzati.
Inoltre, è stata predisposta uno specifico processo di gestione per la cancellazione dei dati personali gestiti successivamente alla cessazione del contratto in essere con le aziende clienti (rif. **Procedura 8 – "*Cancellazione Dati*"**).

5. Cookie

I "Cookie" sono di regola stringhe di testo che i siti web (cd. Publisher, o "prime parti") visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano ed archiviano – direttamente, nel caso dei publisher e indirettamente, cioè per il tramite di questi ultimi, nel caso delle "terze parti" - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo.
Il considerando 30 del GDPR espressamente afferma che *"Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei **(cookies**) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle"*.
Le informazioni codificate nei cookie possono quindi includere dati personali (come un indirizzo IP, un nome utente, un identificativo univoco o un indirizzo e-mail) e il loro utilizzo deve, pertanto, essere conforme alle disposizioni in materia di trattamento dei dati personali (cfr. "*Linee guida cookie e altri strumenti di tracciamento"* - Garante della Privacy - 10 giugno 2021).
Eudaimon ha reso i propri applicativi compliant con le prescrizioni dell'Autorità Garante e ha sintetizzato, a beneficio delle proprie persone, le regole per l'utilizzo dei cookie (rif. **Procedura 2 – "*Cookie*"**)

6. Misure di Sicurezza

Il GDPR impone al Titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
In adempimento di ciò, Eudaimon S.p.A. ha sviluppato e mantiene una serie di misure di natura tecnico-organizzativa finalizzata alla corretta e sicura gestione dei dati in termini di riservatezza, integrità e disponibilità, così come descritto nel documento ***White Paper Misure***

Tecniche ed Organizzative Eudaimon, redatto ai sensi dell'art. 30 par. 1 lett. g) e messo a disposizione, per fini informativi, a tutti gli stakeholder.
Per il mantenimento di un livello di sicurezza adeguato e per l'efficace applicazione di tali misure, il Titolare ha provveduto a redigere e mettere a disposizione dei Destinatari una serie di Policy relative al compimento delle più comuni attività e trattamenti legati all'ordinaria operatività aziendale.
Ogni Destinatario è tenuto a prendere visione e a conoscere le policy relative alle attività di propria competenza e ad uniformarsi al relativo contenuto durante la propria attività.

7. Soggetti autorizzati (Incaricati) e Responsabili del trattamento dei dati

Gli autorizzati trattamento (o Incaricato) sono tutte quelle persone fisiche che materialmente svolgono operazioni sui dati personali operando in subordinazione al Titolare del trattamento.
In tale categoria rientrano tutti i dipendenti e collaboratori di un'azienda che operano a qualsiasi titolo sotto la diretta autorità e secondo le istruzioni impartite dal Datore di lavoro/Titolare.
All'interno del modello di Governance privacy di Eudaimon, tutto il personale operativo riceve, al momento dell'instaurazione del rapporto, apposita nomina quale Incaricato del trattamento con cui vengono formalizzati gli impegni privacy e di riservatezza sui dati.

Inoltre, Eudaimon, nell'ambito della propria attività, si avvale della collaborazione di soggetti terzi, esterni all'organizzazione, i quali a vario, titolo, ricevono e trattano dati personali raccolti dalla Società.
In questo contesto, ogni qual volta un terzo effettui operazioni di Trattamento di Dati personali per conto di Eudaimon, l'azienda si impegna a nominare tale soggetto quale Responsabile del trattamento mediante apposito Atto di Nomina che, ai sensi dell'art. 28 GDPR, disciplina:

- la materia trattata
- la durata del trattamento
- la natura e la finalità del trattamento
- il tipo di dati personali e le categorie di interessati
- gli obblighi del Responsabile e i diritti del Titolare del trattamento.

A norma del regolamento, Eudaimon si impegna a ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti degli Interessati. Tali soggetti non sono autorizzati ad avvalersi di altro responsabile (sub-responsabile) senza l'espressa autorizzazione scritta di Eudaimon
Ogni Interessato può ottenere da Eudaimon, a semplice richiesta, l'elenco completo dei soggetti terzi, nominati Responsabili esterni del trattamento (nonché degli eventuali sub-responsabili), che trattano i suoi dati per conto dell'Azienda.

Per approfondimento sui principi e sulle regole alla base delle designazioni privacy si rimanda alla **Procedura 3 – "Nomina soggetti".**

8. Trasferimento dei Dati personali verso Paesi Terzi

Il GDPR stabilisce che il trasferimento di dati personali oggetto di trattamento (o destinati ad essere oggetto di trattamento dopo il trasferimento) verso un paese terzo (extra UE) può avvenire solo qualora ricorra almeno una delle seguenti condizioni:

A. art. 45 GDPR - il Paese terzo ha ricevuto da parte della Commissione Europea una **decisione di adeguatezza** (i paesi per cui è stata adottata una decisione di adeguatezza sono, ad oggi: Andorra – Argentina – Australia – Canada - Faer Oer – Giappone – Guernsey – Isola di Man – Israele – Jersey – Nuova Zelanda – Regno Unito UK – Svizzera – Uruguay)

B. il Titolare ha fornito **garanzie adeguate** e gli Interessati dispongono di diritti azionabili e mezzi di ricorso effettivi – art. 46 GDPR.
Possono costituire garanzie adeguate, a titolo esemplificativo:
- le norme vincolanti d'impresa;
- le clausole tipo di protezione dei dati adottate dalla Commissione Europea (*Standard Contractual Clauses*);
- le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione Europea;
- un codice di condotta ex art. 40 GDPR
- un meccanismo di certificazione approvato ai sensi dell'art. 42 GDPR

L'Azienda ha provveduto ad individuare le attività connesse alla propria normale operatività per cui è necessario/possibile un trasferimento di dati verso un paese terzo e ha curato la presenza di adeguate condizioni di legittimità per tale trasferimento. Ad eccezioni di tali fattispecie, non vengono effettuati trasferimenti di sorta.

In ogni caso, i Destinatari del presente Modello sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di trasferimento di Dati Personali, la sussistenza di almeno uno dei requisiti sopra indicati.
In caso di dubbi relativi alla possibilità di trasferire tali dati verso paesi terzi devono rivolgersi al RPD.

9. Violazioni di dati personali ("*Data Breach*")

Un *Data Breach* (circostanza cui il GDPR si riferisce come "Violazione dei dati personali") consiste in una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali oggetto di trattamento (art. 4 n. 12 GDPR).
Al verificarsi di un *Data Breach* il titolare deve effettuare alcune attività informative espressamente previste dal GDPR:

a) Notificare l'avvenuta violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (Art. 33 GDPR)

b) Comunica la violazione agli Interessati cui si riferiscono i dati violati senza ingiustificato ritardo (Art. 34 GDPR)

Non tutti casi di distruzione/perdita/modifica/divulgazione di dati rientrano nella definizione di *Data Breach* e, affinché esso si configuri, la violazione deve comportare un rischio per i diritti e le libertà delle persone.
Ciò significa che tale violazione deve essere suscettibile di avere un effetto significativo e dannoso sugli individui (ad esempio, causare discriminazione, danni alla reputazione, perdita finanziaria, perdita di riservatezza o qualsiasi altro significativo svantaggio economico o sociale).
Si rende quindi necessario effettuare una valutazione caso per caso al fine di verificare se sia occorso o meno un *Data Breach*.

In forza del principio di *accountability*, l'Azienda Titolare ha implementato una procedura operativa (rif. ***Procedura 6 – "Data Breach"***) tesa ad evitare il rischio di violazione dei dati e ad individuare le azioni necessarie da implementare tutte le volte in cui sia occorsa una violazione dei Dati personali ovvero vi sia una sospetta violazione dei Dati personali. A norma dell'art. 33 par. 5 GDPR, le violazioni rilevate e le relative circostanze e conseguenze nonché i provvedimenti adottati per porvi rimedio sono documentati e inseriti in apposito registro.
I Destinatari sono tenuti a seguire le linee guida della procedura e a segnalare ogni potenziale violazione dei dati di cui possano venire a conoscenza, inviando una e-mail all'indirizzo rpd@eudaimon.it

10. Diritti dell'Interessato

Il GDPR (al Capo III) riconosce agli Interessati una serie di Diritti:

- **Diritto di accesso (art. 15 GDPR)**
  L'Interessato potrà ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle relative informazioni
- **Diritto di rettifica (art. 16 GDPR)**
  L'Interessato potrà chiedere modifiche ai propri dati personali nel caso in cui l'interessato ritenga che tali dati personali non siano aggiornati o accurati
- **Diritto alla cancellazione (c.d. "*Diritto all'oblio*" - (art. 17 GDPR)**
  L'Interessato potrà richiedere la cancellazione dei Dati Personali trattati che lo riguardano, qualora non più necessari per le finalità per cui sono stati conferiti.
- **Diritto di limitazione del trattamento (art. 18 GDPR)**
  L'Interessato potrà, in alcune ipotesi specifiche (a. inesattezza dei dati per il periodo necessario alla correzione b. trattamento illecito c. esercizio del diritto di opposizione) ottenere la limitazione e quindi il blocco di un trattamento che lo riguarda
- **Diritto alla portabilità dei dati (art. 20 GDPR)**
  L'Interessato potrà trasferire i suoi Dati Personali verso un altro Titolare del Trattamento, ricevendo dai propri dati in un formato leggibile e strutturato
- **Diritto di opposizione (art. 21 GDPR) e di non sottoposizione a processo decisionale automatizzato (art. 22 GDPR)**
  L'Interessato potrà in qualsiasi momento, per motivi connessi alla sua situazione particolare, opporsi al trattamento dei dati personali che lo riguardano e, in particolare di far cessare qualunque trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona
- **Diritto di revoca del consenso**
  L'Interessato potrà revocare il consenso rilasciato per determinati trattamenti, senza pregiudicare la liceità dei trattamenti effettuati prima della revoca
- **Diritto di Reclamo (art. 77 GDPR)**
  L'Interessato potrà inoltre proporre reclamo al Garante per la Protezione dei Dati Personali, qualora dovesse ravvisare una violazione dei propri diritti ai sensi della normativa applicabile in materia di protezione dei dati personali

Il Titolare è tenuto a fornire all'Interessato una chiara informazione dei diritti a lui riconosciuti e delle modalità con cui li può esercitare, nonché ad agevolarne l´esercizio adottando ogni misura (tecnica e organizzativa) a ciò idonea.
Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22), il Responsabile è tenuto a collaborare con il Titolare ai fini dell'esercizio dei diritti degli Interessati (art. 28, paragrafo 3, lettera e).
Al fine di favorire e garantire il corretto ed efficace esercizio dei diritti da parte degli Interessati, Eudaimon ha predisposto e formalizzato un apposito processo di gestione (rif. ***Procedura 7 Diritti interessato***). L'anzidetta Procedura individua altresì i soggetti deputati alla gestione delle richieste avanzate dagli Interessati e le relative modalità e tempistiche di gestione delle richieste.
A tal riguardo, i Destinatari sono tenuti, in conformità con quanto previsto dalla Procedura, ad eseguire i compiti e le attività ad essi eventualmente assegnati e, in generale, ad assistere l'Azienda al fine di consentire allo stesso la corretta gestione delle richieste presentate dagli Interessati.

11. Registro delle attività di trattamento

Eudaimon ha provveduto a creare un apposito registro in cui sono mappate tutte diverse operazioni di trattamento dei Dati personali effettuate sotto la sua responsabilità.

Il Registro contiene tutte le informazioni di cui all'art. 30 par 1. Lett. a – d del GDPR e rappresenta un utile strumento per la completa ricognizione e valutazione dei Trattamenti effettuati, anche ai fini dell'analisi del rischio e della corretta pianificazione dei Trattamenti.
Il Titolare è responsabile alla corretta tenuta del Registro dei Trattamenti, nonché alla sua integrazione ed aggiornamento. A tale riguardo, i Destinatari sono tenuti ad assisterlo in tali compiti e a fornirgli tutti le informazioni necessarie per espletare correttamente le predette attività.
La Società ha redatto e mantiene aggiornato anche un registro di tutte le categorie di attività relative al trattamento svolte per conto di un diverso titolare del trattamento (art. 30 par. 2 GDPR).

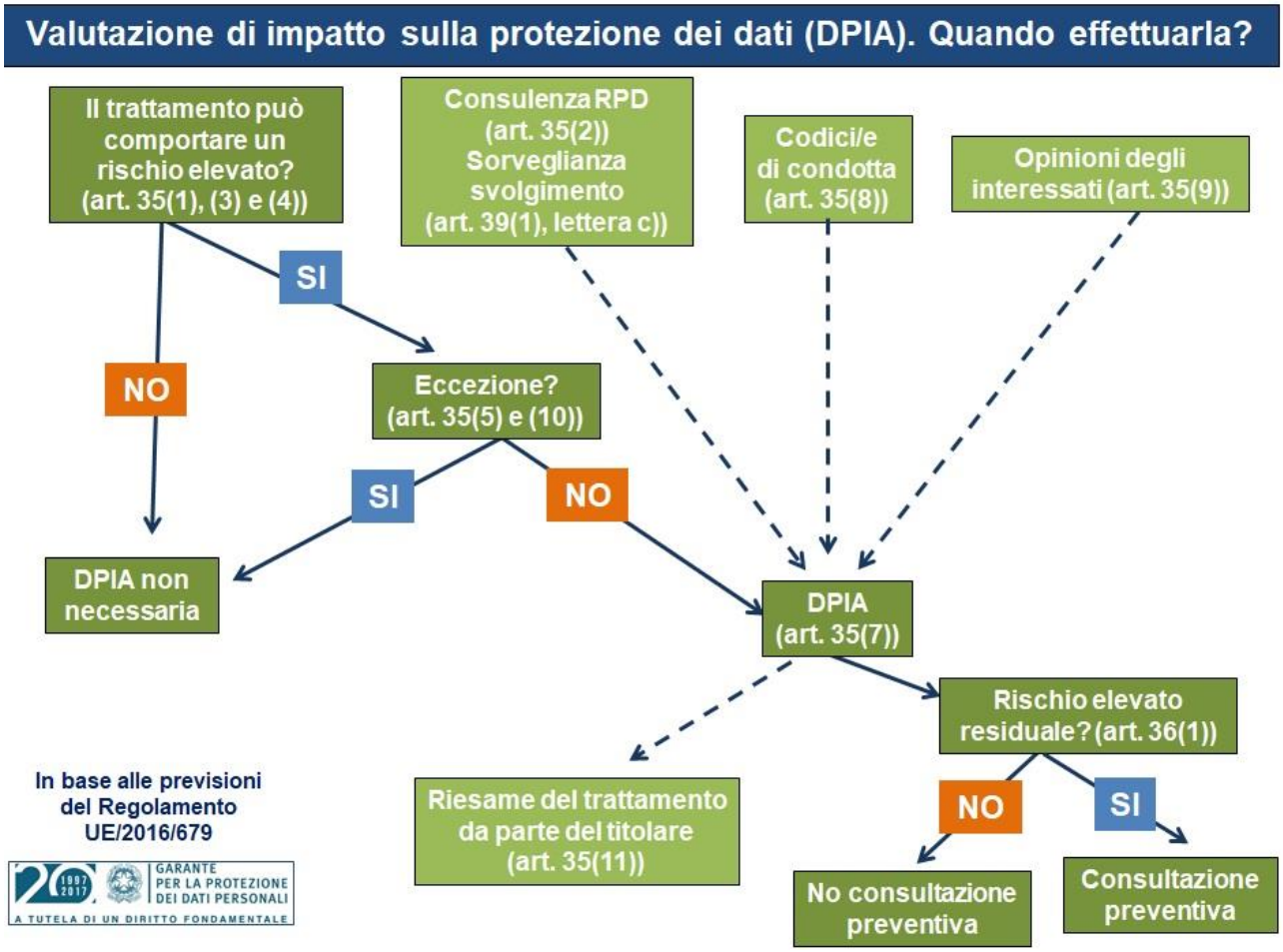
12. Valutazione d'Impatto sulla Protezione dei Dati

Tutte le volte in cui un determinato tipo di Trattamento dei Dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua, prima di procedere al trattamento, una valutazione dell'impatto (*Data Privacy Impact Assessment – DPIA*) dei trattamenti previsti sulla protezione dei Dati personali (art. 35 GDPR). Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi analoghi.
La DPIA è un processo progettato per descrivere il trattamento, valutare la necessità e la proporzionalità di un trattamento e per aiutare a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali (valutandoli e determinando le misure per affrontarli).
Le DPIA sono strumenti importanti per la responsabilizzazione (accountability) del titolare poiché lo aiutano
non solo a conformarsi ai requisiti del GDPR, ma anche a dimostrare che sono state prese misure appropriate per garantire la conformità al Regolamento.
La DPIA deve contenere

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nel caso in cui, all'esito della valutazione di impatto, il Titolare ritenga che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione e dovesse risultare dalla valutazione d'impatto che il trattamento (in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio) possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, dovrà ricorrere alla consultazione preventiva dell'Autorità ai sensi dell'art. 36 RGPD.

Si riporta di seguito la metodologia operativa (*flow chart*) elaborata dal Garante per la Privacy e messa a disposizione dei vari Titolare per verificare se è necessario procedere ad una valutazione d'impatto in relazione ai trattamenti posti in essere.



Eudaimon, dopo attenta valutazione ha prudenzialmente operato una DPIA in relazione ai trattamenti operati sui dati personali dei propri utenti (beneficiari e fruitori dei servizi di welfare) per finalità connesse all'erogazione dei propri servizi.
L'assessment ha avuto esito positivo rilevando impatti di tipo **Trascurabile** e **Limitato**.
La Società si propone di procedere ad un nuovo DPIA qualora dovessero verificarsi modifiche sostanziali nelle modalità di trattamento e/o dovessero essere introdotte nuove tipologie di trattamento.
In aggiunta e ad integrazione di quanto sopra, Eudaimon ha adottato e fatto proprio un approccio metodologico orientato al rischio (*"Risk-based approach"*) considerando debitamente e monitorando, nell'esecuzione dei propri compiti di Titolare del trattamento, i rischi e le minacce in termini di Riservatezza, Integrità e Disponibilità dei dati (rif. **Procedura 5 – "*Risk Assessment*"**).

13. Formazione

Per la corretta esecuzione delle operazioni di trattamento e per l'efficace funzionamento del presente Modello, Eudaimon cura la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

a) Onboarding

Nella fase di inserimento in azienda di nuovo personale, viene erogata alle singole risorse una sessione formazione specifica con modalità e-learning.
La formazione deve essere erogata entro i primi 15 giorni di attività e ha lo scopo di mettere i destinatari nelle condizioni di:

- ✓ acquisire conoscenza dei principi e dei contenuti del Trattamento dei Dati personali
- ✓ conoscere l'impostazione privacy osservata da Eudaimon

- ✓ conoscere le modalità operative con le quali deve essere realizzata la propria attività

L'efficacia del corso viene misurata con somministrazione di apposito questionario on-line finalizzato a valutare il grado di apprendimento conseguito e ad orientare ulteriori interventi formativi.

b) Aggiornamento

A livello generale, con cadenza annuale viene tenuto una sessione di formazione generale con scopo di aggiornamento, obbligatoria per tutto il personale in servizio presso la Società.
Tale evento, che solitamente si svolge nell'ultimo quarter dell'anno (ottobre-dicembre) verte su:

- Overview generale dell'impianto normativo e dell'impostazione Eudaimon
- Descrizione delle principali novità normative ed eventuali impatti sull'operato di Eudaimon
- Report sui trattamenti e sulle attività di sorveglianza della compliancy GDPR
- Aggiornamenti e/o variazioni intercorse
- Obiettivi di miglioramento

La sessione viene registrata ed Eudaimon ne cura la somministrazione differita (e-learning) agli assenti.
L'efficacia del corso viene misurata con somministrazione di apposito questionario on-line finalizzato a valutare il grado di apprendimento conseguito e ad orientare ulteriori interventi formativi.

14. Sanzioni

Il GDPR (art. 83) prevede, a fronte del compimento di violazioni del Regolamento, l'applicazione delle seguenti sanzioni amministrative pecuniarie:

- una multa fino a **10 milioni di euro** o, se superiore, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, nei casi previsti dal paragrafo 4 (i.e. mancato adempimento agli obblighi generali e specifici gravanti sul Titolare a norma del Regolamento);
- una multa fino a **20 milioni di euro** o, se superiore, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, nei casi previsti dal paragrafo 5 (i.e. violazione dei principi base del trattamento; dei diritti degli Interessati; delle regole generali sui trasferimenti extra UE).

Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, tenendo debito conto di elementi quali: la natura, la gravità e la durata della violazione; il carattere (doloso/colposo) della violazione; le misure adottate dal Titolare: eventuali precedenti violazioni.

L'art. 82 del GDPR, inoltre, disciplina il diritto al risarcimento e responsabilità in forza del quale chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

15. Rapporti con il Sistema di Gestione Integrato (SGI) ISO 9001:2015

Eudaimon ha da tempo adottato un Sistema di gestione Integrato (SGI) la cui conformità alla norma UNI EN ISO 9001:2015 - *Sistemi di gestione per la qualità,* è stata certificata da Certiquality S.r.l. Organismo di Certificazione accreditato facente parte di IQNet, (International Certification Network).
La certificazione è stata rilasciata per la prima volta in data 08/04/2019 e rinnovata, con nuova emissione in data 04/04/2022.

Eudaimon ha integrato nel proprio sistema di gestione diversi adempimenti in tema di trattamento dei dati personali, di modo da esplicitare ai propri operativi le modalità corrette con cui svolgere la propria attività nel rispetto delle prescrizioni del Regolamento Generale per la Protezione dei Dati.
Analogamente, la Società ha mutuato dal proprio SGI e, più in generale, dallo standard ISO, i criteri per la progettazione e l'implementazione del presente Modello organizzativo che, oltre a costituire uno strumento di garanzia e di dimostrazione della conformità normativa al GDPR, rappresenta un'estensione del suddetto Sistema di Gestione.

16. Rapporti con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001

Eudaimon S.p.A. si è dotata di un Modello di Organizzazione, Gestione e Controllo (MOGC), ai sensi del Decreto Legislativo 8 giugno 2001 n. 231, il cui scopo è la costruzione di un sistema strutturato ed organico di procedure e di attività di controllo, da svolgersi anche in via preventiva, volto ad evitare il rischio di commissione delle diverse tipologie di reato contemplate dal Decreto.
La decisione di dotarsi di tale modello è stata assunta nella convinzione che la sua adozione possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto di EUDAIMON, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari.
Il presente Modello Organizzativo Privacy si pone in continuità con le finalità del MOGC, costituendo un ulteriore Presidio di controllo posto dalla Società per evitare il rischio di incorrere in violazioni normative connesse al trattamento dei dati personali.

17. Inosservanza delle disposizioni del Modello Organizzativo Privacy

Il presente Modello Organizzativo, nonché le Procedure e le Policy che ne formano parte integrante e sostanziale, ha carattere vincolante per i Destinatari.
Eventuali comportamenti che costituiscono violazione del presente Modello possono avere gravi ripercussioni sulla Società la quale potrà essere perseguita e sanzionata in conseguenza della condotta dei Destinatari.
I Destinatari che pongono in essere condotte in violazione del presente Modello potranno ricevere una sanzione proporzionata, efficace e dissuasiva, nel rispetto e secondo i principi previsti dal Codice Civile, dallo Statuto dei Lavoratori (Legge 20 maggio 1970 n. 300) e dai Contratti Collettivi applicati.

18. Contatti

In caso di quesiti o dubbi in merito all'applicazione del presente Policy Privacy e/o in merito a qualsivoglia Procedura, si prega di contattare il Responsabile della Protezione dei Dati (RPD) all'indirizzo e-mail: rpd@eudaimon.it

19. Allegati

A. Procedure operative privacy
B. Documenti da utilizzare ai fini dell'applicazione del Modello Organizzativo Privacy
C. White Paper Misure Tecniche ed Organizzative Eudaimon