**Kineo Energy e Facility S.r.l.**
Via dell'Arcoveggio, 70
40129 Bologna (BO)
Tel: 051 0185061 - Fax: 051 0822193
C.F.-P.IVA-R.I. 01160950323

# ELENCO DELLE MISURE DI SICUREZZA

Ai sensi dell'art. 32 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, di seguito *Regolamento*, ogni Titolare del trattamento (**Kineo Energy e Facility S.r.l.**, nella persona del suo legale rappresentante *pro tempore*), "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (…), mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*". Nel valutare l'adeguatezza del livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (comma 2).

Tra le misure da adottare, "*tra le altre, se del caso*", vi sono:

- **la pseudonimizzazione e la cifratura dei dati personali** (misura non esistente, la cui introduzione può essere valutata dal Titolare del trattamento). Si tratta di una misura non obbligatoria. Nei *Considerandа* di Parlamento e Consiglio Europeo si sottolinea che: "*per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è*

*opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale*" (C. 83).

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (misura già presente);
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (misura già presente);
- **una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento (misura non esistente, la cui introduzione può essere valutata dal Titolare del trattamento);
- Accesso limitato ai dati personali da parte dei soli Incaricati autorizzati al trattamento, istruiti in tal senso dal Titolare del trattamento (misura già presente) (comma 4).
- Si rammenta, con riferimento alle misure di sicurezza, la possibilità di aderire a **codici di condotta o sistemi di certificazione**, alla cui adesione è assegnata una funzione probatoria di conformità al *Regolamento* (opzione da valutare in considerazione delle conseguenze in termini di presunzione relativa di conformità) (comma 3).
- Si rammenta, inoltre, che la mancata adozione delle predette misure dà luogo a sanzioni amministrative pecuniarie fino a 10.000.000 euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83.4 del *Regolamento*).

## MISURE DI SICUREZZA DI CARATTERE ORGANIZZATIVO E TECNICO

## MISURE DI SICUREZZA GENERALI

- Descrizione scritta degli interventi effettuati da terzi. Quando ci si avvale di soggetti esterni per l'adozione pratica delle misure di sicurezza minima, si richiede la descrizione scritta dell'intervento effettuato che ne attesta la conformità Al *Regolamento* (misura esistente).
- Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione. Periodicamente, con cadenza annuale, sono aggiornati gli ambiti del trattamento consentito agli incaricati e agli addetti alla gestione o manutenzione dei sistemi elettronici (misura esistente).
- Istruzioni dettagliate agli incaricati. A ogni incaricato sono state consegnate istruzioni dettagliate e complete riguardanti il trattamento dei dati personali, a seconda dei suoi compiti e dei dati trattati (misura esistente).
- Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali (misura esistente).
- Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento (misura esistente).
- Istruzioni per i supporti removibili, nel caso in cui supportino dati sensibili o giudiziari (misura esistente).
- Istruzioni scritte finalizzate al controllo e alla custodia dei documenti cartacei (misura esistente).
- Distruzione dei supporti removibili. Nel caso di dati sensibili o giudiziari, i supporti removibili che contengono tali dati, se non utilizzati, sono distrutti o resi inutilizzabili ovvero possono essere usati da personale non autorizzato solo dopo che i dati in essi contenuti sono resi non intellegibili e tecnicamente irrecuperabili (misura esistente).

- Redazione di un piano di formazione per gli incaricati. È previsto un piano di formazione degli incaricati, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevedere eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare. La formazione è programmata al momento dell'ingresso in azienda, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali (misura esistente).
- Il Titolare del trattamento ha valutato l'opportunità di inserire la documentazione formativa sulla piattaforma on-line dell'Azienda. A essa i neo-assunti e tutti i dipendenti hanno accesso tramite credenziali. La formazione è un diritto e un dovere per i dipendenti. Per tale ragione, l'adempimento del dovere formativo rappresenta l'oggetto di una obbligazione contrattuale, di cui il dipendente si fa carico attraverso la sottoscrizione di apposita dichiarazione di presa visione (**misura da implementare**).
- Procedure per il ripristino dei dati. Sono state adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi non superiori ai 7 giorni.

## MISURE DI SICUREZZA ADOTTATE CON RIFERIMENTO A TRATTAMENTI NON AUTOMATIZZATI

- Dotazione di serrature per l'archivio e per l'ufficio (misura esistente).
- Archivio ad accesso controllato. L'accesso all'archivio è controllato dagli incaricati al trattamento. Dopo l'orario di chiusura possono accedere all'archivio solo le persone preventivamente autorizzate o identificate e registrate (misura esistente).
- Controllo dei documenti con dati sensibili o giudiziari da parte degli incaricati. Quando i documenti contenenti dati sensibili o giudiziari sono affidati agli incaricati del trattamento, i medesimi atti sono controllati e custoditi dagli

incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate (misura esistente).

- Custodia in classificatori o armadi non accessibili. I dati cartacei sono archiviati in modo da permettere l'accesso esclusivamente agli incaricati al trattamento degli stessi e di non essere accessibili a persone non autorizzate (misura esistente).

## MISURE DI SICUREZZA ADOTTATE CON RIFERIMENTO A TRATTAMENTI AUTOMATIZZATI

- Sistema Operativo. Il Sistema operativo deve poter autenticare in maniera sicura e univoca gli incaricati al trattamento dei dati (misura esistente).
- Copie di *back-up*. Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza giornaliera (misura esistente).
- Antivirus. Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati giornalmente (misura esistente).
- Credenziali di autenticazione assegnate individualmente a ogni incaricato. Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autenticazione univocamente associata all'incaricato e relativa a uno specifico trattamento o a un insieme di trattamenti. Inoltre, il codice di identificazione, quando utilizzato, non è mai assegnato ad altri incaricati, nemmeno in tempi diversi. Si richiede una parola chiave di almeno 8 caratteri. È prevista la disattivazione delle vecchie credenziali. Sono impartite disposizioni scritte per la disponibilità dei dati. L'autenticazione avviene mediante *user-id* e *password* (misura esistente).
- Profili di autorizzazione di ambito diverso per diversi incaricati. Nel caso in cui gli incaricati possano accedere solo a certi tipi di dati o effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. È utilizzato un sistema di autorizzazione. I profili di autorizzazione

sono specificati prima di ogni trattamento. Vi è una verifica periodica del profilo di autorizzazione (misura esistente).

- Aggiornamento *software* semestrale (annuale). Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti sono effettuati semestralmente (o annualmente se sono presenti solo dati comuni), (misura esistente).
- Installazione di un *firewall*. Nel caso di trattamento di dati sensibili o giudiziari con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un *firewall software* o *hardware* per evitare l'accesso abusivo ad essi (misura esistente).