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[1] 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[2] (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);

---

[1] Cfr. il relativo paragrafo 3.3.): "Al riguardo, si ritiene che il trattamento dei dati personali mediante i sistemi di acquisizione e gestione delle segnalazioni di presunte condotte illecite – in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore [...] – presenti rischi specifici per i diritti e le libertà degli interessati. Ciò, anche considerata, la "vulnerabilità" degli interessati (soggetti segnalanti e segnalati) nel contesto lavorativo...".

[2]Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne la necessità e la proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali; la DPIA è uno strumento importante in termini di accountability in quanto aiuta il Titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali precetti: in altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme.
Cfr., altresì, ISO/IEC 29134:2017: "Una valutazione dell'impatto sulla privacy (PIA) è uno strumento per valutare i potenziali impatti sulla privacy di un processo, sistema informativo, programma, modulo software, dispositivo o altra iniziativa che tratta informazioni personali identificabili (PII) e, in consultazione con le parti interessate, per intraprendere le azioni necessarie al trattamento del rischio di privacy. [...] Una PIA è più di uno strumento: è un processo che inizia nelle primissime fasi di un'iniziativa, quando ci sono ancora opportunità di influenzare il suo risultato e quindi garantire la privacy by design. È un processo che continua fino a quando, e anche dopo, il progetto è stato implementato"; "3.7. Valutazione dell'impatto sulla privacy PIA: processo globale di identificazione, analisi, valutazione, consultazione, comunicazione e pianificazione del trattamento dei potenziali impatti sulla privacy in relazione al trattamento delle informazioni personali identificabili, inquadrato nel più ampio quadro di gestione dei rischi di un'organizzazione"; 5.1. [...] una PIA può essere effettuata allo scopo di: identificare gli impatti sulla privacy, i rischi per la privacy e le responsabilità; fornire input al design per la protezione della privacy; esaminare i rischi per la privacy di un nuovo sistema informativo e valutarne l'impatto e la probabilità; fornire la base per la fornitura di informazioni sulla privacy ai committenti PII su qualsiasi azione di mitigazione PII raccomandata; mantenere gli aggiornamenti successivi e gli upgrade con funzionalità aggiuntive che potrebbero avere un impatto sulle PII che vengono gestite; condividere e mitigare i rischi per la privacy con le parti interessate, o fornire prove relative alla conformità. [...] Una PIA è stata spesso descritta come un sistema di allarme preventivo. Fornisce un modo per rilevare i potenziali rischi per la privacy derivanti dal trattamento delle PII e quindi informare un'organizzazione su dove dovrebbero prendere precauzioni e costruire salvaguardie su misura prima, non dopo, che l'organizzazione faccia grossi investimenti. I costi di modifica di un progetto in fase di pianificazione saranno di solito una frazione di quelli sostenuti in seguito. [...] Quindi, una PIA aiuta a identificare precocemente i problemi di privacy e/o a ridurre i costi in termini di tempo di gestione, spese legali e potenziali preoccupazioni dei media o del pubblico considerando i problemi di privacy in anticipo. Può anche aiutare un'organizzazione a evitare errori di privacy costosi o imbarazzanti. Anche se una PIA dovrebbe essere più di un semplice controllo di conformità, essa contribuisce comunque alla dimostrazione da parte di un'organizzazione della sua conformità con i requisiti di privacy e protezione dei dati rilevanti nel caso di un successivo reclamo, audit sulla privacy o indagine di conformità. Nel caso in cui si verifichi un rischio o una violazione della privacy, il rapporto PIA può fornire la prova che l'organizzazione ha agito in modo appropriato nel tentativo di prevenire l'evento. Questo può aiutare a ridurre o addirittura eliminare qualsiasi responsabilità, pubblicità negativa e perdita di reputazione". Cfr. ISO/IEC 29134:2023: "Un'organizzazione deve condurre una PIA nuova o aggiornata se percepisce impatti sulla privacy da: una tecnologia, un servizio o un'altra iniziativa nuova o futura in cui le PII sono o saranno trattate; una decisione che prevede il trattamento di PII sensibili; modifiche alle leggi e ai regolamenti applicabili in materia di privacy, alle politiche e agli standard interni, al funzionamento del sistema informativo, alle finalità e ai mezzi di elaborazione dei dati, ai flussi di dati nuovi o modificati; espansione dell'attività o acquisizioni. È possibile che un'organizzazione desideri stabilire una politica che definisca le soglie per l'attivazione di una PIA nuovo o aggiornato e le misure tecniche e organizzative iniziali da applicare".

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)[3].

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?[4]

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[5] di una circostanziata[6] (presunta) violazione/condotta illecita[7] ex artt. 1 comma 1) e 2 comma 1) del D. Lgs. n. 24 del 10.3.2023[8], fatta eccezione delle

---

[3]E ai sensi del paragrafo 6.3.3) e ss. della ISO/IEC 29134:2023.

[4] Un punto importante da considerare è che potrebbe eventualmente essere preferibile eseguire diversi processi di valutazione del rischio per diverse operazioni di trattamento dei dati, anche se questi sono gestiti attraverso gli stessi mezzi tecnici (es. reti IT; sistemi; applicazioni); ciò è particolarmente importante nel caso di operazioni che coinvolgono dati di diversa natura e sensibilità e che, quindi, comportano, diversi livelli di rischio per l'interessato.

[5]Cfr. art. 2 comma 1) lettera c) del D. Lgs. n. 24/2023: "segnalazione" o "segnalare": "la comunicazione scritta od orale di informazioni sulle violazioni". Cfr. anche: art. 2 comma 1) lettera d) del D. Lgs. n. 24/2023: "segnalazione interna": "lacomunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna di cui all'articolo 4"; art. 2 comma 1) lettera e) del D. Lgs. n. 24/2023: "segnalazione esterna": "la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'articolo 7"; art. 2 comma 1) lettera f) del D. Lgs. n. 24/2023: "divulgazione pubblica" o "divulgare pubblicamente": "rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone".

[6] Cfr. art. 2 comma 1) lettera b) del D. Lgs. n. 23/2023: "informazioni sulle violazioni": "informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base degli elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali informazioni". Anche solo in via analogica, cfr. il 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 (cd. whistleblowing)" a firma dell'Autorità Nazionale Anticorruzione (ANAC), paragrafo 2.3.: "E' necessario che la segnalazione sia il più possibile circostanziata [...]. In particolare, è necessario risultino chiare: le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione; la descrizione del fatto; le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti. Cfr., altresì, sul punto, in via analogica, il documento "La disciplina in materia di whistleblowing. Nota illustrativa", Confindustria, gennaio 2018: "Tali denunce, inoltre, devono essere circostanziate e fondate su elementi di fatto precisi e concordanti, così da non disperdere l'efficacia della nuova misura e agevolare, invece, l'emersione di condotte che con molta probabilità risulteranno illecite". Cfr. infine, sul punto in via analogica, il documento "Il whistleblowing" a firma dell'Associazione dei Componenti degli Organismi di Vigilanza ex D. Lgs. n. 231/2001 (AODV), 18.7.2019: "...le segnalazioni possono essere fatte solo agendo in buona fede e che, pertanto, non sono considerate meritevoli di tutela le segnalazioni fondate su meri sospetti o voci. Sul punto si ritiene condivisibile il criterio indicato dalle Linee guida ANAC per qualificare la segnalazione in base al quale non è "necessario che il dipendente sia certo dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi. Si ritiene, invece, sufficiente che il dipendente, in base alle proprie conoscenze, ritenga altamente probabile l'essersi verificato un fatto illecito nel senso sopra indicato".

[7] Cfr. art. 2 comma 1) lettera a) punti 2), 3), 4), 5) e 6) del D. Lgs. n. 24/2023: "violazioni": "comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in: "2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazione dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6)"; "3) illeciti che rientrano nell'ambito di applicazione degli atti dell'unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; sicurezza degli alimenti e dei mangimi e salute e benessere

segnalazioni/contestazioni ex art. 1 comma 2)[9] del D. Lgs. n. 24/2023 (infra "**segnalazione**" e/o "**whistleblowing**"), ivi incluse le conseguenti ed eventuali attività istruttorie/di accertamento e di protezione[10], 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?[11]

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**"[12] (a meno che la stessa venga effettuata in modalità anonima, nel rispetto dei provvedimenti di cd. soft law in materia), del "**segnalato/persona coinvolta**"[13] e, in via eventuale, di ulteriori "**soggetti terzi**" (es. "facilitatore"[14]; 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?[15]

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

---

degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi"; "4) atti od omissioni che ledono gli interessi finanziari dell'unione di cui all'articolo 325 del Trattato sul funzionamento dell'unione europea specificati nel diritto derivato pertinente dell'unione europea"; "5) atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'unione europea, comprese le violazioni delle norme dell'unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società"; "6) atti o comportamenti che vanificano l'oggetto delle disposizioni di cui agli atti dell'unione nei settori indicati nei numeri 3), 4) e 5)".

[8] Intitolato: "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali".

[9] Art. 1 comma 2) del D. Lgs. n. 24/2023: "Le disposizioni del presente decreto non si applicano: a) alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate; b) alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'unione europea o nazionali indicati nella parte II dell'allegato al presente decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al presente decreto; c) alle segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'unione europea".

[10]Cfr. Capo III) del D. Lgs. n. 24/2023 (da leggersi, in combinato disposto, con i relativi artt. 3 comma 5) e 12).

[11] Le tipologie di dati personali possono, da un lato, aiutare a definire l'operazione di trattamento, mentre dall'altro lato possono dare una prima indicazione del potenziale livello di rischio.

[12] Cfr. art. 2 comma 1) lettera g) del D. Lgs. n. 24/2023: "persona segnalante": "la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo". Per la definizione di "contesto lavorativo", cfr. art. 2 comma 1) lettera i) del D. Lgs. n. 24/2023: "contesto lavorativo": "le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile". Cfr., anche, art. 3 comma 3) del D. Lgs. n. 24/2023: "3. Salvo quanto previsto nei commi 1 e 2, le disposizioni del presente decreto si applicano alle seguenti persone che segnalano, denunciano all'autorità giudiziaria o contabile o divulgano pubblicamente informazioni sulle violazioni di cui sono venute a conoscenza nell'ambito del proprio contesto lavorativo: a) i dipendenti delle amministrazioni pubbliche [...]; b) i dipendenti degli enti pubblici economici, degli enti di diritto privato sottoposti a controllo pubblico ai sensi dell'articolo 2359 del codice civile, delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio; c) i lavoratori subordinati di soggetti del settore privato, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n.96; d) i lavoratori autonomi [...] i titolari di un rapporto di collaborazione [...] che svolgono la propria attività lavorativa presso soggetti del settore pubblico; e) i lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore pubblico [...] che forniscono beni o servizi o che realizzano opere in favore di terzi; f) i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico; g) i volontari e i tirocinanti, retribuiti e non retribuiti, che forniscono la propria attività presso soggetti del settore pubblico; h) gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico".

[13]Cfr. art. 2 comma 1) lettera l) del D. Lgs. n. 24/2023: "persona coinvolta": "la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente".

[14] Cfr. art. 2 comma 1) lettera h) del D. Lgs. n. 24/2023: "facilitatore": "una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata".

[15]La finalità è direttamente collegata all'operazione di trattamento e può aiutare l'ente a comprendere i limiti del trattamento; nel corso del trattamento potrebbe essere necessario distinguere le operazioni di trattamento dei dati in base allo scopo, anche quando si tratta della stessa tipologia dei dati.

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*[16]*; 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[17] 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?[18]
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 internetdi PALERMO ENERGIA.
Nel dettaglio, occorre descrivere, di seguito, le principali caratteristiche della piattaforma (denominata "WHISTLEBLOWING PA"[19], 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?[20]
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

---

[16]Ed art. 6 paragrafo 1) lettera a) del GDPR, al ricorrere delle ipotesi ex art. 12 commi 2) e 5) del D. Lgs. n. 24/2023.

[17]"1. Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. 2. L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2 quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196. 3. Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale. 4. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria. 5. Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. 6. È dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, nella ipotesi di cui al comma 5, secondo periodo, nonché nelle procedure di segnalazione interna ed esterna di cui al presente capo quando la rivelazione della identità della persona segnalante e delle informazioni di cui al comma 2 è indispensabile anche ai fini della difesa della persona coinvolta. 7. I soggetti del settore pubblico e del settore privato, l'ANAC, nonché le autorità amministrative di cui l'ANAC trasmette le segnalazioni esterne di loro competenza, tutela l'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante. 8. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. 9. Ferma la previsione dei commi da 1 a 8, nelle procedure di segnalazione interna ed esterna di cui al presente capo, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti".

[18] Il trattamento dei dati personali potrebbe avvenire in modo automatizzato o non automatizzato o in entrambi i casi, comprese particolari reti, sistemi o applicazioni informatiche; l'ente potrebbe anche fare affidamento parzialmente o totalmente sui mezzi tecnici di un responsabile del trattamento dei dati per la fornitura del servizio. È importante, quindi, comprendere chiaramente le modalità del trattamento, prestando particolare attenzione al fatto che queste possono cambiare nelle diverse fasi del trattamento.

[19]È un servizio qualificato ACN, dal 19.1.2023 (livello di qualificazione: QC1); piattaforma cloud attraverso la quale è erogato il servizio: VMware; reti di accesso: rete internet (ridondata su operatori: Cogent, MINMAP, AMSIX AMS-IX, TIM, MIX, NTT, GTT), rete tor.

[20] L'ubicazione dei dati personali è un fattore importante, soprattutto quando vengono utilizzati i servizi del Responsabile del trattamento ex art. 28 del GDPR. È importante notare che, quando i dati personali vengono elaborati in un paese terzo extra SEE devono essere messe in atto i relativi e necessari meccanismi di protezione di cui al Capo V) del GDPR.

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?[21]
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?[22]
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[23], 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"[24] e di "proporzionalità"[25] applicato all'operazione di trattamento di specie.

Orbene, risulta necessario, innanzitutto, rilevare che il "**test di necessità**" si compone di quattro passaggi[26] tra loro consecutivi:

---

[21] Definire chiaramente i soggetti interessati è importante per l'ente come parte della comprensione dell'operazione di trattamento dei dati; in alcuni casi, a seconda delle categorie di soggetti interessati è già possibile ottenere un'indicazione del potenziale livello di rischio in questa fase.
[22] La definizione dei destinatari aiuta a comprendere le comunicazioni e/o i trasferimenti autorizzati; infatti, alcune volte tali attività possono comportare dei rischi specifici che già in questa fase è opportuno che l'organizzazione riconosca.
[23] La necessità e la proporzionalità di una misura legislativa che comporti una limitazione dei diritti fondamentali alla privacy e alla protezione dei dati personali sono un duplice requisito essenziale a cui deve conformarsi qualsiasi misura proposta che implichi il trattamento dei dati personali: è essenziale sottolineare che la necessità e la proporzionalità, anche se legate l'una all'altra, comportano due test diversi.
[24] Cfr. documento "Valutazione della necessità delle misure che limitano il diritto fondamentale alla protezione dei dati personali. Tool Kit" a firma dell'EDPS del 11.4.2017: "La necessità implica una valutazione combinata, basata sui fatti, dell'efficacia della misura rispetto all'obiettivo perseguito e della sua minore invasività rispetto alle altre opzioni per il raggiungimento dello stesso obiettivo. La necessità è anche un principio di qualità dei dati e una condizione ricorrente in quasi tutti i requisiti sulla liceità del trattamento dei dati personali derivanti dal diritto derivato dall'UE in materia di protezione dei dati. [...] Dalla giurisprudenza della CGUE deriva che la condizione di stretta necessità è orizzontale indipendentemente dal settore in questione [...] Una misura proposta dovrebbe essere supportata da prove che descrivano il problema che la misura deve affrontare, come sarà affrontato dalla misura e perché le misure esistenti e meno invasive non possono affrontarlo sufficientemente. Un'analisi della giurisprudenza della CGUE e della Corte EDU indica che la necessità nel diritto alla protezione dei dati è un concetto basato sui fatti, piuttosto che una nozione giuridica meramente astratta, e che il concetto deve essere considerato alla luce delle circostanze specifiche che circondano il caso nonché le disposizioni del provvedimento e lo scopo concreto che si prefigge di raggiungere".
[25] Cfr. documento "Valutazione della necessità delle misure che limitano il diritto fondamentale alla protezione dei dati personali. Tool Kit" a firma dell'EDPS del 11.4.2017: "Secondo costante giurisprudenza della CGUE, "il principio di proporzionalità esige che gli atti delle istituzioni dell'unione siano idonei a conseguire gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non eccedano i limiti di quanto è opportuno e necessario per il raggiungimento di tali obiettivi" (cfr. CGUE, causa C-62/2014, Gauweiler, punto 67). La proporzionalità in senso lato comprende sia la necessità che la appropriatezza di una misura, vale a dire la misura in cui esiste un nesso logico tra le misure e l'obiettivo (legittimo) perseguito [...] i vantaggi derivanti dalla misura non dovrebbero essere controbilanciati dagli svantaggi che la misura provoca rispetto all'esercizio dei diritti fondamentali. Quest'ultimo elemento descrive la proporzionalità in senso stretto e costituisce il test di proporzionalità. [...] c'è una certa sovrapposizione tra le nozioni di necessità e proporzionalità, e a seconda della misura in questione le due prove possono essere svolte contemporaneamente o addirittura in ordine inverso. In linea di massima, tuttavia, occorre innanzitutto accertare se sia necessaria una limitazione di un diritto fondamentale prima di procedere alla valutazione della proporzionalità.".
Cfr. CGUE, Causa C-257/06, Productores de Musica de Espana (Promusicae) contro Telefonica de Espana SAU: "il requisito della proporzionalità all'interno di una società democratica – o proporzionalità strictosensu – deriva sia dall'articolo 15, paragrafo 1, della direttiva 2002/58 e dall'articolo 52, paragrafo 1, della Carta, sia da una giurisprudenza consolidata: è stato costantemente affermato che una misura che interferisce con i diritti fondamentali può essere considerata proporzionata solo se gli svantaggi causati non sono proporzionati agli scopi perseguiti".
[26] Ogni passaggio è composto da una serie di domande volte a facilitare la valutazione di necessità. Se la valutazione di uno qualsiasi degli elementi dettagliati nei passaggi da 2) a 4) porta alla conclusione che una misura potrebbe non soddisfare il requisito della necessità, allora la misura non dovrebbe essere proposta ovvero dovrebbe essere riconsiderata in linea con il risultato del test di necessità.

1. Descrizione, in modo dettagliato, dell'operazione di trattamento di dati personali di specie[27];
2. Identificazione degli eventuali diritti e libertà fondamentali oggetto di eventuale limitazione in ragione dell'operazione di trattamento di dati personali di specie[28];
3. Descrizione della finalità di trattamento[29], la quale deve (realmente) soddisfare un obiettivo di interesse generale[30] riconosciuto dall'UE, ovvero proteggere i diritti e le libertà altrui[31];
4. Valutazione circa l'appropriatezza, la reale efficacia[32] (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[33]): il perseguimento di tale scopo può determinare la limitazione dei diritti del soggetto interessato nel rispetto dell'art. 2 undecies del Codice Privacy[34], 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[35], occorre, ora, effettuare il conseguente **"test di proporzionalità"**[36], nel rispetto del documento intitolato "Linee guida dell'EDPS sulla valutazione della proporzionalità delle misure

---

[27] L'operazione di trattamento deve essere sufficientemente descritta al fine di consentire una chiara comprensione di cosa esattamente si vuole svolgere, e per quale finalità di trattamento; a tal fine, è opportuno porsi, anche in modo implicito, i seguenti quesiti: (i) determinare se la misura implica l'uso di dati personali; (ii) in caso di trattamento di dati personali, descrivere: obiettivo (anche di interesse generale, ove esistente); categorie di dati personali; soggetti interessati; destinatari dei dati; ove necessario, operazioni di trattamento previste (es. raccolta; conservazione); durata del trattamento.

[28] Cfr. Cfr. documento "Valutazione della necessità delle misure che limitano il diritto fondamentale alla protezione dei dati personali. Tool Kit" a firma dell'EDPS del 11.4.2017: "A tal riguardo, la costante giurisprudenza della CGUE afferma che "per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, non importa se le informazioni sono sensibili o se le persone interessate sono state in qualche modo arrecate. [...] Il rifiuto di consentire all'interessato l'opportunità di confutare i dati conservati e consultati (cioè, il diritto di accesso e di rettifica dei dati) costituisce anche una limitazione del suo diritto al rispetto della vita privata"; oltre a tali aspetti, è necessario verificare, in particolar modo, se sussiste una potenziale differenza di trattamento tra gli individui, idonea a creare delle discriminazioni.

[29] La finalità di trattamento deve essere concreta, effettiva e, dunque, non meramente ipotetica.

[30] Cfr. documento "Valutazione della necessità delle misure che limitano il diritto fondamentale alla protezione dei dati personali. Tool Kit" a firma dell'EDPS del 11.4.2017: "Gli obiettivi di interesse generale dell'UE comprendono, ad esempio, gli obiettivi generali di cui all'art. 3 o 4, paragrafo 2, TUE e altri interessi tutelati da specifiche disposizioni dei trattati, così come interpretato nella giurisprudenza della CGUE".

[31] Sono da intendersi, in primo luogo, quelli sanciti dalla Carta dei diritti fondamentali dell'UE.

[32] La misura deve essere realmente efficace, ossia essenziale per raggiungere l'obiettivo perseguito. Non tutto ciò che potrebbe rivelarsi utile per un determinato scopo è desiderabile o può essere considerata una misura necessaria in una società democratica; la semplice convenienza o convenienza in sé non è sufficiente (cfr. Parere n. 9/2004 e n. 3/2012 del WP Art. 29). Se la misura proposta prevede il trattamento di dati personali cd. particolari, è opportuno applicare una soglia più alta circa la valutazione dell'efficacia della stessa.

[33] Cfr. sul punto: Comunità Europea, Raccomandazione della Commissione del 15 febbraio 2005; OCSE, documento "Principi OCSE sul governo societario", 2004.

[34] Cfr., in via analogica, 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" a firma dell'ANAC, paragrafo 3.1.: "La norma richiamata stabilisce che, nell'ambito di una segnalazione whistleblowing, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati [...], non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) n. 2016/679, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante".

[35] Se la valutazione della misura porta alla conclusione che soddisfa il requisito della necessità, allora essa può essere sottoposta al conseguente test di proporzionalità. In altre parole, in base al test di proporzionalità la misura, valutata come necessaria, viene ulteriormente vagliata al fine di verificare se essa è proporzionata all'obiettivo che si vuole perseguire.

[36] Il concetto di proporzionalità è un concetto giuridico ben consolidato nel diritto dell'UE; è un principio generale del diritto dell'UE che richiede che "il contenuto e la forma dell'azione dell'unione non eccedano quanto necessario per raggiungere gli obiettivi..." (cfr. art. 5, paragrafo 4, TUE). Secondo la giurisprudenza consolidata della CGUE, "il principio di proporzionalità esige che gli atti delle istituzioni dell'UE siano appropriati al raggiungimento degli obiettivi legittimi perseguiti dalla legislazione in questione e non superino i limiti di ciò che è appropriato e necessario per raggiungere tali obiettivi" (cfr. CGUE, Causa C-62/2014, par. 67; e Causa C-331/88, par. 13: "Per quanto riguarda il controllo della proporzionalità, il principio di proporzionalità, che è uno dei principi generali del diritto comunitario, esige che le misure adottate dalle istituzioni comunitarie non superino i limiti di ciò che è appropriato e necessario per raggiungere gli obiettivi legittimamente perseguiti dalla normativa in questione; quando vi è una scelta tra più misure appropriate si deve ricorrere a quella meno onerosa e gli svantaggi causati non devono essere sproporzionati rispetto agli scopi perseguiti". Quindi la proporzionalità in senso lato comprende sia la necessità che l'adeguatezza (proporzionalità in senso stretto) di una misura, cioè la misura in cui vi è un legame logico tra la misura e l'obiettivo legittimo perseguito. Affinché una misura rispetti il principio di proporzionalità sancito dall'art. 52 paragrafo 1) della Carta dei diritti fondamentali dell'UE, i vantaggi che ne derivano non devono essere controbilanciati dagli svantaggi che la misura comporta per l'esercizio dei diritti fondamentali: in sostanza, tale principio richiede un equilibrio tra i mezzi utilizzati e lo scopo (o il risultato raggiunto) voluto. Un test di proporzionalità implica generalmente la valutazione di quali "garanzie" dovrebbero accompagnare una misura al fine di ridurre i rischi posti dalla misura prevista per i diritti e le libertà fondamentali degli individui interessati ad un livello "accettabile/proporzionato". Il principio di proporzionalità è stato incorporato nell'art. 5 paragrafo 1) della "Convenzione 108" modernizzata che prevede: "Il trattamento dei dati deve essere proporzionato rispetto alla finalità legittima perseguita e riflettere in tutte le fasi del trattamento un giusto equilibrio tra tutti gli interessi coinvolti, pubblici o privati, e i diritti e le libertà in gioco". Al centro della nozione di proporzionalità c'è il concetto di bilanciamento: la ponderazione dell'intensità dell'interferenza rispetto all'importanza dell'obiettivo raggiunto nel contesto dato; la proporzionalità è una valutazione in concreto, di contesto.

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[37], 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[38];
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[39].

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[40] 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.

---

[37] È importante notare che sia la misura che i suoi obiettivi dovrebbero essere già stati identificati nelle fasi del test di necessità; in questa fase, è necessario riconsiderare questi obiettivi al fine di accertare, sempre ex ante ma ora in concreto, la loro importanza e in che misura sono effettivamente soddisfatti. A tal riguardo, si ricorda che, secondo la valutazione d'impatto della Commissione, gli obiettivi devono essere SMART: specifici (ossia, abbastanza precisi e concreti); misurabili; raggiungibili; realistici; dipendenti dal tempo (ossia, legati a una data fissa o a un periodo di tempo entro il quale i risultati dovrebbero essere raggiunti).

[38] È importante notare che i diritti e le libertà fondamentali limitati dalla misura sono già stati identificati nelle fasi del test di necessità; in questa fase, è necessario riconsiderare questi diritti e libertà fondamentali al fine di accertare, sempre ex ante ma in concreto, come verrebbero colpiti.

[39] Se l'esercizio di bilanciamento in questione porta alla conclusione che una misura proposta non soddisfa il requisito della proporzionalità, allora la misura non dovrebbe essere proposta o dovrebbe essere modificata in modo da soddisfare questi requisiti.

[40] Considerando n. 75) del GDPR: "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di violazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, inparticolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati". Dunque, come ricordato dal WP 29 all'interno delle proprie Linee Guida n. 248/2017 il riferimento ai "diritti e le libertà" degli interessati va inteso, in primo luogo, come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

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[41]); il più alto di questi livelli deve essere considerato come il risultato finale.

Dunque, il livello di impatto[42] 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.

---

[41]Cfr.ISO/IEC 29134:2023: "La definizione dei criteri di rischio deve basarsi su quanto segue: danni agli utenti del prodotto, del servizio o del sistema. Il danno può includere danni fisici, finanziari, di reputazione, imbarazzo e invasione della vita domestica. Inoltre, nel considerare l'impatto su un individuo dei rischi per la privacy delle sue PII, l'organizzazione deve prendere in considerazione diversi tipi di privacy, come la privacy corporea, la privacy della posizione e dello spazio, la privacy comportamentale, la privacy delle comunicazioni, la privacy dei dati e delle immagini, la privacy dei pensieri e dei sentimenti e la privacy delle associazioni". Cfr. Considerando n. 75) del GDPR ("I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati"), da leggersi, assieme, al successivo Considerando n. 85) del GDPR.

[42]Cfr. ISO/IEC 29134:2023, Allegato A): "Il livello di impatto delle conseguenze identificate deve essere stimato, tenendo conto di tali conseguenze e dei controlli pianificati o implementati. In altre parole, a quanto ammonterebbe il danno causato da tutti i potenziali impatti? 1) Trascurabile: I committenti delle PII non subiranno alcun effetto o subiranno alcuni inconvenienti che supereranno senza difficoltà (tempo speso per reinserire le

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[43] 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[44]; 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.

---

informazioni, fastidi, irritazioni, ecc.); 2) Limitato: I committenti di PII possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione dell'accesso ai servizi aziendali, paura, mancanza di comprensione, stress, piccoli disturbi fisici, ecc.); 3) Significativo: I committenti di PII possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera delle banche, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento dello stato di salute, ecc.); 4) Massimo: I committenti di PII possono andare incontro a conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debiti inservibili o incapacità di lavorare, disturbi psicologici o fisici di lunga durata, morte, ecc.). Tabella A. 1.): Livello di impatto n. 1): PII accessibili al pubblico (ad esempio, elenchi telefonici, rubriche o selezione di dati); Livello di impatto n. 2): PII che richiedono un interesse legittimo per l'accesso (ad esempio, file pubblici riservati o membri di una lista di distribuzione); Livello di impatto n. 3): PII la cui divulgazione non autorizzata può pregiudicare la reputazione del titolare della PII (ad esempio, informazioni sul reddito, sulle prestazioni sociali, sulle imposte sulla proprietà o sulle sanzioni); Livello di impatto n. 4): PII la cui divulgazione, modifica, perdita o distruzione non autorizzata può pregiudicare l'esistenza o la salute, la libertà e la vita del titolare della PII (ad esempio, informazioni sull'impegno in un istituto, su una sentenza, su revisioni del personale, su dati sanitari, su debiti non saldati, o se il titolare della PII rischia di diventare una vittima di un caso penale.

[43] Cfr. ISO/IEC 29134:2023, Tabella B.1., intitolata "Minacce generiche".

[44] Cfr. ISO/IEC 29134:2023, tabella A.3): "La probabilità che ogni minaccia venga sfruttata deve essere stimata, tenendo conto delle vulnerabilità degli asset di supporto e delle capacità delle fonti di rischio di sfruttarle (competenze, tempo disponibile, risorse finanziarie, vicinanza al sistema informativo, motivazione, senso di impunità, ecc.). In altre parole, in che misura le proprietà degli asset di supporto possono essere sfruttate per portare a termine una minaccia? 1) Trascurabile: La realizzazione di una minaccia sfruttando le proprietà degli asset di supporto non sembra possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in una stanza protetta da un lettore di badge e da un codice di accesso); 2) Limitato: La realizzazione di una minaccia sfruttando le proprietà degli asset di supporto sembra essere difficile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in una stanza protetta da un lettore badge); 3) Significativo: L'attuazione di una minaccia sfruttando le proprietà degli asset di supporto sembra essere possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in uffici a cui non si può accedere senza aver prima effettuato il check-in alla reception); 4) Massimo: Realizzare una minaccia sfruttando le proprietà degli asset di supporto sembra essere estremamente facile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in un atrio)".

- 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 operaPALERMO 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")[45].

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"

[45] Se tutte le risposte sono "positive", l'ente dovrebbe considerare la probabilità della minaccia alta, mentre se sono tutte "negative" la probabilità della minaccia dovrebbe essere considerata bassa; invece, per i casi con due o tre risposte positive, l'ente dovrebbe assegnare la probabilità di minaccia come media.

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[46] è da considerarsi **BASSO**.

Passaggio 5: valutazione del rischio[47].
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.

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 24-06-2025 (data di ultimo aggiornamento).

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

[46]Cfr. ISO/IEC 29134:2023, paragrafo 6.4.4.2): "Per stimare la probabilità delle minacce [...], l'organizzazione deve considerare le capacità delle fonti di rischio, le vulnerabilità degli asset di supporto e i controlli esistenti o previsti. Si può utilizzare l'Allegato A.".
[47] L'ente deve valutare, in modo libero e discrezionale (ma comunque fondato su un'adeguata giustificazione), il livello di rischio ottenuto, tenute conto le caratteristiche specifiche dell'operazione di trattamento di specie.Cfr. ISO/IEC 29134:2023, paragrafo 6.4.5.1): "Le opzioni disponibili per il trattamento del rischio privacy sono quattro: riduzione del rischio, ritenzione del rischio, evitamento del rischio e trasferimento del rischio".