Modello Organizzativo Privacy

Approvato dal Consiglio di Amministrazione di ERG S.p.A. il 15 Ottobre 2024

Indice

1. DEFINIZIONI

In aggiunta alle definizioni contenute in altre parti del presente "Modello Organizzativo Privacy" (di seguito il "Modello Organizzativo" o il "Modello" o il "MOP"), i termini e le espressioni con lettera iniziale maiuscola ivi utilizzati hanno il significato ad essi qui di seguito attribuito, essendo peraltro precisato che il medesimo significato vale sia al singolare che al plurale:

- **Amministratore di Sistema**: persona fisica cui è demandata, in nome e/o per conto di Società del Gruppo, la gestione e/o la manutenzione di un sistema informatico e di elaborazione dati o di sue componenti sia hardware che software;
- **Autorità di Controllo**: autorità pubblica incaricata di sorvegliare l'applicazione della normativa sulla protezione dei Dati Personali ed in particolare del GDPR al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al Trattamento (ad esempio, per Italia, deve intendersi il Garante per la protezione dei Dati Personali);
- **Autorizzato o Autorizzato al Trattamento**: persona fisica autorizzata a compiere materialmente le operazioni di Trattamento per conto del Titolare. Con riferimento alle Società del Gruppo, è Autorizzato tutto il Personale che, in virtù delle mansioni svolte sulla base del Manuale Organizzativo, si trovi a trattare Dati Personali nonché i membri degli organi di amministrazione (diversi dai Delegati Privacy) e di controllo di tutte le Società del Gruppo, ivi inclusi i componenti dei relativi Organismi di Vigilanza, limitatamente alle rispettive aree di competenza;
- **CISO o Chief Information Security Officer**: Personale responsabile della strategia di sicurezza informatica e della sua implementazione per garantire la sicurezza e protezione dei sistemi del Gruppo ERG;
- **DPIA o Data Protection Impact Assessment**: attività di valutazione delle conseguenze che il Trattamento potrebbe arrecare ai diritti e alle libertà degli Interessati ad esito della quale vengono definite le Misure di Sicurezza proporzionate al rischio del Trattamento al fine di mitigarlo in misura adeguata;
- **Dato Comune**: qualsiasi Dato Personale diverso dai Dati Giudiziari e dai Dati Particolari;
- **Dato Giudiziario**: qualsiasi Dato Personale relativo a condanne penali, a reati od a connesse misure di sicurezza;
- **Dato Particolare**: qualsiasi Dato Personale idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché relativo a dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **Dato o Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento (i) un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, (ii) un identificativo online o (iii) uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di cui una Società del Gruppo sia Titolare, Responsabile o Sub-responsabile;
- **Delegato Privacy**: la persona fisica alla quale il Titolare del Trattamento ha conferito tutti i poteri e le competenze sulle decisioni in ordine alle finalità e alle modalità del Trattamento, ivi compreso il profilo della sicurezza;
- **Disposizioni o Disposizioni Privacy**: leggi e regolamenti pro tempore vigenti in tutti i Paesi in cui le Società del Gruppo svolgono (in tutto o in parte) le loro attività, aventi ad oggetto la protezione dei Dati Personali;
- **ERG**: ERG S.p.A.;
- **ERG Power Generation**: ERG Power Generation S.p.A.;
- **GDPR**: il Regolamento (UE) 2016/679 sulla protezione dei Dati Personali;
- **Gruppo ERG o Gruppo o Società del Gruppo**: ERG e le Società Controllate;
- **Interessato o Soggetto Interessato**: la persona fisica identificata o identificabile cui si riferiscono i Dati Personali (tra i quali dipendenti, candidati all'assunzione, fornitori, business partner, componenti degli organi di amministrazione e controllo delle Società del Gruppo,

partecipanti ad eventi, visitatori);

- **ISMS Committee**: responsabile del coordinamento tra le varie unità organizzative del Gruppo coinvolte nella gestione degli incidenti di sicurezza informatica, relativi anche ai Dati Personali;
- **Manuale Organizzativo**: il documento che, dato l'assetto in vigore in un determinato momento nel Gruppo ERG, definisce, per ogni ruolo organizzativo presente nell'organigramma:
  - la finalità, intesa come obiettivo principale;
  - le responsabilità, in relazione alle macro - attività in cui sono distinti i principali processi;
  - il profilo atteso di competenze tecniche;
- **Misure di Sicurezza**: misure tecniche e organizzative volte a garantire la protezione dei Dati Personali;
- **Norme Interne**: tutte le norme aziendali di volta in volta adottate nel Gruppo ERG;
- **Personale o Personale del Gruppo ERG**: tutti i soggetti che hanno un contratto di lavoro con una delle Società del Gruppo ERG (compreso il personale in stage, apprendistato e somministrazione);
- **Privacy by Default**: principio in base al quale in ciascun Trattamento devono essere adottate, come impostazione predefinita, le Misure di Sicurezza adeguate a garantire che siano trattati solo i Dati Personali necessari per ogni specifica finalità di Trattamento;
- **Privacy by Design**: principio in base al quale la definizione delle Misure di Sicurezza deve avvenire fin dalla progettazione di ogni processo aziendale, con particolare riferimento alle relative applicazioni informatiche di supporto;
- **Privacy Focal Point**: Personale individuato dal Referente del Trattamento, con il supporto dell'unità organizzativa Organization di ERG, sentito il responsabile dell'unità organizzativa interessata dalla predetta nomina, al fine di facilitare – con riferimento ad una o più Società del Gruppo - la gestione di alcune delle tematiche e degli adempimenti inerenti il Trattamento all'interno della relativa unità organizzativa di appartenenza e supportare il Referente del Trattamento;
- **Profilazione**: qualsiasi forma di Trattamento automatizzato consistente nell'utilizzo di Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **Referente o Referente del Trattamento**: Personale individuato dal Delegato Privacy ed appartenente all'unità organizzativa Compliance 231 & Privacy con il compito di gestire – con riferimento ad una o più Società del Gruppo - alcune delle tematiche e degli adempimenti inerenti il Trattamento dei Dati Personali e supportare il Delegato Privacy;
- **Registro o Registro dei Trattamenti**: registro delle attività di Trattamento svolte dal Titolare o da Responsabili del Trattamento per conto del Titolare;
- **Responsabile o Responsabile del Trattamento**: la persona fisica o giuridica (ivi incluse le Società del Gruppo), l'autorità pubblica, l'agenzia o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento (ad esempio fornitori);
- **Società Controllate**: le società controllate da ERG ai sensi dell'art. 93 del Testo Unico della Finanza;
- **Sub-Responsabile**: la persona fisica o giuridica (ivi incluse le Società del Gruppo), l'autorità pubblica, l'agenzia o altro organismo che tratta Dati Personali per conto del Responsabile del Trattamento;
- **Terze Parti**: le persone giuridiche (ivi incluse le Società del Gruppo) o fisiche (diverse dagli Autorizzati al Trattamento) alle quali le Società del Gruppo, in qualità di Titolari, possono mettere a disposizione alcuni Dati Personali e che, in alcuni casi, agiscono quali Responsabili del Trattamento;
- **Titolare o Titolare del Trattamento**: la persona fisica o giuridica (ivi incluse le Società del Gruppo), l'autorità pubblica, l'agenzia o altro organismo che, singolarmente o insieme ad altri, determina le finalità e le modalità del Trattamento nonché gli strumenti utilizzati;

- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute, con o senza l'ausilio di processi automatizzati, e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Violazione di Dati Personali o Data Breach**: ogni evento che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati dal Titolare del Trattamento.

2. OBIETTIVO E AMBITO DI APPLICAZIONE

Attraverso il MOP vengono individuate le Norme Interne e definite le Misure di Sicurezza adottate per garantire la conformità alle Disposizioni Privacy vigenti in tutti i Paesi in cui le Società del Gruppo ERG svolgono (in tutto o in parte) le loro attività.
L'attuazione del Modello Organizzativo è obbligatoria per ERG e per tutte le Società del Gruppo. Il MOP è stato approvato dal Consiglio di Amministrazione di ERG e, progressivamente, dai competenti organi sociali di ciascuna Società del Gruppo.

Tutto il Personale del Gruppo ERG è responsabile dell'applicazione del Modello, con particolare riferimento agli Autorizzati al Trattamento, i quali devono contribuire fattivamente alla protezione dei Dati Personali oggetto di Trattamento nonché al rispetto delle Disposizioni Privacy.
L'osservanza delle disposizioni del MOP deve considerarsi parte essenziale delle obbligazioni contrattuali del Personale del Gruppo ERG.
Le Terze Parti che hanno rapporti con Società del Gruppo devono conoscere il MOP e rispettarlo per tutti gli aspetti che riguardano anche la loro attività svolta nell'interesse o per conto delle Società del Gruppo.

3. RIFERIMENTI

Riferimenti esterni

- Regolamento (UE) 2016/679;
- Codice in materia di protezione dei Dati Personali, Decreto legislativo 30 giugno 2003, n. 196 (anche, di seguito, "Codice Privacy"), come modificato dal D. Lgs. 101 del 2018;
- Provvedimenti emanati dal Garante per la protezione dei Dati Personali, tra cui in particolare: Provvedimento del Garante Privacy - 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema;
- UK Data Protection Act 2018;
- Normativa e provvedimenti in materia di protezione dei Dati Personali emanati dalle Autorità di Controllo dei Paesi in cui opera il Gruppo ERG (es. Spagna, Francia, Germania, UK) in materia di protezione dei Dati Personali;
- ISO/IEC 27001/2022: Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistema di gestione della sicurezza delle informazioni.

Riferimenti interni

- Codice Etico;
- Procedura "Gestione data breach";
- Procedura "Gestione visite ispettive";
- Linea Guida "Crisis Communication Management";
- Linea Guida "Whistleblowing";
- PR-ISMS-11.1_Procedura "Gestione incidenti informatici";

- PR-ISMS_11.0.3_ Procedura "Regolamento sulla Sicurezza delle informazioni aziendali";
- POL-ISMS_ 4.0.1_Politica "Sicurezza delle informazioni";
- PR- ISMS-11.0.6_ Procedura "Classificazione delle informazioni";
- PR- ISMS-7.2_Procedura “Gestione degli strumenti informatici”;
- Modelli di organizzazione e gestione ex D.Lgs. n. 231/01, adottati dalle società italiane del Gruppo ERG, ove applicabili.

4. PRINCIPI PRIVACY

Nello svolgimento di ogni attività di Trattamento, il Gruppo ERG opera in conformità ai seguenti principi:

- liceità, correttezza e trasparenza del Trattamento nei confronti dell’Interessato;
- limitazione della finalità del Trattamento, compreso l’obbligo di assicurare che eventuali Trattamenti successivi non siano incompatibili con le finalità della raccolta dei Dati Personali;
- minimizzazione dei Dati, nel senso che i Dati Personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del Trattamento;
- esattezza e aggiornamento dei Dati, compresa la tempestiva cancellazione o rettifica dei Dati Personali che risultino inesatti rispetto alle finalità del Trattamento;
- limitazione della conservazione, ovvero necessità di provvedere alla conservazione dei Dati Personali per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il Trattamento;
- integrità e riservatezza, garantendo che la sicurezza dei Dati Personali oggetto del Trattamento sia adeguata;
- accountability (responsabilizzazione), inteso come l’impegno a mettere in atto Misure di Sicurezza adeguate a garantire che il Trattamento è effettuato conformemente alle Disposizioni Normative, fornendo adeguata dimostrazione dell’adempimento di tale impegno.

5. MODELLO ORGANIZZATIVO: RUOLI E RESPONSABILITÀ

Il Gruppo ERG ha definito una struttura organizzativa interna (di seguito “Organizzazione Privacy”) dedicata alla protezione dei Dati Personali, composta dalle seguenti figure:

- Titolari del Trattamento;
- Delegati Privacy;
- Responsabili e Sub Responsabili del Trattamento;
- Referenti del Trattamento;
- Autorizzati al Trattamento;
- Privacy Focal Point;
- Head of Compliance 231 & Privacy;
- Chief Information Security Officer (CISO);
- Head of ICT Governance, Integration & Security;
- Amministratori di Sistema;
- Chief Audit Officer.

Nell’ipotesi in cui le Disposizioni Privacy dovessero richiedere la nomina di un Data Protection Officer (di seguito “DPO”), il relativo Delegato Privacy procede alla nomina dello stesso. Il DPO sarà chiamato a svolgere, tenuto conto dell’Organizzazione Privacy, le attività espressamente menzionate dalle predette Disposizioni.
Nell’allegato 1 al presente documento è riportato il grafico con l’Organizzazione Privacy.

5.1. Titolari del Trattamento e Delegati Privacy

Ciascun Titolare del Trattamento, in quanto responsabile di determinare le finalità e le modalità del Trattamento, nonché gli strumenti utilizzati, ha, in particolare, il compito di definire:

- la tipologia dei Dati Personali da trattare;
- le modalità e i sistemi utilizzati per il Trattamento;

- le finalità del Trattamento;
- la necessità di trasferire o meno i Dati Personali a Terze Parti;
- le modalità e il periodo di conservazione dei Dati Personali;
- le Misure di Sicurezza da adottare per la protezione dei Dati Personali.

In considerazione di quanto sopra, ogni Società del Gruppo agisce in qualità di Titolare relativamente ai Trattamenti, effettuati nel proprio interesse (i) direttamente e/o (ii) da Terze Parti (ivi incluse Società del Gruppo) per proprio conto.

Ciascun Titolare designa il Delegato Privacy, ovvero la persona fisica al quale il Titolare conferisce tutti i poteri e le competenze sulle decisioni in ordine alle finalità e alle modalità di ciascun Trattamento.

Il Delegato Privacy (i) in caso di organo di amministrazione collegiale, viene nominato attraverso una specifica delibera dell'organo di amministrazione medesimo o (ii) in caso di organo di amministrazione monocratico, coincide con l'amministratore unico.

5.2. Responsabile del Trattamento e Sub-Responsabile del Trattamento

Ogni Società del Gruppo, in qualità di Titolare, nomina come Responsabili tutte le Terze Parti (ivi incluse Società del Gruppo, fornitori o partner commerciali) che effettuano il Trattamento per conto e nell'interesse della stessa.
Il Titolare, a seconda dei casi, può autorizzare il Responsabile a nominare come Sub-Responsabile una o più Terze Parti (ivi incluse Società del Gruppo). Il Sub-Responsabile così designato è tenuto a rispettare gli stessi obblighi stabiliti nel contratto stipulato tra il Titolare e il Responsabile, che rimane pienamente responsabile per il rispetto degli obblighi relativi al Trattamento da parte del Sub-Responsabile.
Il Titolare deve avvalersi unicamente di Responsabili che presentino garanzie sufficienti per mettere in atto Misure di Sicurezza adeguate in modo tale che il Trattamento sia in linea con le Disposizioni Privacy e garantisca la tutela dei diritti dell'Interessato.

La nomina del Responsabile e le modalità del Trattamento da parte dello stesso sono disciplinate nell'ambito di un contratto attraverso il quale vengono definite, in particolare:

- l'oggetto e la durata del Trattamento;
- la natura e la finalità del Trattamento;
- la tipologia di Dati Personali trattati e le categorie di Soggetti Interessati coinvolti;
- le istruzioni/restrizioni per qualsiasi trasferimento di Dati Personali;
- l'applicazione delle Misure di Sicurezza adeguate;
- gli obblighi e i diritti del Titolare e del Responsabile.

Il Responsabile ha, in particolare, il compito di:

- assicurarsi che il Trattamento avvenga secondo le istruzioni impartite dal Titolare;
- adottare tutte le misure tecniche e organizzative idonee a garantire la sicurezza del Trattamento;
- richiedere l'autorizzazione scritta del Titolare al fine di nominare e potersi avvalere di un Sub-Responsabile;
- procedere all'identificazione, nell'ambito della propria struttura, degli Autorizzati al Trattamento, fornendo agli stessi adeguate istruzioni in relazione al Trattamento effettuato/da effettuare e garantendo che gli stessi abbiano un adeguato obbligo legale di riservatezza;
- monitorare le operazioni di Trattamento svolte dai propri Autorizzati e verificare che vengano eseguite in conformità alle istruzioni agli stessi impartite e solo relativamente agli ambiti di Trattamento loro consentiti;
- informare tempestivamente il Titolare in merito alle richieste degli Interessati che dovessero pervenire al Responsabile e collaborare con il Titolare al fine di garantire l'effettivo esercizio da parte degli stessi di tutti i diritti previsti dalle Disposizioni Privacy;
- informare tempestivamente il Titolare del Trattamento di ogni violazione, anche potenziale, dei Dati Personali trattati;

- consentire al Titolare di effettuare delle attività di ispezione in merito alle modalità di esecuzione del Trattamento.

In caso di dubbi sulla possibile qualificazione di una Terza Parte come Responsabile deve essere contattata l'unità organizzativa Compliance 231 & Privacy per ottenere indicazioni in merito.

Il modello organizzativo del Gruppo prevede la centralizzazione delle attività comuni alle Società del Gruppo ERG. In particolare, ERG garantisce l'indirizzo strategico ed ha la responsabilità diretta del business development e della gestione di tutti i processi di supporto al business per tutte le società del Gruppo attraverso un contratto infragruppo con ERG Power Generation che, a sua volta, ha analoghi contratti infragruppo con le altre Società del Gruppo (di seguito i "Contratti Infragruppo").

Nell'ambito dei Contratti Infragruppo,

- ERG, relativamente ai Trattamenti effettuati nell'interesse e per conto di ERG Power Generation, agisce in qualità di Responsabile;
- ERG Power Generation, relativamente ai Trattamenti effettuati nell'interesse e per conto di altre Società del Gruppo, agisce in qualità di Responsabile;
- ERG, relativamente ai Trattamenti effettuati nell'interesse di altre Società del Gruppo ma per conto di ERG Power Generation, agisce in qualità di Sub-Responsabile.

5.3. Referente del Trattamento

Ogni Delegato Privacy di Società del Gruppo con Personale può, a seconda dei casi, designare un Referente, da individuarsi tra il Personale nell'ambito dell'unità organizzativa Compliance 231 & Privacy, che per esperienza, capacità ed affidabilità sia in grado di supportare il Delegato Privacy al rispetto delle Disposizioni, ivi compreso il profilo relativo alla sicurezza.
Nell'esecuzione del proprio incarico il Referente dovrà attenersi alle istruzioni ricevute dal Delegato Privacy.

Il Referente ha, in particolare, il compito di:

- mettere a disposizione del Delegato Privacy tutte le informazioni necessarie per dimostrare il rispetto degli obblighi relativi alle Disposizioni;
- fornire consulenza al Delegato Privacy e agli Autorizzati su tematiche relative ai Trattamenti;
- fornire, se richiesto, pareri in merito alla tenuta del Registro dei Trattamenti e allo svolgimento della DPIA;
- informare tempestivamente il Delegato Privacy di eventuali violazioni relative al Trattamento;
- sottoscrivere e formalizzare le nomine a Responsabile del Trattamento;
- sottoscrivere e formalizzare, con il supporto dell'unità organizzativa Organization di ERG, le nomine a Privacy Focal Point, sentito il responsabile dell'unità organizzativa interessata dalla predetta nomina;
- sottoscrivere e formalizzare, su indicazione dell'unità organizzativa Information & Communication Technology, le nomine ad Amministratore di Sistema;
- supportare il Delegato Privacy nell'eventuale interazione con l'Autorità di Controllo, ovvero qualsiasi altra Autorità Pubblica, in caso di richiesta di informazioni o effettuazione di controlli ed accessi sui Dati Personali trattati dal Titolare;
- provvedere alla formazione periodica del Personale del Gruppo ERG in materia di Trattamento dei Dati Personali;
- mantenersi costantemente aggiornato sulle modifiche apportate alle Disposizioni Privacy e valutare le relative modalità di adeguamento.

5.4. Autorizzati al Trattamento

Il Personale che, in virtù delle mansioni svolte sulla base del Manuale Organizzativo, si trovi a trattare Dati Personali, nonché i membri degli organi di amministrazione (diversi dai Delegati Privacy) e di controllo di tutte le Società del Gruppo, ivi inclusi i componenti dei relativi Organismi di Vigilanza, sono Autorizzati al Trattamento.

Ciascun Autorizzato deve limitarsi a trattare i Dati Personali in funzione di quanto strettamente necessario all'esercizio delle proprie mansioni o incarichi ed ha in particolare il compito di:

- trattare i Dati Personali in modo lecito e secondo correttezza;
- verificare che i Dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- informare prontamente il Referente qualora si verifichi la necessità di porre in essere operazioni di Trattamento per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute;
- mantenere i Dati Personali in modo accurato e aggiornato, dalla raccolta alla distruzione, impedendone l'accesso da parte di terzi non autorizzati;
- assicurare la tracciabilità e rintracciabilità dei Dati Personali (accessi, modifiche, archiviazione) durante tutto il loro ciclo di vita;
- conservare i Dati solo per la durata necessaria allo scopo indicato e/o per il tempo previsto rispettando le Misure di Sicurezza predisposte dal CISO, sentito il Delegato Privacy;
- comunicare o trasferire i Dati Personali esclusivamente ad altri Autorizzati e/o a Terze Parti legittimate a riceverli, per le finalità per le quali i Dati sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- informare prontamente l'unità organizzativa Compliance 231 & Privacy in merito alle richieste degli interessati che dovessero pervenire e collaborare con la stessa al fine di garantire l'effettivo esercizio da parte degli Interessati di tutti i diritti previsti dalle Disposizioni.

In caso di **violazione dei Dati** (ovvero la distruzione intenzionale o non, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai Dati trasmessi, conservati o comunque trattati), l'Autorizzato sarà tenuto a comunicare tempestivamente tale violazione al Referente, all'Head of Compliance 231 & Privacy e all'Head of ICT Governance, Integration & Security, che provvederà a convocare l'ISMS Committee. Il Delegato Privacy dovrà successivamente notificare l'evento all'Autorità di Controllo senza ingiustificato ritardo, e ove possibile, **entro 72 ore** dal momento in cui viene rilevato l'evento di violazione dei Dati Personali.
In caso di dubbi o questioni inerenti all'applicazione del MOP, ciascun Autorizzato deve contattare l'unità organizzativa Compliance 231 & Privacy per ottenere indicazioni in merito.

5.5. Privacy Focal Point

Ogni Referente di Società del Gruppo con Personale, con il supporto dell'unità organizzativa Organization di ERG, sentito il responsabile dell'unità organizzativa interessata, può designare uno o più Privacy Focal Point, da individuarsi tra il Personale nell'ambito delle unità organizzative del Gruppo, che per esperienza, capacità e affidabilità siano in grado di fornire supporto all'unità organizzativa Compliance 231 & Privacy e/o al Referente per il corretto Trattamento dei Dati.
Il Privacy Focal Point, relativamente all'unità organizzativa di appartenenza, ha, in particolare, il compito di:

- collaborare con il Referente e l'unità organizzativa Compliance 231 & Privacy nell'esecuzione degli adempimenti previsti dalle Disposizioni Privacy;
- coinvolgere il Referente e/o l'unità organizzativa Compliance 231 & Privacy a fronte di eventuali nuovi Trattamenti da effettuare o di modifiche ai Trattamenti esistenti;
- fornire all'unità organizzativa Compliance 231 & Privacy le informazioni necessarie all'aggiornamento del Registro dei Trattamenti e, ove necessario, all'effettuazione della DPIA;
- collaborare e contribuire alle attività di controllo (es. audit interno o verifiche ispettive dell'Autorità di Controllo) mettendo a disposizione tutte le informazioni richieste;
- partecipare alle sessioni formative e di aggiornamento (es. training su temi specifici, tavoli di lavoro);
- segnalare eventuali criticità inerenti i Trattamenti.

In caso di dubbi o questioni inerenti all'applicazione del MOP, ciascun Privacy Focal Point deve contattare l'unità organizzativa Compliance 231 & Privacy per ottenere indicazioni in merito.

5.6. Compliance 231 & Privacy

L'unità organizzativa Compliance 231 & Privacy ha, in particolare, i seguenti compiti:

- supportare operativamente i Referenti nell'esecuzione delle relative mansioni;
- proporre l'adozione e/o l'aggiornamento di procedure rilevanti in materia di protezione dei Dati;
- coordinare le attività per l'aggiornamento del Registro dei Trattamenti e per l'effettuazione della DPIA;
- predisporre le Informative Privacy e i Consensi al Trattamento;
- gestire le risposte alle richieste da parte degli Interessati;
- supportare le unità organizzative e in particolare i Privacy Focal Point in caso di dubbi su tematiche relative alla protezione dei Dati e nello sviluppo di nuovi progetti;
- cooperare nella gestione di Data Breach;
- cooperare con il CISO e con l'unità organizzativa ICT Governance, Integration & Security, in merito alle tematiche di loro competenza (i.e. sicurezza informatica e definizione di Misure di Sicurezza);
- migliorare l'efficienza dei processi per la protezione dei Dati.

5.7. Chief Information Security Officer (CISO)

Il CISO è responsabile della gestione degli aspetti di natura tecnica e di sicurezza informatica nell'ambito del Trattamento dei Dati e opera mediante l'unità organizzativa ICT Governance, Integration & Security.

Il CISO ha, in particolare, il compito di:

- gestire la strategia di sicurezza informatica del Gruppo ERG e la sua implementazione per garantire che i sistemi, i servizi e le informazioni aziendali, inclusi i Dati Personali, siano adeguatamente sicuri e protetti;
- definire, mantenere e comunicare la visione, la strategia, le politiche e le procedure della sicurezza informatica;
- gestire l'implementazione della politica di sicurezza informatica in tutto il Gruppo.

5.8. ICT Governance, Integration & security

L'unità organizzativa ICT Governance, Integration & Security assicura lo sviluppo ed il regolare allineamento della governance & security ICT rispetto alle esigenze del Gruppo ERG, garantendo adeguate metodologie e strumenti di integrazione e data management ed implementando la strategia di sicurezza informatica affinché i sistemi, i servizi e i Dati Personali siano adeguatamente sicuri e protetti, coerentemente con i principi di Privacy by Design e Privacy by Default.

L'unità organizzativa ICT Governance, Integration & Security ha, in particolare, il compito di:

- individuare idonee e preventive Misure di Sicurezza volte a garantire un livello di sicurezza adeguato al rischio del Trattamento, al fine di assicurare la riservatezza, l'integrità, la disponibilità dei sistemi e delle attività di Trattamento;
- aggiornare periodicamente il Referente e l'unità organizzativa Compliance 231 & Privacy su nuovi progetti che comportino l'adozione di sistemi per il Trattamento di Dati Personali e, in generale, sullo stato di implementazione delle Misure di Sicurezza previste a protezione dei Dati Personali in conformità a quanto definito;
- fornire supporto tecnico a qualsiasi unità organizzativa che effettui il trattamento di Dati Personali, attraverso l'utilizzo dei sistemi informativi aziendali;
- identificare gli Amministratori di Sistema interni, garantendo un'adeguata attività di vigilanza sull'attività operativa svolta (raccolta e il monitoraggio dei log, attività di verifica periodica sull'attività svolta, conservazione gli estremi identificativi degli amministratori di sistema);

- verificare che lo smaltimento dei rifiuti elettrici ed elettronici contenenti Dati Personali avvenga secondo quanto previsto dalla normativa di riferimento o se tale attività è affidata a un fornitore esterno, verificare che vengano adottate adeguate Misure di Sicurezza;
- definire tecnicamente Misure di Sicurezza logiche per l'accesso alle basi dati elettroniche e adeguate Misure di Sicurezza fisiche per l'accesso ai locali adibiti a data center;
- convocare l'ISMS Commitee responsabile del coordinamento delle varie unità organizzative coinvolte nella gestione degli incidenti di sicurezza informatica relativi anche ai Dati Personali, in conformità alle Disposizioni Privacy e alle Norme Interne;
- implementare, nel rispetto della Procedura "Gestione dei Data Breach", specifici flussi di notifica in caso di eventi di violazione dei Dati Personali rilevati o in caso di anomalie che possano far presumere possibili compromissioni di tali dati collaborando con il Referente per i prescritti adempimenti relativi alla notifica all'Autorità di Controllo e all'Interessato laddove necessario;
- comunicare tempestivamente l'avvenuto ripristino della disponibilità e dell'accesso ai Dati Personali in caso di incidente fisico o tecnico.

5.9. Internal Audit

Nell'ambito del Piano di Audit, l'unità organizzativa Internal Audit può effettuare delle verifiche sul livello di conformità del Gruppo ERG alle regole definite nel presente documento, anche col supporto di altre unità organizzative quali, a titolo esemplificativo, Compliance 231 & Privacy e Information & Communication Technology.
Internal Audit informa il Referente e il Titolare circa i risultati degli audit condotti nell'ambito del Trattamento di Dati Personali.

6. MODELLO DI GESTIONE

Le operazioni di Trattamento devono essere strettamente limitate a quanto necessario a perseguire le finalità indicate nell'Informativa Privacy e, in ogni caso, compatibili con dette finalità.
Di seguito sono riportate le fasi del ciclo di vita del Dato Personale al cui interno sono dettagliate le modalità di gestione operativa:

- Raccolta;
- Trattamento;
- Cessazione del Trattamento e Cancellazione.

6.1. Raccolta

6.1.1 Finalità

Il Trattamento dei Dati Personali da parte delle Società del Gruppo ERG deve avvenire per il perseguimento di finalità legittime preventivamente individuate.
I Dati Personali (raccolti o ricevuti) devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro Trattamento.
Si riportano qui di seguito, a mero titolo esemplificativo, talune finalità:

- selezione e assunzione del Personale e gestione del rapporto di lavoro con il medesimo;
- gestione dei rapporti con clienti, fornitori e business partner;
- gestione dei rapporti con i componenti degli organi di amministrazione e di controllo delle Società del Gruppo;
- gestione degli accessi alle sedi delle Società del Gruppo;
- tutela della sicurezza di persone o beni attraverso strumenti di videosorveglianza;
- analisi su preferenze/scelte ed elaborazioni statistiche;
- gestione delle registrazioni degli utenti ai siti web/piattaforme del Gruppo ERG;
- attività di Profilazione.

6.1.2 Base giuridica

Ciascun Trattamento richiede l'identificazione della base giuridica che lo legittima.

Per quanto riguarda i Dati Personali trattati nell'ambito del Gruppo ERG, le basi giuridiche del Trattamento sono:

a. **il consenso**: quando il Trattamento viene esplicitamente autorizzato dall'Interessato per una o più specifiche finalità (es. Trattamento di Dati Particolari o Dati Giudiziari) (il "Consenso al Trattamento").
   Affinché il trattamento fondato su tale base giuridica sia considerato lecito, occorre che il Consenso al Trattamento sia espresso mediante un atto positivo con il quale l'Interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il Trattamento dei Dati Personali che lo riguardano, ovvero una dichiarazione scritta (anche attraverso mezzi elettronici, ad es. la selezione di un'apposita casella in un sito web).
   Gli Interessati hanno la possibilità di revocare, in qualsiasi momento, il Consenso al Trattamento precedentemente prestato allo svolgimento di determinate operazioni di Trattamento. In tali ipotesi, le operazioni di Trattamento svolte in virtù di tale consenso dovranno essere prontamente interrotte salvo che sussista altro fondamento giuridico per il Trattamento.

b. **l'esecuzione di un contratto o di previsioni precontrattuali**: quando il Trattamento è connesso all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (ad esempio, per assumere un candidato occorrerà raccogliere i suoi dati personali come nome, cognome, indirizzo, etc.).
   Affinché il Trattamento fondato su tale base giuridica sia considerato lecito, occorre che:
   - vi sia un valido contratto fra la Società del Gruppo e l'Interessato;
   - il Trattamento di quei Dati forniti dall'Interessato sia oggettivamente necessario per l'esecuzione del contratto;
   - sia fornita all'Interessato l'Informativa Privacy con l'indicazione della base giuridica del Trattamento.

c. **l'adempimento ad un obbligo di legge:** quando il Trattamento è imposto da una legge, e/o regolamento (es. adempimenti amministrativi e fiscali: gestione cedolini paga).
   Affinché il Trattamento fondato su tale base giuridica sia considerato lecito, occorre che:
   - l'obbligo debba essere definito dalla legge europea o nazionale di uno Stato;
   - tali disposizioni debbano stabilire un obbligo imperativo di Trattamento sufficientemente chiaro e preciso;
   - tali disposizioni debbano almeno definire le finalità del Trattamento in questione;
   - tale obbligo debba essere imposto al Titolare del Trattamento e non agli Interessati dal Trattamento.

d. **l'interesse legittimo del Titolare:** quando il Trattamento è necessario per esigenze specifiche del Titolare a condizione però che il Trattamento non sia eccessivamente invasivo per l'Interessato (es. installare un sistema di videosorveglianza per fini di sicurezza).
   Affinché il Trattamento fondato su tale base giuridica sia considerato lecito, occorre effettuare un bilanciamento fra gli interessi del Titolare e i diritti riconosciuti all'Interessato al fine valutare e dimostrare la prevalenza degli interessi del Titolare sui diritti dell'Interessato.
   Nel fare il bilanciamento fra gli interessi occorre valutare:
   - se il Trattamento sia realmente necessario tenendo conto del possibile pregiudizio che ne deriverebbe al Titolare qualora non effettuasse il Trattamento;
   - l'impatto sugli Interessati e la loro ragionevole aspettativa riguardo a ciò che accadrà ai loro Dati Personali;
   - la presenza di misure addizionali di protezione dei Dati che possano limitare gli impatti del Trattamento sugli Interessati.

6.1.3 Informativa privacy

Il Titolare deve fornire all'Interessato tutte le informazioni relative al Trattamento dei Dati Personali che lo riguardano, in forma concisa, comprensibile e facilmente accessibile, con linguaggio semplice e chiaro, per iscritto o con altri mezzi, anche in formato elettronico (sito web) (l'"Informativa Privacy"). L'informativa Privacy è strutturata indicando almeno i seguenti elementi:

- gli estremi identificativi del Titolare del Trattamento e le relative modalità di contatto;
- le finalità del Trattamento;
- la base giuridica sulla quale si fonda il Trattamento;
- le categorie dei Dati Personali;
- l'obbligatorietà o meno del conferimento dei Dati Personali e le conseguenze di un eventuale rifiuto;
- la possibilità di trasferimento in Paesi situati al di fuori dell'Unione Europea, qualora applicabile;
- i destinatari o le eventuali categorie di destinatari dei Dati Personali;
- il periodo di conservazione oppure, ove non sia possibile definirlo a priori, i criteri utilizzati per determinarlo;
- i dati di contatto al fine di esercitare i propri diritti;
- l'esistenza dei diritti riconosciuti all'Interessato;
- il diritto di proporre reclamo all'Autorità di Controllo;
- l'esistenza di un eventuale processo decisionale automatizzato (privo di intervento umano), compresa la Profilazione, le logiche applicate e le conseguenze per l'Interessato;
- la fonte dalla quale sono acquisiti i Dati nel caso non siano forniti al Titolare direttamente dall'Interessato.

L'Informativa Privacy deve essere fornita all'Interessato al momento della raccolta dei Dati Personali o, se i Dati sono ottenuti da altra fonte, entro un termine ragionevole ma, al più tardi, entro un mese.

Nelle ipotesi in cui subentrino nuovi Trattamenti o nuove modalità di svolgimento di Trattamenti preesistenti, sarà responsabilità di ciascuna unità organizzativa contattare preventivamente il Referente, anche per il tramite del Focal Point Privacy, per tutti gli approfondimenti e le attività da implementare (analisi delle Disposizioni Privacy, analisi del rischio e di sicurezza, integrazione dell'Informativa Privacy).

6.2. Trattamento – Principi generali

Le operazioni di trattamento effettuate dalle Società del Gruppo ERG devono attenersi ai principi generali dettati dalle norme e riportati all'art. 4 del MOP.

6.3. Cessazione del Trattamento – Cancellazione e Distruzione

Onde assicurare che i Dati Personali non siano conservati più a lungo del necessario, occorre che sia stabilito un termine per la cessazione del Trattamento e per la cancellazione o anonimizzazione. Le Società del Gruppo devono:

- definire un periodo di conservazione dei Dati Personali in relazione alle specifiche finalità del Trattamento;
- assicurare che il periodo di conservazione dei Dati Personali sia limitato al minimo necessario;
- adottare tutte le misure ragionevoli per cancellare o anonimizzare i Dati, fermo il periodo di conservazione definito e fatti salvi gli adempimenti legati ad obblighi di legge o a finalità difensive.

7. REGOLE OPERATIVE: MACRO PROCESSI

7.1. Registro dei trattamenti

Ogni Società del Gruppo ERG con Personale, che tratta Dati quale Titolare o quale Responsabile, ove previsto dalle disposizioni del GDPR, è tenuta a compilare il Registro con riferimento alle attività di trattamento effettuate sotto la sua responsabilità.
Il Registro dei Trattamenti dovrà includere, tra le altre, le informazioni di seguito indicate:

- Titolare del Trattamento e Delegato Privacy;
- unità organizzativa: struttura organizzativa della Società del Gruppo che utilizza i Dati Personali per lo svolgimento delle sue attività lavorative;
- finalità del Trattamento: scopo della raccolta dei Dati;
- categorie di Dati Personali trattati: Dato Comune, Dato Particolare e Dato Giudiziario.
- ruolo assunto nel Trattamento: indica se il Trattamento è effettuato in qualità di Titolare, Responsabile o Sub-Responsabile;
- categoria dell'Interessato: macro-classificazione dell'Interessato (es. dipendenti, candidati all'assunzione, fornitori e business partner se persone fisiche, componenti degli organi di amministrazione e controllo delle Società del Gruppo, partecipanti ad eventi, visitatori);
- periodo di conservazione: periodo di conservazione dei dati, comunicato anche all'Interessato tramite l'Informativa Privacy;
- generale descrizione delle Misure di Sicurezza adottate;
- DPIA: eventuale esecuzione di un data protection impact assessment per il Trattamento dei Dati Personali;
- sistemi informatici utilizzati e archivi (fisici e logici);
- categorie di destinatari Terze Parti (nome dell'entità giuridica che tratta/riceve i Dati);
- eventuale trasferimento del Dato fuori dall'EU.

Il Registro dei Trattamenti è uno dei principali elementi di accountability del Titolare e costituisce parte integrante del sistema di corretta gestione dei Dati Personali e del MOP.
Il Registro, redatto in forma scritta, anche in formato elettronico deve essere tenuto a disposizione dell'Autorità di Controllo.

7.2. Privacy by design e by default

La protezione dei Dati, secondo i principi di Privacy by Design e Privacy by Default, deve:

- essere integrata all'interno del ciclo di vita dei processi/sistemi/applicativi nei quali vengono trattati Dati Personali dal momento della progettazione;
- considerare l'intero ciclo di vita dei Dati Personali, dalla raccolta alla cancellazione, tenendo in debita considerazione anche il trasferimento, la conservazione, l'elaborazione, la consultazione e la comunicazione;
- salvaguardare la confidenzialità, integrità e disponibilità dei Dati Personali trattati;
- prevedere che, per impostazione predefinita dei processi/sistemi, vengano trattati solo i Dati Personali necessari per ogni specifica finalità del Trattamento;
- prevedere che per impostazione predefinita dei processi/sistemi, i Dati Personali trattati non siano resi accessibili a un numero indefinito di persone fisiche senza una reale esigenza ed il consenso dell'Interessato (laddove applicabile).

I principi di Privacy by Design e Privacy by Default devono essere integrati nell'intera organizzazione del Gruppo ERG; pertanto, tutte le unità organizzative dovranno prestare attenzione a che lo sviluppo di progetti, processi organizzativi, sistemi informatici, prodotti e servizi venga sottoposto ad una preventiva verifica al fine di valutare fin dalla fase di progettazione l'impatto ai fini del Trattamento dei Dati Personali, individuare eventuali misure adeguate al contenimento del rischio ed aggiornare il Registro dei Trattamenti.
Ciò richiede che vi sia una estrema consapevolezza dell'importanza della protezione dei Dati all'interno del Gruppo e che ciascuna unità organizzativa fornisca il proprio contributo alla corretta e tempestiva applicazione dei principi richiamati. L'applicazione di tali principi deve inoltre essere monitorata e supervisionata dal Referente.

7.3. Data Protection Impact Assessment (DPIA)

Quando un tipo di Trattamento presenta un rischio elevato per i diritti e le libertà degli Interessati (es. l'uso di nuove tecnologie), il Titolare esegue, prima di procedere al Trattamento, una valutazione dell'impatto dello stesso sui Dati Personali in riferimento ai predetti diritti e libertà.
Tale valutazione deve essere eseguita in tutti i casi nel quali una prima analisi porti a ritenere che il Trattamento presenti dei rischi specifici in base alla tipologia dei Dati trattati, alle caratteristiche ed alle modalità del Trattamento, agli strumenti utilizzati ed alle possibili ricadute sui diritti e le libertà degli Interessati. Inoltre, una volta che la valutazione sia stata condotta, sarà comunque necessario che venga aggiornata periodicamente al fine di rivedere i risultati anche in considerazione dei cambiamenti intervenuti nel Trattamento. La valutazione prende in considerazione l'intero ciclo di vita dei Dati Personali, dalla raccolta alla cancellazione e tiene conto di eventuali elementi specifici richiesti dal particolare contesto nel quale avvengono i Trattamenti (es. Profilazione, dati dei minori, ecc.) nonché delle Disposizioni Privacy.
La valutazione d'impatto è, comunque, eseguita nei seguenti casi:

- Trattamento automatizzato, compresa la Profilazione, sulla quale si fondano decisioni automatizzate che hanno effetti giuridici o incidono in modo analogo significativamente sugli Interessati;
- Trattamento, su larga scala, di Dati Particolari che presentano un elevato rischio per i diritti e le libertà degli Interessati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
- Trattamento di Dati soggetti a valutazione d'impatto richiesti dall' Autorità di Controllo tramite elenchi resi pubblici dalla stessa Autorità.

Nel dettaglio, tale valutazione d'impatto sulla protezione dei Dati comprende:

- una descrizione chiara ed esaustiva dei Trattamenti previsti e delle finalità del Trattamento;
- una valutazione della necessità e proporzionalità dei Trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- un elenco delle garanzie, delle Misure di Sicurezza e dei meccanismi per garantire la protezione dei Dati Personali che il Titolare valuta necessario adottare al fine di dimostrare la conformità del Trattamento alle prescrizioni delle Disposizioni Privacy.

7.4. Data Breach

Qualunque evento che comporti – in modo accidentale e/o illecito – la perdita di riservatezza, di integrità e/o di disponibilità di Dati Personali trattati dal Titolare rappresenta una violazione ("Data Breach") che, in talune fattispecie, potrebbe configurare un danno materiale e/o immateriale agli Interessati.
A titolo esemplificativo e non esaustivo, gli eventi di possibile violazione dei Dati Personali possono essere costituiti da:

- perdita di Dati (siano essi in formato elettronico o cartaceo) intesa come accertata impossibilità di ripristino degli stessi. A titolo di esempio: eventi di incendio/allagamento di archivi cartacei;
- accesso non autorizzato ai Dati (sistemi informatici o archivi cartacei) inteso come violazione della confidenzialità dei Dati contenuti nei sistemi informatici o archivi. A titolo di esempio: un attacco informatico tramite lo sfruttamento di vulnerabilità dei sistemi o l'uso abusivo di credenziali di autenticazione; la consultazione di archivi cartacei il cui accesso è ristretto al solo personale autorizzato;
- perdita dell'integrità dei Dati intesa come compromissione irrimediabile della correttezza, congruenza e consistenza dei Dati. A titolo di esempio: compromissione derivante da modifica non autorizzata dei Dati, da errore umano o da incidenti di natura informatica;
- rivelazione o divulgazione di Dati a soggetti terzi non legittimati, anche non identificati, ad esempio tramite la posta elettronica o anche verbalmente.

Per tali motivi, il Gruppo ERG ha provveduto ad adottare la Procedura "Gestione Data Breach" per una corretta gestione degli incidenti di sicurezza relativi ai Dati Personali che si richiama

integralmente.

Le regole per garantire il rispetto dei principi indicati dalle Disposizioni Privacy nel caso di eventuale Data Breach possono riassumersi in:

- modalità di individuazione di un evento che può costituire una violazione;
- modalità e casistica di segnalazione al Titolare e al Delegato Privacy per il tramite del Referente;
- valutazione dell'evento accaduto;
- eventuale comunicazione agli Interessati;
- modalità di segnalazione entro 72 ore dall'evento all'Autorità di Controllo nel caso in cui gli accertamenti eseguiti rilevino un probabile rischio per i diritti e le libertà degli Interessati.

7.5. Diritti degli interessati

In conformità alle norme sul trattamento dei Dati Personali, il Gruppo ERG, quale Titolare del Trattamento, garantisce e dispone le misure atte ad assicurare l'esercizio, da parte dell'Interessato, dei seguenti diritti:

- diritto di accesso: il diritto di ottenere dal Titolare del Trattamento la conferma che sia o meno in corso il Trattamento dei Dati Personali e, in tal caso, di ottenerne informazioni in merito;
- diritto di rettifica: il diritto di ottenere la rettifica di Dati Personali inesatti e/o l'integrazione di Dati Personali incompleti;
- diritto alla cancellazione: il diritto di ottenere che i Dati Personali trattati vengano cancellati per motivi legittimi;
- diritto di limitazione di Trattamento: affinché i Dati trattati dal Titolare del Trattamento vengano contrassegnati in modo da limitarne il loro Trattamento in futuro;
- diritto alla portabilità dei Dati: il diritto di ottenere la ricezione di Dati Personali, o la trasmissione dei Dati ad altro Titolare del Trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- diritto di opposizione: il diritto di opporsi in qualunque momento al Trattamento dei Dati, salvo che vi siano motivi legittimi per procedere al Trattamento che siano prevalenti (per esempio per l'esercizio o la difesa in sede giudiziaria);
- processo decisionale automatizzato: diritto di non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione.

Prima del riscontro è indispensabile accertare l'identità dell'Interessato attraverso copia di un documento di identità in corso di validità.
Se la richiesta proviene da persona che agisce per conto dell'Interessato è necessario verificare:

- la delega firmata dall'Interessato;
- l'identità dell'Interessato e del soggetto delegato.

Se la richiesta riguarda l'accesso ai Dati di una persona deceduta, è necessario identificare il richiedente e accertarsi che si tratti di un erede, o comunque, di persona legittimata all'esercizio del diritto.

Il Gruppo ERG ha istituto un'apposita casella di posta per la ricezione delle istanze relative all'esercizio dei diritti riconosciuti all'Interessato.
La gestione delle richieste è a carico dell'unità organizzativa Compliance 231& Privacy che:

- presidia i canali dedicati al ricevimento di queste richieste (es. casellaprivacy@erg.eu);
- chiede assistenza alle unità organizzative coinvolte nel Trattamento dei Dati degli Interessati (es. HR, ICT, IR & Communication);
- fornisce riscontro alla richiesta.

La risposta all'Interessato deve essere fornita senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.
Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del

numero delle richieste. In tal caso la Società deve informare l'Interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Infine, l'Interessato ha sempre il diritto di proporre reclamo all'Autorità di Controllo.

7.6. Trattamento dei Dati Personali effettuato da Terze Parti

I Dati Personali possono essere trattati in nome e per conto del Titolare del Trattamento da Terze Parti (fornitori, business partner o consulenti) incaricati a svolgere attività che comportino l'uso di Dati Personali del Titolare. Tali attività posso essere svolte solo previa sottoscrizione di un apposito contratto che deve avere le caratteristiche riportate all'art.5.2 del MOP.

Il Gruppo ERG ha definito uno standard di nomina a Responsabile. Qualora le Terze Parti propongano modifiche allo standard o propongano accordi differenti, è necessario coinvolgere l'unità organizzativa Compliance 231 & Privacy per la revisione degli stessi al fine di garantire il rispetto delle misure necessarie per tutelare i Dati Personali trattati dal Gruppo.

7.7. Trasferimento dei Dati Personali

Nello svolgimento della propria attività può accadere che il Gruppo ERG trasferisca i Dati Personali in Paesi Extra-UE.
Il trasferimento è ammesso esclusivamente se si verifica almeno una delle seguenti condizioni:

- il trasferimento è effettuato verso paesi che garantiscano un adeguato livello di tutela dei Dati Personali e che sono stati individuati dalla Commissione Europea;
- l'Interessato ha manifestato il proprio consenso espresso;
- il trasferimento è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'Interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'Interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'Interessato;
- il trasferimento è necessario per far valere o difendere un diritto in sede giudiziaria, sempre che i Dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- il trasferimento è effettuato verso Terze Parti tramite un contratto che includa le clausole contrattuali standard di protezione dei Dati Personali definite dalle Disposizioni Privacy.

7.8. Ispezioni Autorità di Controllo

Le Autorità di Controllo competenti possono effettuare ispezioni presso le Società del Gruppo finalizzate a verificare l'effettiva applicazione da parte di queste ultime delle Disposizioni Privacy.
Nel corso di tali ispezioni, ERG adotterà le cautele ed i presidi previsti dalle Norme Interne riguardante la gestione delle visite ispettive (Procedura "Gestione visite ispettive").
In generale, a fronte di contatti tra il Personale e funzionari rappresentanti gli uffici dell'Autorità di Controllo, occorre immediatamente avvisare il responsabile del soggetto coinvolto e il Referente.
Documenti o informazioni connesse al Trattamento possono essere consegnati agli ispettori solo con l'autorizzazione del Referente, che dovrà assistere alla visita ispettiva.
Il Referente supporta il Delegato Privacy nell'eventuale interazione con l'Autorità di Controllo, facilitandone l'accesso alle informazioni necessarie e cooperando con la medesima.

8. IMPLEMENTAZIONE E AGGIORNAMENTO DEL MOP

Il Referente, con il supporto dell'unità organizzativa Compliance 231 & Privacy, è responsabile:

- di verificare l'adozione del MOP da parte delle Società del Gruppo ERG;
- dell'aggiornamento del MOP, anche a seguito di eventuali segnalazioni delle unità organizzative e/o di qualsiasi anomalia o difficoltà riguardo all'applicazione del MOP e delle correlate Disposizioni Privacy;
- di fornire consulenza al Personale del Gruppo ERG in merito a qualunque dubbio o

questione inerente all'applicazione del MOP.

Il MOP è un documento in continua evoluzione, che deve essere aggiornato laddove intervengano modifiche normative in materia di protezione dei Dati Personali o cambiamenti organizzativi interni al Gruppo ERG che comportino modifiche alle Norme Interne ed istruzioni contenute nel MOP o nell'Organizzazione Privacy, nonché nei casi in cui il Gruppo modifichi le proprie Misure di Sicurezza tecniche e organizzative.

Per quanto non espressamente regolato all'interno del MOP si richiamano le Norme Interne, anche diverse da quelle citate nel MOP stesso, in quanto tali documenti, oggetto di costante aggiornamento, fanno parte integrante e sostanziale di quest'ultimo.

9. SEGNALAZIONE DELLE VIOLAZIONI E GARANZIE

Le Società del Gruppo ERG garantiscono la possibilità di effettuare segnalazioni di violazioni delle Disposizioni Privacy e del presente MOP.

In particolare, qualora un soggetto ricompreso tra il Personale del Gruppo ERG, le Terze Parti e tutti coloro che operano, in Italia e all'estero, in nome o per conto del Gruppo ERG abbia il ragionevole sospetto che si sia verificato o che possa verificarsi un Data Breach o comunque una violazione del MOP, deve comunicarlo:

- all'unità organizzativa Compliance 231 & Privacy utilizzando uno dei seguenti canali:
  - posta elettronica: casellaprivacy@erg.eu ;
  - posta ordinaria, scrivendo a *Compliance 231 & Privacy* – via De Marini, 1 – 16149 Genova; o
- tramite la piattaforma di whistleblowing del Gruppo ERG alla quale si accede dall'indirizzo https://erg.integrityline.com/frontpage, utilizzando qualsiasi browser, anche attraverso dispositivi mobili. L'invio, la ricezione e la gestione delle Segnalazioni Whistleblowing (comprese le tutele riservate al segnalante) sono regolati dalla Linea Guida "Whistleblowing" adottata dal Gruppo ERG.

10. SISTEMA SANZIONATORIO

La commissione di atti in violazione del MOP nonché, più in generale, la violazione delle Disposizioni Privacy, può esporre il Titolare a diverse tipologie di responsabilità e conseguenti sanzioni (di carattere amministrativo e/o penale).

Tali violazioni costituiscono inadempienza agli obblighi contrattuali e alle Norme Interne e possono dare corso all'avvio di procedimenti per l'irrogazione di sanzioni nei confronti dei relativi autori.

In particolare:

- i dipendenti del Gruppo ERG sono soggetti alle sanzioni previste dal Contratto Collettivo Nazionale di Lavoro (o documento equiparabile) pro tempore applicabile; le stesse saranno applicate dall'unità organizzativa Human Resources;
- i componenti degli organi di amministrazione e di controllo sono soggetti alla revoca dall'incarico deliberata dall'assemblea dei soci di riferimento;
- i collaboratori e le Terze Parti sono soggetti alle sanzioni previste nei contratti stipulati con le Società del Gruppo ERG e possono arrivare alla sospensione e, nei casi più gravi alla risoluzione del rapporto contrattuale.

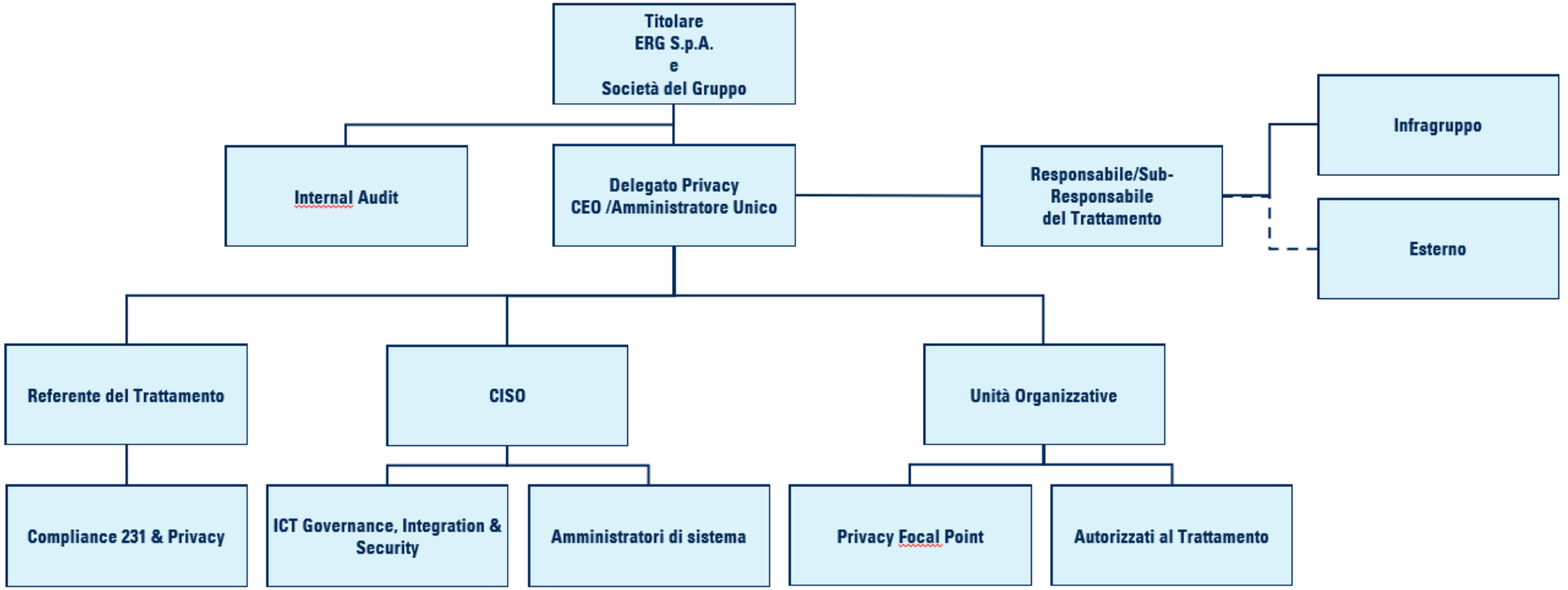
In tutti i casi, la sanzione dovrà essere commisurata al livello di responsabilità del soggetto coinvolto, all'intenzionalità e alla gravità del comportamento e dovrà essere fatta salva la garanzia del contraddittorio e potrà essere applicata indipendentemente dall'avvio di un procedimento da parte dell'Autorità di Controllo.

11. DIFFUSIONE, COMUNICAZIONE E FORMAZIONE

Il MOP è divulgato, tramite i canali comunicativi interni (es. sito intranet aziendale) ed esterni del Gruppo (sito internet), a tutto il Personale del Gruppo ERG e alle Terze Parti, agli stakeholder e agli altri soggetti che intrattengono rapporti con il Gruppo.

Il Gruppo predispone ed attua piani di formazione dedicati al trattamento e alla tutela dei Dati Personali, agli strumenti per prevenire Data Breach, ai contenuti del MOP e alle Disposizioni Privacy, così da assicurare la diffusione e la corretta comprensione dei principi espressi nel MOP e sensibilizzare il Personale del Gruppo ERG.

ALLEGATO 1: ORGANIZZAZIONE PRIVACY DEL GRUPPO ERG



Con riferimento ai servizi infragruppo, alcune società del Gruppo ERG agiscono in qualità di Responsabili o Sub-Responsabili del Trattamento.