Valutazione d'impatto sulla protezione dei dati personali di PALERMO ENERGIA S.p.A., in relazione al "WHISTLEBLOWING", ai sensi degli artt. 25, 35 e del Considerando n. 84, 89 – 91 del Regolamento UE n. 2016/679, ai sensi del Provvedimento n. 17 del 23.1.2020 e n. 235 del 10.6.2021 del Garante Privacy italiano e ai sensi dell'art. 13 comma 6) del D. Lgs. n. 24/2023

Premesse.

Ancor prima di descrivere il trattamento in questione, **PALERMO ENERGIA S.p.A.**, (C. f. e P. IVA: 04939480820) (infra "PALERMO ENERGIA"), in persona del suo legale rappresentante pro tempore, con sede legale in Palermo, via Maqueda, 100,in qualità di Titolare del trattamento ex artt. 4 n. 7) e 24 del Regolamento UE n. 2016/679 (GDPR), precisa, in via preliminare, che la redazione della presente Valutazione d'impatto sulla protezione dei dati personali (DPIA) ex art. 35 del GDPR si è fondata (anche in via analogica), in particolar modo, sulle seguenti fonti normative (di primo e di secondo livello) e giurisprudenziali: documenti intitolati "Templates", "Methodology" e "Knowledge Bases" a firma della Commission NationaleInformatique&Libertes (CNIL); Linee Guida n. 248/2017 del Working Party Art. 29 (infra "WP 29"; ora, EDPB); Linee Guida n. 4/2019 dell'EDPB; Manuale sulla sicurezza nel trattamento dei dati personali dell'ENISA; Linee Guida per le PMI sulla sicurezza del trattamento dei dati personali dell'ENISA; Linee Guida n. 7/2020 dell'EDPB; Provvedimento n. 467 del 11.10.2018 a firma del Garante Privacy italiano; GDPR; D.Lgs. n. 196/2003 novellato (Codice Privacy); Carta dei diritti fondamentali dell'UE; Dichiarazione Universale dei Diritti Umani ONU del 1948; Costituzione italiana; Convenzione n. 108/1981 del Consiglio d'Europa, poi modernizzata nel 2018; Trattato sul funzionamento dell'UE; Legge n. 98 del 21.2.1989 (in ratifica della Convenzione di Strasburgo del 28.1.1981); documento intitolato "Guidance on AI and data protection" a firma dell'Information Commissioner's Office (ICO); ISO/IEC 29134/2017 ("Tecnologia dell'informazione–Tecniche di sicurezza–Linee guida per la valutazione dell'impatto sulla privacy"), e successiva versione del 5/2023; "Tool Kit sul test di necessità e di proporzionalità di una misura limitativa del diritto fondamentale alla protezione dei dati personali" a firma dell'EDPS del 11.4.2017; "Analisi del rischio e valutazione d'impatto nel trattamento dei dati personali" a firma dell'AEPD (AgenciaEspanolaProtectionDatos: Garante Privacy Spagnolo), Giugno 2021; "Linee guida dell'EDPS sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali" a firma dell'EDPS del 19.12.2019; documento n. 18/2017 intitolato "La nuova disciplina del whistleblowing" a firma di ASSONIME; documento intitolato "PAS 1998:2008. Whistleblowing Arrangements Code of Practice" a firma di British Standards (BSI); documento "Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)", Determinazione n. 6 del 28.4.2015 a firma dell'Autorità Nazionale Anticorruzione (ANAC); Parere n. 1/2006 del WP 29; documento "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)" a firma dell'ANAC; documento "Il whistleblowing" del 18.7.2019 a firma dell'Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs. n. 231/2001 (AODV); Provvedimento n. 215 del 4.12.2019 a firma del Garante Privacy italiano [doc. web n. 9215763]; documento "La disciplina in materia di whistleblowing. Nota illustrativa" del Gennaio 2018 a firma di Confindustria; Provvedimento n. 17 del 23.1.2020 a firma del Garante Privacy italiano [doc. web

n. 9269618]; documento "Linee guida sul trattamento dei dati personali all'interno di una procedura di whistleblowing" del Dicembre 2019 a firma dell'European Data Protection Supervisor (EDPS); Provvedimento n. 512 del 19.12.2018 a firma del Garante Privacy italiano [doc. web n. 9069653]; Provvedimento n. 235 del 10.6.2021 a firma del Garante Privacy italiano [doc. web n. 9685922]; Provvedimento n. 236 del 10.6.2021 a firma del Garante Privacy italiano [doc. web n. 9685947]; parere del Garante Privacy italiano del 12.5.2020 intitolato "Oggetto: richiesta di parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231"; ISO/IEC 37002:2021 (intitolata "Sistemi di gestione delle denunce. Linee guida"); D. Lgs. n. 24/2023; documento "La disciplina del whistleblowing: le novità introdotte dal D. Lgs. n. 24/2023 attuativo della Direttiva Europea n. 1937/2019" a firma dell'ANAC; documento "Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne" a firma dell'ANAC, approvato con Delibera n. 311 del 12.7.2023.

Passaggio 1: definizione dell'operazione di trattamento ed il suo contesto (art. 35 paragrafo 7) lettera a) del GDPR).

Questo primo passaggio rappresenta il punto di partenza della valutazione del rischio ed è fondamentale per PALERMO ENERGIA al fine di definire i confini del sistema di elaborazione dei dati qui valutato, ed il suo contesto di riferimento: in ragione di ciò, PALERMO ENERGIA deve, infatti, considerare le diverse fasi del trattamento dei dati (es. raccolta, conservazione ed utilizzo).
A tal fine, è necessario che il Titolare del trattamento si ponga le seguenti domande.

1a. Qual è l'operazione di trattamento dei dati personali?

Per quanto qui consta, PALERMO ENERGIA ha adottato una procedura ex art. 5 comma 1) lettera e) del D. Lgs. n. 24/2023, volta a consentire la ricezione, analisi, valutazione, verifica e gestione di una segnalazione di una circostanziata (presunta) violazione/condotta illecita ex artt. 1 comma 1) e 2 comma 1) del D. Lgs. n. 24 del 10.3.2023, fatta eccezione delle segnalazioni/contestazioni ex art. 1 comma 2) del D. Lgs. n. 24/2023 (infra "**segnalazione**" e/o "**whistleblowing**"), ivi incluse le conseguenti ed eventuali attività istruttorie/di accertamento e di protezione, ivi incluso l'eventuale esercizio del sistema disciplinare, nonché l'eventuale esercizio, tutela o difesa di un diritto, anche in sede giudiziale.

1b. Quali sono le tipologie di dati personali oggetto di trattamento?

A tal riguardo, PALERMO ENERGIA precisa che la segnalazione è potenzialmente idonea a contenere, per natura, i dati personali ex art. 4 n. 1) del GDPR del "**segnalante/whistleblower**" (a meno che la stessa venga effettuata in modalità anonima, nel rispetto dei provvedimenti di cd. soft law in materia), del "**segnalato/persona coinvolta**" e, in via eventuale, di ulteriori "**soggetti terzi**" (es. "facilitatore"; testimone; collega di lavoro del segnalante/segnalato), nonché può racchiudere i dati personali cd. particolari ex art. 9 paragrafo 1) del GDPR e/o i dati personali cd. giudiziari ex art. 10 del GDPR riferibili, direttamente o indirettamente, ad uno o più dei descritti soggetti: a tal riguardo, PALERMO ENERGIA evidenzia, ulteriormente, che si impegna a trattare solo quelle informazioni, contenute nella segnalazione, indispensabili ai fini dell'esecuzione della (macro) finalità in questione, provvedendo, pertanto, a cancellare e/o anonimizzare prontamente quelle informazioni a tal fine eccedenti e non necessarie, nel rispetto del principio di minimizzazione/di pertinenza/non eccedenza/indispensabilità ex art. 5 paragrafo 1) lettera c) del GDPR e art. 13 comma 2) del D. Lgs. n. 24/2023 (infra, per semplicità, solo "**dati personali**").

In merito, PALERMO ENERGIA precisa, altresì, che il "segnalante/whistleblower", il "segnalato/persona coinvolta" e/o il "soggetto/i terzo/i" rivestono, in modo singolare, la qualifica di soggetto interessato ex art. 4 n. 1) del GDPR.

1c. Qual è lo scopo del trattamento?

1c1. A tal fine, PALERMO ENERGIA persegue la seguente (macro) finalità di trattamento: **(i)**ricezione, analisi, valutazione, verifica e gestione di una segnalazione, ivi incluse le conseguenti ed eventuali attività istruttorie/di accertamento e di protezione, ivi incluso l'eventuale esercizio del sistema disciplinare, nonché l'eventuale esercizio, tutela o difesa di un diritto, anche in sede giudiziale (*basi giuridiche, oltre al citato D. Lgs. n. 24/2023: art. 6 paragrafo 1) lettera c) del GDPR, per i dati personali; art. 9 paragrafo 2) lettera f) del GDPR, per gli eventuali dati personali cd. particolari; art. 10 del GDPR (da leggersi, assieme, all'art. 2 octies commi 1) e 3) lettera e) del novellato Codice Privacy), per i dati personali cd. giudiziari*).

In relazione all'attività di analisi, valutazione, verifica e gestione di una segnalazione (ivi incluse le conseguenti ed eventuali attività istruttorie), PALERMO ENERGIA precisa che si impegna a rispettare, inter alia, le tutele di riservatezza previste dagli artt. 3 commi 4) e 5), e 12 del D. Lgs. n. 24/2023, nonché le misure di protezione di cui al relativo capo III).

1d. Quali sono i mezzi utilizzati per il trattamento dei dati personali?

I mezzi utilizzati per la (macro) finalità di trattamento in questione sono meglio descritti nell'apposita sezione del sito internet comunale, tra cui in particolar modo:

a. Piattaforma telematica (infra "piattaforma), accessibile e fruibile dal sito internet di PALERMO ENERGIA.

Nel dettaglio, occorre descrivere, di seguito, le principali caratteristiche della piattaforma (denominata "WHISTLEBLOWING PA"[1], fornita dall'impresa WHISTLEBLOWING SOLUTIONS IMPRESA SOCIALE S.R.L., e basata sul software GLOBAL LEAKS: stato di gestione della segnalazione da parte del segnalante, ivi incluso l'invio, nei confronti di quest'ultimo, di notifiche crittografate aventi ad oggetto una nuova comunicazione ovvero un aggiornamento sulle comunicazioni precedenti; possibilità di inviare la segnalazione in modalità anonima; possibilità di scambiare file tra PALERMO ENERGIA e il segnalante; chat con il segnalante; (auto) dichiarazione di conformità al GDPR, alla ISO 37002, agli standard OWASP e alla normativa di settore; svolgimento di penetration test multiplici, con rapporti pubblici completi; nessuna traccia nella chache del browser; protezione completa contro gli invii automatici (prevenzione dallo spam); soggetto a peer review continua, e audit di sicurezza periodici; no registrazione dell'indirizzo IP, delle informazioni sul browser; crittografia per il trasporto e la conservazione della segnalazione, ivi inclusa la documentazione eventualmente allegata; protocollo di rete sicuro HTTPS (Hypertext Transfer Protocol Secure), con certificati di grafo A+; piano di supporto a lungo termine (LTS); supporto di back up integrato; database integrato; supporto per MFA.

1e. Da parte di chi (e in che termini) avviene il trattamento dei dati personali

Il trattamento in questione viene effettuato da PALERMO ENERGIA per il tramite dei nominati soggetti cd. autorizzati/designati a trattare i dati personali del relativo soggetto interessato ai fini dell'esecuzione della (macro) finalità di trattamento in questione: nello specifico, si precisa che PALERMO ENERGIA ha individuato nel proprio nominato Responsabile della Corruzione e della

Trasparenza (RPCT) l'organo deputato, in via principale e preferenziale, alla ricezione di una segnalazione, ivi inclusa l'esecuzione della relativa attività istruttoria e di accertamento.

Con riguardo al termine di conservazione, PALERMO ENERGIA individua i seguenti periodi/criteri di conservazione, al termine del quale i dati personali, trattati per l'esecuzione della (macro) finalità di trattamento in questione, del relativo soggetto interessato saranno soggetti a cancellazione, distruzione ovvero anonimizzazione: **(i)**di norma, non oltre il termine di n. 5 anni, a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto dell'art. 14 comma 1) del D. Lgs. n. 24/2023; **(ii)** invece, nel caso in cui alla segnalazione segua un'azione giudiziaria e/o disciplinare nei confronti del segnalante e/o del segnalato, sino alla conclusione del relativo procedimento e allo spirare dei relativi termini di una eventuale impugnazione, criterio temporale eventualmente prorogabile ai fine di rispettare un onere normativo (anche sopraggiunto) ovvero per far valere o difendere un diritto, anche in sede giudiziale.

1f. Quali sono le categorie di soggetti interessati?
I soggetti interessati ex art. 4 n. 1) del GDPR coinvolti nel trattamento di specie sono stati meglio descritti nel precedente paragrafo 1b).

1g. Quali sono i destinatari dei dati?
I dati personali oggetto di trattamento possono essere comunicati, in via generale, alle seguenti categorie di destinatari ex art. 4 n. 9) del GDPR, ove opportuno o necessario: **(a)** per la (macro) finalità di trattamento di cui al precedente punto 1c1): soggetti autorizzati ex artt. 4 n. 10), 29 e 32 paragrafo 4) del GDPR al trattamento da parte di PALERMO ENERGIA (in primis, Responsabile della prevenzione, della corruzione e della trasparenza, nel rispetto dell'art. 4 comma 5) del D. Lgs. n. 24/2023); ANAC; autorità giudiziaria ordinaria/contabile; consulenti o imprese di varia natura che forniscono, comunque, servizi e/o prestazioni, anche professionali, connesse, anche in via indiretta, all'espletamento della (macro) finalità di trattamento in questione (es. società IT; consulente legale).
PALERMO ENERGIA precisa, altresì, che i dati personali del relativo soggetto interessato non saranno oggetto di alcuna diffusione ex art. 2 ter comma 4) lettera b) del Codice Privacy, ai fini dell'esecuzione della (macro) finalità di trattamento in questione.

Passaggio 2: valutazione della necessità e della proporzionalità del trattamento, in considerazione delle informazioni raccolte ed illustrate nel "Passaggio 1" di sopra (art. 35 paragrafo 7) lettera b) del GDPR).
Tenuto a mente l'art. 52 paragrafo 1) della Carta dei diritti fondamentali dell'UE ("Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'unione o all'esigenza di proteggere i diritti e le libertà altrui"), occorre, ora, effettuare un'analisi giuridica circa il rispetto del requisito di "necessità" e di "proporzionalità" applicato all'operazione di trattamento di specie.

Orbene, risulta necessario, innanzitutto, rilevare che il "**test di necessità**" si compone di quattro passaggi tra loro consecutivi:

1. Descrizione, in modo dettagliato, dell'operazione di trattamento di dati personali di specie;

2. Identificazione degli eventuali diritti e libertà fondamentali oggetto di eventuale limitazione in ragione dell'operazione di trattamento di dati personali di specie;
3. Descrizione della finalità di trattamento, la quale deve (realmente) soddisfare un obiettivo di interesse generale riconosciuto dall'UE, ovvero proteggere i diritti e le libertà altrui;
4. Valutazione circa l'appropriatezza, la reale efficacia (e la minor invadenza possibile, rispetto ad altre opzioni idonee a perseguire il medesimo obiettivo) dell'operazione di trattamento di dati personali di specie.

Con riguardo al caso de quo, si può sostenere, dunque, che l'operazione di trattamento, meglio descritta al precedente "Passaggio 1", persegue un obiettivo concreto ed effettivo, attraverso l'esecuzione di una attività di trattamento volta a svolgere un controllo (anche interno) mirato a pretendere l'esecuzione di un comportamento conforme ad un'etica (della legalità) / integrità/interesse aziendale/pubblicistico (cd. principio di buon governo societario, volto a garantirne il corretto funzionamento): il perseguimento di tale scopo può determinare la limitazione dei diritti del soggetto interessato nel rispetto dell'art. 2 undecies del Codice Privacy, senza che possa, tuttavia, registrarsi alcuna forma di disparità ovvero di discriminazione nei confronti di tale soggetto, aspetto invero ben regolamentato dalla normativa di settore.

Orbene, considerato l'esito positivo del preliminare test di necessità, occorre, ora, effettuare il conseguente "**test di proporzionalità**", nel rispetto del documento intitolato "Linee guida dell'EDPS sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali" a firma dell'EDPS del 19.12.2019, applicabile, in via analogica, al caso di specie.

Al pari del test di necessità, anche il test di proporzionalità si compone di quattro passaggi tra loro consecutivi:

1. Valutare l'importanza (e la legittimità) dell'obiettivo perseguito, nonché valutare, di conseguenza, se l'attività di trattamento perseguita soddisfa realmente tale obiettivo;
2. Valutare l'impatto sui diritti fondamentali di tale attività di trattamento[2];
3. Valutare gli aspetti intrinseci dell'attività di trattamento (es. vantaggio/svantaggio; costo/beneficio);
4. Assumere una decisione (es. sì/no) sull'attività di trattamento.

Tanto premesso, si afferma che, tenuto a mente l'esito positivo del preliminare test di necessità sopra svolto, l'operazione di trattamento, meglio descritta al precedente "Passaggio 1", è idonea, appropriata, necessaria, essenziale ed efficace a conseguire il (macro) obiettivo prefissato, al punto che i relativi vantaggi conseguiti (e conseguibili) vengono contro bilanciati, in senso positivo, dagli svantaggi/limitazioni registrabili in via potenziale ovvero effettiva.

Passaggio 3: comprensione e valutazione dell'impatto (art. 35 paragrafo 7) lettera c) del GDPR).
In questa fase, PALERMO ENERGIA è tenuta a valutare il potenziale impatto sui diritti e sulle libertà delle persone fisiche che potrebbe comportare un incidente di sicurezza (data breach), il quale può essere associato a qualsiasi tipologia di violazione della riservatezza, integrità ovvero della disponibilità dei dati personali.

3a. Livelli di impatto.
A tal fine, è necessario prendere in considerazione i seguenti 4 livelli di impatto (Basso; Medio; Alto; Molto Alto):

BASSO: Le persone possono incontrare alcuni inconvenienti minori che, però, possono superare senza problemi (es. tempo speso per reinserire le informazioni; fastidi; irritazioni);
MEDIO: Gli individui possono incontrare dei disagi significativi che saranno in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi; rifiuto di accesso ai servizi essenziali; paura; mancanza di comprensione; stress; disturbi fisici minori);
ALTO: Le persone possono incontrare delle conseguenze negative che dovrebbero essere in grado di superare anche se con gravi difficoltà (es. appropriazione indebita di fondi; inserimento nella lista nera da parte di istituzioni finanziarie; danni alla proprietà; perdita del lavoro; mandato di comparizione; peggioramento della salute);
MOLTO ALTO: Le persone possono subire delle conseguenze significative o addirittura irreversibili che potrebbero non superare (es. incapacità lavorativa; disturbi psicologici o fisici a lungo periodo; morte).

3b. Come valutare l'impatto.
La valutazione d'impatto può essere soltanto qualitativa, tenendo conto delle specificità di una particolare operazione di trattamento dei dati personali: a tal fine, soccorrono i seguenti criteri:

I. Tipologia dei dati personali: questo parametro può, per sua natura, aumentare o diminuire immediatamente il livello di impatto, in base alla criticità dei dati; tuttavia, la valutazione non può essere basata solo sulla distinzione delle categorie dei dati: infatti, anche i dati personali che non rientrano nella categoria "particolare" possono rivelare informazioni molto critiche su un individuo (es. posizione; abitudini; informazioni finanziarie) e, quindi, determinare significativi effetti in caso di violazione.
II. Criticità dell'operazione di trattamento: in merito, particolare attenzione deve essere prestata alle operazioni di trattamento che si basano o possono portare al tracciamento, monitoraggio o sorveglianza sistematica degli individui.
III. Volume dei dati personali trattati: questo parametro si riferisce alla quantità dei dati personali che viene elaborata per un singolo individuo; più sono i dati, maggiori sono i potenziali effetti negativi. Il volume dovrebbe essere considerato sia in termini di tempo (es. la stessa tipologia di dati per un certo periodo di tempo) che di contenuto.
IV. Particolarità del Titolare e/o del Responsabile del trattamento: questo parametro si riferisce al campo di attività ed alle attività essenziali dell'ente che, per loro natura, possono rivelare informazioni aggiuntive per un determinato set di dati (e, quindi, influenzare potenzialmente il livello di impatto).
V. Particolarità dei soggetti interessati: l'impatto potrebbe aumentare nel caso in cui gli interessati appartengono ad un gruppo sociale con esigenze particolari (es. minori).
VI. Identificabilità dei soggetti interessati (ovverosia, quanto sia facile per una parte che ha accesso al set di dati metterli in relazione univocamente con una determinata persona; per considerare l'identificabilità, si dovrebbe tenere in conto sia delle possibilità di identificazione diretta (es. nome della persona interessata) sia di quelle di identificazione indiretta (es. numero di identificazione o altro identificatore).
VII. Effetti secondari per i diritti e le libertà degli individui (es. quando il trattamento include l'username e la password, è necessario tenere conto del fatto che le persone tendono a

riutilizzare le stesse password sui diversi servizi online (e, quindi, una potenziale violazione di queste password potrebbe anche portare a ulteriori violazioni).

3c. Valutazione dell'impatto.
L'impatto deve essere valutato separatamente per perdita di riservatezza, perdita di integrità e, infine, perdita di disponibilità (n.d.r.: è importante considerare tutti i possibili casi di divulgazione, alterazione o distruzione non autorizzata ovvero accidentale e valutare l'impatto sulla base dello scenario peggiore).

- Riflettere sull'impatto che una divulgazione non autorizzata o accidentale (perdita di riservatezza) dei dati personali oggetto di trattamento potrebbe avere sul relativo soggetto interessato (es. un file cartaceo o laptop contenente dati personali viene perso; l'attrezzatura viene smaltita senza la preventiva distruzione dei dati personali; i dati personali vengono inviati erroneamente ad una serie di destinatari non autorizzati; alcuni clienti potrebbero accedere agli account di altri clienti).
  Valutazione: ☐ Basso ☐ Medio ✓ Alto ☐ Molto Alto.
- Riflettere sull'impatto che un'alterazione non autorizzata o accidentale (perdita di integrità) dei dati personali oggetto di trattamento potrebbe avere sul relativo soggetto interessato (es. è stato modificato un record necessario per la fornitura di un servizio online e l'individuo deve richiedere il servizio in modalità offline; è stato modificato un record per l'accuratezza della cartella di una persona in un servizio medico).
  Valutazione: ☐ Basso ☐ Medio ✓ Alto ☐ Molto Alto.
- Riflettere sull'impatto che una distruzione non autorizzata o accidentale (perdita di disponibilità) dei dati personali oggetto di trattamento potrebbe avere sul relativo soggetto interessato (es. danneggiamento database clienti; perdita di cartella personale e, pertanto, l'individuo deve fornire nuovamente alcune informazioni all'ente; un file viene perso/danneggiato e non viene eseguito il backup di queste informazioni; un servizio critico è inattivo (es. cartella clinica online) e non può essere recuperato immediatamente).
  Valutazione: ☐ Basso ☐ Medio ✓ Alto ☐ Molto Alto.

Dopo aver eseguito la suddetta valutazione, si ottengono tre diversi livelli di impatto (per perdita di riservatezza, di integrità e di disponibilità); il più alto di questi livelli deve essere considerato come il risultato finale.

Dunque, il livello di impatto è da considerarsi **ALTO**: a completamento ed a giustificazione della scelta effettuata, è opportuno osservare che l'eventuale "perdita di riservatezza" è potenzialmente idonea a determinare rilevanti conseguenze negative (es. discriminazione; conseguenze materiali/sociali/lavorative), tanto quanto le ipotesi di "perdita di integrità" e/o di "perdita di disponibilità", addirittura potenzialmente lesive, anche in modo rilevante, di aspetti sociali/lavorativi del relativo soggetto interessato.

Passaggio 4: definizione delle possibili minacce e valutazione della loro probabilità.
In proposito, si precisa che una minaccia è da definirsi come qualsiasi circostanza o evento che ha il potenziale di influire negativamente sulla sicurezza dei dati personali: dunque, lo scopo è quello di comprendere le minacce (interne ed esterne) legate al trattamento in questione, onde così valutarne la relativa probabilità.

4a. Come definire le minacce e la loro probabilità.

A tal fine, è opportuno formulare una serie di domande onde così agevolare la comprensione delle minacce e calcolare la relativa probabilità di accadimento; esse sono legate a quattro dimensioni/settori principali:

- Risorse di rete e tecniche (hardware e software): le connessioni di rete possono introdurre minacce sia da fonti esterne (es. aggressori esterni che mirano ad accedere da remoto al sistema o arrestare il sistema medesimo) sia da fonti interne (es. interconnessione con altri sistemi IT); le minacce comuni associate alle risorse di rete e tecniche includono l'intercettazione dei canali di comunicazione, l'accesso non autorizzato ai database, l'indisponibilità dei servizi forniti, l'interruzione dei collegamenti di comunicazione, l'uso improprio/anomalo dei sistemi di comunicazione.
- Processi/Procedure relative all'operazione di trattamento: in molti casi le minacce alla sicurezza derivano dalla mancanza di processi e procedure interne appropriate che impongono regole e pratiche specifiche all'interno dell'organizzazione per il trattamento dei dati personali; tali minacce includono l'accesso ai dati da parte di persone non autorizzate, la modifica/distruzione non autorizzata, lo smaltimento accidentale o la perdita di apparecchiature elettroniche.
- Diverse parti coinvolte nell'operazione di trattamento: minacce alla sicurezza possono derivare anche da coloro che eseguono il trattamento dei dati personali ovvero il personale della società coinvolto nel trattamento nonché altri soggetti che svolgono parte del trattamento.
- Settore di attività e scala del trattamento: il settore di attività di un'impresa, così come il volume dei dati elaborati, possono anche influenzare, in modo significativo, la tipologia ed il livello di minacce alla sicurezza (es. se la tipologia di dati personali è considerata una risorsa preziosa o se il trattamento riguarda l'intera popolazione di un paese).

Come annunziato, PALERMO ENERGIA procede a rispondere alle seguenti domande riguardanti i 4 settori sopra illustrati:

SEZIONE "RISORSE DI RETE E TECNICHE"

- Qualche parte del trattamento avviene tramite internet? Si.
- È possibile fornire l'accesso al sistema interno di elaborazione dei dati tramite internet? Si.
- Il sistema di trattamento è interconnesso ad un altro sistema IT esterno o interno all'ente? Si.
- Le persone non autorizzate possono accedere facilmente all'ambiente di elaborazione dei dati? No.
- Il sistema di elaborazione è stato progettato, implementato o mantenuto senza seguire le migliori pratiche? No.
- Non viene identificata ogni segnalazione pervenuta mediante l'attribuzione, ad essa, di un codice univoco (anche progressivo, ove necessario), registrando la data e l'ora di ricezione? No.
- Non viene garantito l'accesso sicuro e protetto alla piattaforma agli utenti autorizzati, mediante l'adozione di sistemi di autenticazione e autorizzazione opportuni? No.
- Non viene consentito, nel corso dell'istruttoria, lo scambio di messaggi/documenti tra segnalante ed organo istruttore, mediante meccanismi interni alla piattaforma tesi a tutelare l'identità del segnalante? No.

- Non viene consentito al segnalante di verificare, in qualsiasi momento, lo stato di avanzamento dell'istruttoria della segnalazione? No.
- Non è previsto un protocollo di rete sicuro? No.
- Non è previsto lo strumento della crittografia per il trasporto e la conservazione della segnalazione, ivi inclusa la relativa documentazione allegata? No.
- Non è previsto l'utilizzo di apposite credenziali di autenticazione in uso esclusivo dei soggetti autorizzati al trattamento? No.

SEZIONE "PROCESSI/PROCEDURE RELATIVE ALL'OPERAZIONE DI TRATTAMENTO"

- I ruoli e le responsabilità in relazione al trattamento dei dati personali sono vaghi o non chiaramente definiti? No.
- L'uso della rete, del sistema e delle risorse all'interno della società è ambiguo o non è chiaramente definito? No.
- Il personale autorizzato può utilizzare il proprio dispositivo per connettersi al sistema di elaborazione dei dati? Si, laddove necessario.
- Al personale autorizzato è consentito trasferire, archiviare o trattare in altro modo i dati personali al di fuori dei locali della società? No.
- È possibile eseguire attività di trattamento senza creare file di registro? No.

SEZIONE "PARTI COINVOLTE NELL'OPERAZIONE DI TRATTAMENTO"

- Il trattamento viene eseguito da un numero indefinito di dipendenti? No.
- Qualche parte dell'operazione di trattamento viene eseguita da una terza parte? Si.
- Gli obblighi delle parti coinvolte nel trattamento sono ambigui o non chiaramente indicati? No.
- Il personale autorizzato coinvolto nel trattamento non ha familiarità con questioni di sicurezza? No.
- Il personale autorizzato coinvolto nel trattamento trascura la sicurezza nella memorizzazione o conservazione dei dati? No.

SEZIONE "SETTORE DI ATTIVITA' E SCALA DEL TRATTAMENTO"

- Il (macro) settore ove opera PALERMO ENERGIA è incline ad attacchi informatici? No: infatti, in base all'ultimo rapporto di CLUSIT, gli attacchi cyber crime nel settore in cui opera PALERMO ENERGIA hanno registrato la seguente percentuale: 2,1 %.
- L'ente ha subito attacchi informatici o altre tipologie di violazioni negli ultimi due anni? No.
- Le operazioni di trattamento riguardano un grande volume di persone e/o di dati personali? No.
- Esistono best practices di sicurezza per il settore di attività di PALERMO ENERGIA che non sono state adeguatamente seguite? No.

4b. Valutazione della probabilità che si verifichi una minaccia.

La valutazione della probabilità che si verifichi una minaccia può essere soltanto qualitativa, dato che è strettamente correlata allo specifico ambiente di trattamento dei dati personali.

A tal fine, sono stati definiti tre livelli di probabilità di occorrenza di una minaccia, vale a dire:
BASSO: è improbabile che la minaccia si concretizzi;
MEDIO: è possibile che la minaccia si materializzi;
ALTO: è probabile che la minaccia si concretizzi.

A seguito della descrizione dei 3 sopra indicati livelli, PALERMO ENERGIA è tenuta a valutare la probabilità delle minacce per ciascuna delle 4 diverse aree sopra descritte (ovverosia, sezione "risorse di rete e tecniche", "processi/procedure relative all'operazione di trattamento", "parti coinvolte nell'operazione di trattamento" e "settore di attività e scala del trattamento").

Area di valutazione "RETE E RISORSE TECNICHE"
Probabilità di accadimento: ☐ Basso = Punteggio: 1.
✓ Medio = Punteggio: 2.
☐ Alto = Punteggio: 3.

Area di valutazione "PROCESSI/PROCEDURE RELATIVE ALL'OPERAZIONE DI TRATTAMENTO"
Probabilità di accadimento: ✓ Basso = Punteggio: 1.
☐ Medio = Punteggio: 2.
☐ Alto = Punteggio: 3.

Area di valutazione "PARTI COINVOLTE NELL'OPERAZIONE DI TRATTAMENTO"
Probabilità di accadimento: ✓Basso = Punteggio: 1.
☐ Medio = Punteggio: 2.
☐ Alto = Punteggio: 3.

Area di valutazione "SETTORE DI ATTIVITA' E SCALA DEL TRATTAMENTO"
Probabilità di accadimento: ✓Basso = Punteggio: 1.
☐Medio = Punteggio: 2.
☐ Alto = Punteggio: 3.

La probabilità finale del verificarsi di una minaccia viene calcolata dopo aver sommato il risultato dei 4 differenti passaggi ottenuti di sopra e dopo aver associato tale risultato alle scale della seguente tabella.

Scala di probabilità della minaccia	Livello di probabilità della minaccia
4 – 5	Basso
6 – 8	Medio
9 – 12	Alto

Atteso, dunque, che il punteggio del risultato di sopra è pari a 5, PALERMO ENERGIA deduce che il livello di probabilità della minaccia è da considerarsi **BASSO**.

Passaggio 5: valutazione del rischio.
Dopo aver valutato l'impatto dell'operazione di trattamento e la relativa probabilità di occorrenza della minaccia, è ora possibile effettuare la valutazione finale del rischio, mediante la seguente moltiplicazione:

PROBABILITA' DELLA MINACCIA x IMPATTO = LIVELLO DI RISCHIO

Nel caso specifico, PALERMO ENERGIA deduce che:

Basso (probabilità della minaccia) x Alto (Impatto) = **MEDIO** (livello di rischio).

Passaggio 6: opinione dei soggetti interessati e parere del nominato DPO (art. 35 paragrafi 2) e 9) del GDPR).
PALERMO ENERGIA precisa che, nel rispetto dell'art. 35 paragrafo 9) del GDPR, non ha ritenuto necessario raccogliere le opinioni, al riguardo, da parte dei relativi soggetti interessati, in ragione dell'esito finale della DPIA in parola giacché è stato considerato un adempimento sproporzionato ed impraticabile: in merito, il Titolare precisa che ha attuato, al riguardo, le misure di sicurezza prescritte dalla sezione A.2. ("Misure di sicurezza tecniche ed organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore MEDIO") del "Manuela sulla sicurezza nel trattamento dei dati personali" a firma dell'ENISA, e prescritte dagli atti di soft law emessi sul tema e meglio indicati nell'incipit del presente documento.
Infine, PALERMO ENERGIA ha domandato, in merito, l'opinione del nominato DPO (avv. Gabriele Borghi del Foro di Reggio Emilia), il quale ha formalmente rilasciato il proprio nulla osta (senza alcuna riserva ovvero eccezione) al trattamento in oggetto, meglio descritto nella presente DPIA.

Passaggio 7: convalida della DPIA da parte del Titolare del trattamento.
In conclusione, PALERMO ENERGIA convalida formalmente, in qualità di Titolare del trattamento, la presente DPIA.

Palermo, **lì 22/04/2025** (data di ultimo aggiornamento).

PALERMO ENERGIA S.p.A.
(in persona del suo legale rappresentante pro tempore)