REGOLAMENTO EUROPEO 2016/679

Manuale Privacy

ELETTROMIL SRL

Privacy

INDICE

Allegati:
nomine
informative
certificazioni impianti
manutenzione impianti

CAPITOLO 1 - Introduzione

Generalità

Il Regolamento Europeo 2016/679, entrato in vigore il 25 Maggio 2016 e applicativo dal 25 Maggio 2018, disciplina la normativa in materia di tutela della privacy, partendo dal presupposto che *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano".*

In data 19 settembre 2018 è entrato in vigore il Decreto legislativo 101/2018 recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati".*

Il Regolamento garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Per garantire che i rischi di distruzione, perdita, accessi non controllati, furto dei dati personali, siano ridotti al minimo devono essere adottate idonee e preventive misure di sicurezza.

Il presente Manuale Privacy è redatto per definire tutte le misure di sicurezza che la società Elettromil srl ha adottato e che debbono essere adottate in via preventiva dall'azienda, conformemente a quanto previsto dal Regolamento Europeo Privacy UE/2016/679.

Nel Manuale Privacy sono riportate le misure adottate per prevenire e ridurre al minimo i rischi di diffusione o comunicazione nonché distruzione, perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del trattamento, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

Obiettivi

Per l'attuazione della tutela dei dati personali trattati, l'Azienda si impegna a porre in essere quanto di seguito espresso:

- definire la finalità del trattamento dei dati
- definire i principi del trattamento dei dati
- definire gli strumenti utilizzati per il trattamento dei dati
- definire i profili di sicurezza.

A tale scopo provvede alla:

- individuazione in forma scritta dei designati al trattamento dei dati
- predisposizione delle misure di sicurezza
- elaborazione del manuale della privacy
- vigilanza sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati

- formazione del personale relativamente alle disposizioni previste dal GDPR in materia di protezione dei dati personali

Campo di applicazione

Il Manuale Privacy definisce le politiche e gli standards di sicurezza in merito al trattamento dei dati personali, individuando le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza.

Il presente Manuale riguarda il trattamento di tutti i dati personali:

- personali
- identificativi
- particolari.

Trattati con:
- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione
- Archivi cartacei

Il Documento deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

Il Regolamento prevede che il Manuale Privacy sia definito con un contenuto informativo minimo, cioè è indispensabile, che contenga:

- l'elenco dei trattamenti di dati personali;

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

- l'analisi dei rischi che incombono sui dati;

- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

- la previsione di interventi formativi dei designati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire 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 già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al GDPR, all'esterno della struttura del Titolare;

- per i dati personali idonei a rivelare lo stato di salute, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Finalità

Le misure individuate perseguono la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

In tal senso il presente documento individua soggetti, compiti e responsabilità in materia di sicurezza dei trattamenti, descrivendo le modalità per l'analisi e la valutazione dei rischi, nonché le misure necessarie per ridurre tali rischi al minimo. In termini operativi il presente documento individua non soltanto la protezione del patrimonio informativo da accessi non autorizzati e rischi di cancellazione, distruzione o perdita di dati, ma anche la limitazione degli effetti causati dall'eventuale occorrenza di tali cause.

La stesura del presente documento è aderente alle seguenti linee guida:

a- analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento;

b- l'individuazione e la valutazione del rischio;

c- l'individuazione delle misure preventive e correttive;

d- l'individuazione di istruzioni ai designati e la previsione di un programma formativo;

e- la gestione da parte di terzi delle banche dati aziendali.

CAPITOLO 2 - Anagrafica Aziendale

Elettromil SRL

Sede Legale: Via Sardegna 29, Roma

Sede operativa per il manuale privacy: Via dei Mestieri 10, Castiglione del Lago (PG)

Descrizione attività svolta: progettazione, produzione, riparazione di trasformatori di reattanze di media e bassa tensione e relativa carpenteria metallica.

CAPITOLO 3 - Riferimenti Normativi

1. REGOLAMENTO EUROPEO 2016/679

2. Decreto legislativo 101/2018 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati*".

Definizioni

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

Dato personale:qualsiasi informazione riguardante una persona fisica identificata o identificabile (**Interessato**).

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persone fisica in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, la affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche ed organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identifica o identificabile.

Titolare del Trattamento: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Destinatario: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Terzo: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che non sia

l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Consenso dell'Interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine o i dati dattiloscopici.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi, di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Dati particolari: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati genetici e biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi allo stato di salute e la vita sessuale o all'orientamento sessuale della persona (Art. 9 GDPR 670/2016)

Dati giudiziari: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Designati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile che operano sotto la loro autorità (Art. 2 *quaterdecies* D.lgs. 101/2018).

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli designati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Garante: l'Autorità di cui all'articolo 153 D.lgs 101/2018.

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti

tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato O utente ricevente, identificato o identificabile.

CAPITOLO 4 - Elenco dei trattamenti dei dati personali

In questa sezione sono riportate le tipologie di trattamento effettuate dal Titolare.

******

Fornitori

	Fornitori
Raccolta	**x**
Registrazione	**x**
Organizzazione	**x**
Conservazione	**x**
Consultazione	**x**
Elaborazione	**x**
Modificazione	**x**
Selezione	**x**
Estrazione	**x**
Raffronto	**x**
Utilizzo	**x**
Interconnessione	**x**
Blocco	**x**
Comunicazione	**x**
Diffusione	
Cancellazione	**x**
Distruzione	**x**

Elettromil srl entra in possesso dei dati dei fornitori tramite*:*

- comunicati dai fornitori

Elettromil srl entra in possesso dei seguenti dati dei fornitori:
- dati fiscali
- anagrafici
- dati bancari

Elettromil srl conserva i dati identificativi dei Fornitori in archivi cartacei e server.

Finalità del trattamento: esecuzione di obblighi derivanti da un contratto o per adempiere, prima e dopo l'esecuzione del contratto, a specifiche richieste; legittimo interesse; adempimento di obblighi di legge di natura amministrativa, contabile, civilistica, fiscale, regolamenti, normative nazionali e comunitarie, gestione dei fornitori (amministrazione de fornitori, gestione e adempimenti di contratti, ordini, arrivi, fatture), gestione del contenzioso (inadempimenti contrattuali, diffide, transazioni, recupero crediti, arbitrati, controversie giudiziarie).

Il trattamento dei dati funzionali all'espletamento di tali obblighi è necessario per la corretta gestione del rapporto contrattuale di fornitura ed il loro conferimento è obbligatorio per attuare le finalità sopra indicate.

****

Dipendenti

	Dipendenti
Raccolta	**x**
Registrazione	**x**
Organizzazione	**x**
Conservazione	**x**
Consultazione	**x**
Elaborazione	**x**
Modificazione	**x**
Selezione	**x**
Estrazione	**x**
Raffronto	**x**
Utilizzo	**x**
Interconnessione	**x**
Blocco	**x**
Comunicazione	**x**
Diffusione	
Cancellazione	**X**
Distruzione	**X**

Elettromil srl entra in possesso dei dati dei dipendenti tramite:

- direttamente dai dipendenti
- curriculum ricevuti

Elettromil srl è in possesso dei seguenti dati dei dipendenti:

- dati bancari e fiscali
- dati particolari, anagrafici
- dati contrattuali, dati dei familiari, dati personali

Elettromil srl conserva i dati identificativi dei Dipendenti in archivi cartacei e server.

Finalità: adempimenti connessi al versamento delle quote di iscrizione ai sindacati, adempimento di obblighi fiscali e contabili, obblighi retributivi e contributivi, contratto di assunzione, gestione data protection, gestione del contenzioso, gestione del personale, igiene e sicurezza del lavoro, reclutamento, selezione, valutazione e monitoraggio del personale: formazione professionale, test attitudinali, servizi di controllo interno (della sicurezza, della produttività, della qualità dei servizi, dell'integrità del patrimonio), trattamento giuridico ed economico del personale, verifica dell'idoneità al servizio.

****

Notifica dei dati trattati

Il Titolare a seguito dell'analisi dei rischi dei diritti e delle libertà delle persone fisiche, tenuto conto dei tipi, della natura, dell'oggetto e delle finalità dei trattamenti dei dati eseguiti, ha ritenuto la non necessari età della Valutazione d'Impatto ex art. 35 GDPR e conseguentemente di non dover procedere alla consultazione preventiva del Garante ex art. 36 GDPR.

****

Data Retencion

I dati personali di dipendenti, clienti e fornitori vengono conservati per dieci anni dalla conclusione dei rapporti contrattuali o dalla data di emissione del documento, in base alla normativa in materia di prescrizione, fatte salve eventuali interruzioni o sospensioni di termini.

CAPITOLO 5 - Organigramma di compiti e delle responsabilità

TITOLARE DEL TRATTAMENTO

Quando il trattamento è effettuato da una persona giuridica, da una Pubblica Amministrazione o da un qualsiasi altro Ente, Titolare del trattamento è l'Entità nel suo complesso. Il Titolare del trattamento definisce la Politica della Sicurezza dei dati personali, stabilisce gli obiettivi che essa deve perseguire, identifica gli impegni e assegna le risorse necessarie al corretto funzionamento del Sistema Sicurezza al fine di applicare e predisporre le misure di sicurezza idonee alla tutela dei dati trattati.

Compiti e attribuzioni:

- definire la finalità del trattamento dei dati;
- definire le modalità del trattamento dei dati;
- definire gli strumenti utilizzati per il trattamento dei dati;
- definire i profili di sicurezza.

Il Titolare è l'unico soggetto autorizzato, oltre alla P.S., ad accedere alle immagini registrate dal sistema di videosorveglianza.

A tale scopo provvede alla:

- nomina dei Designati e del referente al trattamento dei dati;
- predisposizione delle misure di sicurezza;
- elaborazione del manuale privacy;
- vigilanza sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati;
- formazione del personale relativamente alle disposizioni previste dal GDPR in materia di protezione dei dati personali.

DESIGNATO CON FUNZIONE DI REFERENTE PER IL TRATTAMENTO

Il Titolare ha individuato l'Ing. Daniele Giammetti, quale Designato con funzione di Referente per il Trattamento dei dati personali ex artt. 2 quaterdecies D.lgs 101/2018 e art. 29 GDPR, conferendogli a

mezzo di nomina scritta i seguenti compiti:
a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

b) definire per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

c) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati. A cura del Designato, dovranno poi essere affissi i cartelli contenenti l'informativa, in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica, integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;

d) assicurare che la comunicazione a terzi avvenga entro i limiti stabiliti dalla legge.

e) adempiere agli obblighi di sicurezza di cui al successivo capitolo 7, quali:

- applicare, tramite l'Amministratore di sistema, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;

- rispettare la politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;

- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;

- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

- verificare con cadenza semestrale le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito;

- controllare che tutte le misure di sicurezza riguardanti i dati personali siano applicate;

f) fare osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;

g) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;

h) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;

i) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.

Il Designato tratta i dati personali soltanto su istruzione documentata del Titolare del Trattamento.

Il Designato garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza.

Al termine della durata dell'incarico, su scelta del Titolare, il Designato, deve cancellare o restituire tutti i dati personali relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione preveda la conservazione dei dati.

Il Designato deve consentire e contribuire all'attività di revisione comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questo incaricato.

Il Designato deve informare immediatamente il Titolare, qualora a suo parere, un'istruzione violi il Regolamento o altre disposizioni nazionali o dell'Unione relative alla protezione dei dati.

Il Designato deve vigilare sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati;

Il Designato deve organizzare il piano formativo del personale relativamente alle disposizioni previste dal Codice Europeo in materia di protezione dei dati personali;

L'incarico di designato è attribuito personalmente ed è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.

AMMINISTRATORE DI SISTEMA

L'elettromil srl ha nominato quale Amministratore di sistema il Sig. Emanuele Paolucci, con i seguenti compiti:

- mantenere in efficienza il Sistema Informativo, sia per quanto riguarda il software che l'Hardware;

- comunicare al Titolare eventuali esigenze di installazione di nuovo software o hardware ed attenersi alle sue disposizioni;

- realizzare in proprio e/o tramite personale delle aziende fornitrici e/o di consulenti eventualmente preposti, quanto richiesto dal presente Manuale Privacy, limitatamente a ciò che concerne il sistema informativo;

- eseguire, in proprio e/o tramite personale delle aziende fornitrici, eventuali interventi sull'Hardware e sul software, per nuove installazioni, normale manutenzione o anomalie;

- se il tempo richiesto per l'intervento, compreso quello per "Disaster recovery", è superiore a sette giorni dovrà mettere a disposizione dell'utente una postazione, anche temporanea, che contenga gli stessi dati e fornisca le stesse prestazioni;

- relazionare al Titolare, su richiesta dello stesso, circa lo stato del Sistema informativo, il livello di servizio fornito all'utenza e lo stato di avanzamento di eventuali interventi sull'Hardware e sul Software;

- controllare periodicamente che il software antivirus sia aggiornato;

- implementare il sistema automatico di aggiornamento del software e del sistema operativo;

- e altre operazioni necessarie al fine di ridurre al minimo tutti gli eventuali rischi connessi alla gestione del sistema informativo.

- generazione ed attribuzione ai designati delle credenziali di accesso al sistema;

- controllo del funzionamento e manutenzione del sistema di back up con verifica costante del funzionamento del disco di back up.

- assicurarsi del corretto funzionamento degli strumenti elettronici;

- fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;

In generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

DESIGNATI

l'Elettromil srl ha provveduto a nominare quali designati al trattamento i Sig. Marco Chionne e Yuri Bosetti, individuando i seguenti compiti:

A) custodia delle credenziali di autenticazione:
I designati hanno il compito della custodia delle credenziali di autenticazione. Nello specifico dovranno:

- gestire e custodire le credenziali per l'accesso ai dati della propria postazione;

- predisporre, una busta all'interno della quale deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto, individuato nel cassetto chiuso della scrivania del Sig. Marco Chionne, situata all'interno dell'ufficio del suddetto Sig. Chionne.

B) misure di sicurezza:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al salvataggio periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal presente manuale; in particolare dovrà effettuare un back-up giornaliero;

- di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;

- assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato;

- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro;

- di segnalare tempestivamente all'Amministratore di sistema ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

In relazione agli incarichi affidati, i Designati dovranno:

- fornire al Titolare o al Referente, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività

di controllo;

- in generale, prestare la più ampia e completa collaborazione al Titolare ed al Referente al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

C) trattamento dati:

I Designati dovranno:

- trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;

- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare o dal Referente, in particolare dovrà:

a) per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

b) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;

c) conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

d) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate o riporli nel loro luogo di conservazione;

e) utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;

f) in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione all'Amministratore di sistema;

- segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Titolare e secondo le modalità stabilite dal medesimo; mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e, comunque, in modo lecito e secondo correttezza;

- fornire al Titolare, a semplice richiesta e secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo.

In generale, prestare la più ampia e completa collaborazione al tTtolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

CAPITOLO 6 - Analisi dei rischi

Calcolo dei parametri da inserire nelle schede di valutazione

Attribuzione Score di pericolo (SP) ed azione correttiva.
Ad ogni punto di controllo presente in una check-list pericoli (CLP) è associato uno score di pericolo (SP).

Quando un punto di controllo non è verificato (es. manca il Sistema di Backup dei dati) allora comparirà nella scheda di valutazione l'azione correttiva relativa (es. ''Installare programma per il Backup e ripristino dati',) ed il relativo score di pericolo (SP).

Calcolo della probabilità

PROBABILITÀ P	LIVELLO	DEFINIZIONI / CRITERIO
4	Altamente probabile	Esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi del danno ipotizzato per i lavoratori. Si sono già verificati danni per la stessa mancanza rilevata nella stessa Azienda o in azienda simile o in situazioni operative simili. - TI verificarsi del danno conseguente la mancanza rilevata non susciterebbe alcuno stupore in azienda
3	Probabile	La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto E' noto qualche episodio in cui alla mancanza ha fatto seguito il danno. - TI verificarsi del danno iporizzato, susciterebbe una moderata sorpresa in azienda
2	Poco probabile	La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi Sono noti rari episodi già verificatisi TI verificarsi del danno ipotizzare susciterebbe grande sorpresa
1	Improbabile	La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti Sono estremamente rari episodi già verificatisi - TI verificarsi del danno susciterebbe incredulità

Calcolo dei rischi R e dei tempi di intervento

Per ogni punto di una CLP non verificato (associato al relativo score di pericolo SP) occorre calcolare il rischio legato a quella mancanza (es. mancanza del sistema di Backup).
Il rischio R è dato dallo score di pericolo SP moltiplicato per la probabilità P.

R=SPXP

Mappatura del rischio

Tipo	*Probabilità*	*Pericolo*	*Rischio*
Eventi distruttivi, naturali o artificiali, nonché dolosi accidentali o dovuti ad incuria	1	4	4
Danni provocati da un possibile guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	2	1	2
Sistema di identificazione (esistente)	0	0	0
Mancata impostazione scadenza password	0	4	0
Test Firewall	0	2	0
Impostazione di sistema di Stand by (esistente)	0	0	0
Gruppo di continuità (esistente)	0	0	0
Programma antivirus (esistente ed aggiornato quotidianamente)	0	0	0
Firewall	0	2	0
Utilizzo di device provenienti dall'esterno dell'azienda (chiavetta usb) assente	0	0	0
Back Up (con gruppo di continuità)	1	1	1
Accesso a dati particolari da parte di soggetti non autorizzati	1	1	1
Possibile sottrazione di credenziali di autenticazione	1	2	2
Errore materiale da parte del personale incaricato	1	3	3

Accesso non autorizzato a locali e reparti dove vengono custoditi dati personali	2	2	4
Prove di ripristino dei dati non effettuate	2	2	4
Sistema di videosorveglianza	1	2	2

CAPITOLO 7.1 - Misure di sicurezza

In questa sezione sono riportate, in forma sintetica, le misure di sicurezza adottate ai sensi dell'art. 32 GDPR al fine di limitare i rischi individuati dall'analisi di cui al Capitolo 6.
Per misura si intende:

- lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia;

- tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Senza procedure di controllo periodico, infatti, nessuna misura può essere considerata completa.

Le misure da adottare per garantire l'integrità e la disponibilità dei dati sono sancite dal presente manuale privacy che inoltre indica i provvedimenti che il Titolare, l'ADS, il Referente ed i Designati, devono mettere in atto per garantire il livello di sicurezza dei dati in loro possesso.

******

INDIVIDUAZIONE DEI LUOGHI DEL TRATTAMENTO DEI DATI PERSONALI

I dati personali dei dipendenti e fornitori vengono trattati dal Titolare, dal Referente, dai Designati, e dall'Amministratore di sistema presso la sede operativa dell'Azienda in Castiglione del lago, alla Via dei Mestieri n.10. In particolare i dati vengono trattati nei rispettivi ambienti di lavoro dai designati, Sig.ri Marco Chionne e Yuri Bosetti.

INDIVIDUAZIONE DEGLI ARCHIVI CARTACEI E MISURE DI SICUREZZA:

Tipologia	Armadio generico con serratura		
	Scrivania con serratura		
Sicurezza del locale	Accesso non consentito al pubblico		
	Sistema di allarme		
	Cancello e recinzione		
	Posizionamento al primo piano		
	Sistema antincendio		
	Estintori		
	Chiusura porte uffici con serrature		
	Porta di ingresso principale chiusa		

	e controllata		
	Struttura antisismica		
	Formazione del personale designato al trattamento sulla disciplina di protezione dei dati personali, sui rischi che incombono sui dati e sulle misure disponibili per prevenire eventi dannosi	Piano formativo del personale	
	videosorveglianza	DVR posizionato in alto in modalità non accessibile, chiuso con lucchetto. Le immagini registrate sono visionabili solo dal Titolare e da P.S.	
Note			

All'interno degli uffici dei sopra indicati dei designati e del Referente, sono presenti:
- armadio generico con serratura;
- scrivania con cassetto chiuso a chiave.

MISURE DI SICUREZZA DEI LOCALI:
L'ufficio ove sono archiviati i dati personali è posizionato al primo piano, quindi rialzato rispetto al piano terra. La porta dell'ufficio è dotata di serratura.
L'azienda nel suo complesso è dotata di recinzione videosorvegliata, porta di ingresso con sistema di allarme e sistema antincendio.
La struttura è antisismica.

ELENCO ARCHIVI INFORMATICI E MISURE DI SICUREZZA:
Gli archivi informatici presenti in azienda sono di seguito indicati:

Tipologia	Computer designati in rete		
	Computer Referente in rete		
	Computer Titolari in rete		
	Server		
Tipo di supporto	Hard disks		
Sistemi di protezione	Password	Otto caratteri alfanumerici	

	Firewall	Eseguiti test di funzionamento	
	Antivirus	Aggiornato quotidianamente CLAMWIN	
Sistemi di sicurezza	Back up	quotidiano	
	Supporto del back up	Server	
	Numero copie back up	n.1 copia incrementale	
	Luogo di conservazione dei back up	Archiviato in disco fisso del server, situato in stanza con serratura.	
	Procedure di ripristino	Controllo sul disco di back up effettuato	
	Tempi di ripristino	immediato	
	Formazione del personale designato al trattamento sulla disciplina di protezione dei dati personali, sui rischi che incombono sui dati e sulle misure disponibili per prevenire eventi dannosi	Piano formativo del personale	
Sicurezza del locale	Accesso vietato al pubblico		
	Cancello e recinzione		
	Porta di ingresso principale chiusa e controllata		
	Sistema di allarme		
	estintori		
	Sistema antincendio		
	Uffici dotati di porta con serratura		
	Struttura antisismica		
	Videosorveglianza		
Note			

CAPITOLO 7.2 - Privacy nella Direzione Human Resource

******

AUTORIZZAZIONE/ESCLUSIONE ALL'USO DEGLI STRUMENTI INFORMATICI:

All'inizio del rapporto lavorativo, l'Ente valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di internet e della posta elettronica da parte dei designati.
Successivamente e periodicamente l'Ente valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica.
E' fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.
I casi di esclusione possono riguardare: 1) l'utilizzo del computer o di altri device; 2) l'utilizzo della posta elettronica; 3) l'accesso a internet.
Le eventuali autorizzazioni o esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici, nonché al principio di necessità di cui al GDPR. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi, solo i designati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno nonché il Referente.
Tali autorizzazioni o esclusioni sono divenute necessarie alla luce del provvedimento del Garante 01.03.2007 nonché, da ultimo, sulla base dei principi del GDRP che impone di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.
L'organizzazione è esclusiva titolare e proprietaria dei devices messi a disposizione dei designati e del Referente ai soli fini dell'attività lavorativa. L'ente è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri devices digitali o archiviati in modo cartaceo nei propri locali. I designati ed il Referente non possono presumere o ritenere che le informazioni le registrazioni e i dati da loro trattati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) siano privati o personali.
E' fatto espresso divieto ai designati ed al Referente di copiare, diffondere o comunicare i dati sopra indicati senza espressa autorizzazione del titolare.
I devices assegnati sono uno strumento lavorativo nelle disponibilità del designato esclusivamente per un fine di carattere lavorativo.
La società Elettromil srl, quale titolare del trattamento di tutti i dati personali nonché proprietaria dei devices aziendali, messi a disposizione degli incaricati, ha nominato quali designati al trattamento dei dati di cui sopra, il Responsabile amministrativo, Sig. Marco Chionne, ed il Sig. Yuri Bosetti, quali uniche risorse dell'azienda autorizzate al trattamento dei dati personali tramite la propria postazione lavorativa nonché attraverso l'utilizzo di posta elettronica e certificata. I suddetti designati, sono gli unici a possedere le credenziali di accesso al proprio computer e quindi anche alla posta elettronica.
In base al principio del "need to know" i designati ed il il Referente trattano i dati personali esclusivamente tramite computer in rete, ma con accesso esclusivo alle banche dati di dipendenti, e fornitori, senza che gli altri dipendenti dell'azienda possano accedervi.

I dati personali vengono archiviati nel server al quale non posso accedere terzi che non siano i soggetti sopra indicati. I dati vengono poi salvati quotidianamente dopo il Back up in disco esterno posto in sicurezza all'interno dell'armadio con serratura posto all'interno dell'ufficio del Referente.

Sono state individuate misure di disaster recovery, consistenti nella verifica del funzionamento del disco esterno di back up effettuato trimestralmente.

Le credenziali del Sig. Marco Chionne sono conservate in busta chiusa all'interno di cassetto con serratura della propria scrivania e copia della chiave viene consegnata al legale rappresentante, Sig. Stefano Milic, che la potrà utilizzare in caso di assenza prolungata del designato. Ugualmente si dica per la conservazione delle credenziali del designato Sig. Yuri Bosetti.

LE PASSWORD:

Il designato per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:
1) le password sono assolutamente personali e non vanno mai comunicate ad altri;
2) occorre cambiare la password ogni tre mesi e comunque immediatamente allorquando si ritenga che sia diventata poco sicura;
3) le password devono essere lunghe almeno otto caratteri;
4) le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, post it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, cellulari);
5) evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente.
E' fatto espresso divieto di utilizzare come password:
1) il proprio nome e cognome;
2) data di nascita;
3) password già utilizzate in precedenza;
4) parole banali e comuni.
L'Amministratore di sistema stabilisce una funzione automatica di cambio password che impone al designato la modifica della propria password ogni tre mesi.

OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendali. Il designato deve quindi obbligatoriamente eseguire le seguenti operazioni:
1) se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti;
2) bloccare il proprio computer prima delle pause e, in generale, ogni qual volta abbia bisogno di allontanarsi dalla propria postazione;
3) chiudere la sezione (logout) a fine giornata;
4) spegnere il PC dopo il logout;
5) controllare sempre che non vi siano persone autorizzate alle proprie spalle che possano prendere visione delle schermate del suo computer.

USO DEL PERSONAL COMPUTER

Il sistema informativo aziendale è composto da un server centrale e macchine client connesse ad una rete locale (LAN) che utilizzano i seguenti sistemi operativi Windows 7 PRO ed il gestionale SIGIP. L'antivirus utilizzato è CLAMWIN.
I file creati, elaborati o modificati sul computer dei designati devono essere sempre salvati a fine giornata sul disco esterno al server.
L'ente effettua il Back up dei dati memorizzati sul server ogni giorno salvando i dati su disco fisso separato.

Al designato è vietato:
1) la gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dello stesso designato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa aziendali e negli strumenti informatici aziendali in genere;
2) modificare le configurazioni già impostate sul personal computer;
3) utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Ente;
4) installare alcun software di cui l'Ente non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC consegnato, senza l'espressa autorizzazione dell'organizzazione. Né è peraltro, consentito fare copia del software installato al fine di farne un uso personale;
5) caricare sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
6) aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, o periferiche telecamere, macchine fotografiche, smartphone, chiavi usb, ecc) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Ente;
7) creare o diffondere intenzionalmente o per negligenza programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali ad esempio virus, trojan horses, ecc;
8) accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
9) effettuare in proprio attività manutentive;
10) permettere attività manutentive da parte di soggetti non espressamente autorizzati dall'Ente.

ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, ecc.
L'ente impone su tutte postazioni di lavoro l'utilizzo di sistema antivirus correttamente installato, attivato e aggiornato automaticamente con frequenza quotidiana al riavvio dei computer, individuato in CLAMWIN.
Il designato deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e in particolare deve rispettare le seguenti regole:
1) comunicare all'Ente ogni anomalia o malfunzionamento del sistema antivirus;
2) comunicare all'ente eventuali segnalazioni di presenza di virus o files sospetti;
E' fatto espresso divieto ai designati di:
a) accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
b) ostacolare l'azione dell'antivirus aziendale;
c) disattivare l'antivirus senza l'autorizzazione espressa dell'Ente anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
d) aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi sospetti.
In ogni caso, contattare l'amministratore di sistema prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

INTERNET

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

POSTA ELETTRONICA

L'utilizzo della posta elettronica aziendale è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali non è ammesso. I designati hanno in utilizzo indirizzi nominativi di posta elettronica al quale accedono tramite password personale. La PEC aziendale viene utilizzata dal designato Sig. Marco Chionne il quale detiene le credenziali di accesso.

Gli assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio dell'organizzazione per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'organizzazione, nonché utilizzare il dominio dell'organizzazione per scopi personali.

È vietato redigere messaggi di posta elettronica utilizzando l'indirizzo aziendale, diretti a destinatari esterni dell'organizzazione, senza utilizzare il seguente disclaimer:
"Il presente messaggio e *gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale* e *sono visionabili solo dal destinatario di posta elettronica. La risposta* o *l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare* la *confidenzialità potendo essere viste da altri soggetti appartenenti all'organizzazione oltre al sottoscritto, per finalità di sicurezza informatica, amministrative* e *allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema* e *vi chiediamo di volercene dare cortesemente comunicazione al mittente".*
È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.

È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

Nel caso di assenza prolungata è attivato il servizio di risposta automatica (Auto-reply).

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, il designato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora il designato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica del designato, informandone l'incaricato stesso e redigendo apposito verbale.

DEVICE PERSONALI

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

Ai dipendenti, se espressamente autorizzati dall'ente, è permesso l'utilizzo della posta elettronica aziendale sui loro device personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente per eventuali provvedimenti di sicurezza.

Ai collaboratori è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, ed-rom, DVD, macchine fotografiche, videocamere, tablet, ...).

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri device personali per memorizzare dati dell'ente se espressamente autorizzati dall'ente stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali device dovranno essere preventivamente valutati dall'ente, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

DISTRUZIONE DEI DEVICE

Ogni Device ed ogni memoria esterna affidati agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, ed-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ente che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare l'ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

GESTIONE DATI CARTACEI

Clear Desk Policy

I designati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

I designati sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede Ai Designati di trattare dati cartacei se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'ente.

I principali benefici di una politica della scrivania pulita sono:

1) Una buona impressione a clienti e fornitori che visitano la nostra organizzazione;

2) La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle:

3) La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, ...) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'ente.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.
Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

Stampa dei dati personali:
La stampa dei documenti contenenti dati personali degli interessati avviene unicamente tramite procedura di stampa protetta da password su stampante aziendale.

APPLICAZIONE E CONTROLLO

Il controllo

L'ente, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1.970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

Modalità di verifica

In applicazione del principio di necessità e di minimizzazione dei dati di cui all'art. 5 del GDPR e art.3 del Codice Privacy, l'organizzazione promuove ogni opportuna misura, organizzativa e tecnologica volta a

prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai designati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei designati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da permettere la cancellazione della propria cronologia di navigazione con l'avvertenza che qualora non vi si provveda l'azienda potrà accedervi.

CAPITOLO 8 - Diritto di accesso dell'Interessato

Premessa

Ai sensi degli Artt. 12 e 15 GDPR nonché in base, l'interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso dati personali.

Elettromil srl, ha già fornito attraverso la consegna dell'informativa, comunicazione circa le finalità del trattamento, le categorie dei dati personali in questione, i destinatari, il periodo di conservazione dei dati, nonché l'esistenza del diritto per l'interessato di richiedere la rettifica , la cancellazione o limitazione dei propri dati o di opporsi al loro trattamento, nonché di proporre reclamo.

Modalità di esercizio

Il diritto di accesso può essere esercitato tramite invio di richiesta al Referente, Ing. Daniele Giammetti, senza formalità, tramite mail (privacy@elettromil.it) o oralmente al medesimo.

Il referente, verificata l'identità del richiedente, comunicherà a questi i dati richiesti.
La comunicazione del referente dovrà essere chiara ed intellegibile, la stessa potrà essere anche orale; oppure scritta ove esplicitamente richiesto.

E' consentita la sola esibizione del fascicolo, ove l'estrazione dei dati risultasse difficoltosa.

Limiti alle richieste

L'interessato non potrà richiedere la rettifica ai dati valutativi.

Resta precluso l'accesso ai dati “non definitivi”.

L'accesso è limitato ai soli dati effettivamente detenuti ed oggetto di attuale trattamento.

Non potrà essere esercitato il diritto di accesso per quei dati che sono stati cancellati per esaurimento dello scopo nonché per i dati che siano oggetto di corrispondenza tra dipendenti.

Potrà essere garantito l'accesso solo per quei dati che siano nell'effettiva disponibilità del titolare.

Risposta al dipendente

Il Referente dovrà dare risposta all'interessato, senza giustificato ritardo e comunque entro un mese dalla richiesta, con due mesi di proroga se la risposta è complessa.

In caso di proroga dei tempi della risposta, il Titolare informa il richiedente dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Se il Titolare non ottempera alla richiesta dell'interessato, informa il suddetto, senza ritardo, al più tardi entro un mese dalla richiesta dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'Autorità di controllo o all'Autorità giudiziaria.

Le informazioni vengono fornite dal Titolare gratuitamente. Ove però dovessero risultare manifestatamente infondate o eccessive il Titolare addebiterà un contributo spese ragionevole tenuto conto dei costi amministrativi o potrà rifiutarsi di soddisfare la richiesta dimostrando il carattere infondato o eccessivo della richiesta.

CAPITOLO 9 - Piano formativo

Per un corretto trattamento dei dati è opportuno che il Titolare del trattamento provveda a formare i Referenti e i Designati che si occupano effettivamente della gestione dei dati.
Il Regolamento Europeo richiede infatti che il Manuale Privacy contenga ''*la previsione di interventi formativi dei Designati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire 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 già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali*''.

Piano di formazione

La previsione di interventi di formazione è stata prevista in diversi momenti della vita lavorativa.
E' indispensabile provvedere sia ad una formazione all'atto della nomina, sia ad una formazione continua, orientativamente una volta all'anno e comunque ogni qualvolta ci siano dei cambiamenti rilevanti nella gestione dei rischi, delle misure minime di sicurezza e delle modalità di ripristino dei dati.

PIANO DI FORMAZIONE

TIPOLOGIA DI FORMAZIONE	CLASSI DI INCARICO INTERESSATE	PERIODICITA' DELLA FORMAZIONE	DURATA DELLA FORMAZIONE
Norme e principi giuridici	Referente e Designati	Una volta all'anno	2 ore
Misure di sicurezza	Referente e Designati	Una volta all'anno	2 ore

CAPITOLO 10 Data Breach

L'Articolo 33 del GDPR prevede l'obbligo di notifica di una violazione dei dati personali all'autorità di controllo

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente, a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il Referente del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del Referente quale punto di contatto per il Garante, presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Ai sensi dell'Articolo 34 GDPR, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'Interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui al punto precedente.

Non è richiesta la comunicazione all'interessato, se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una

comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

CAPITOLO 11 - Provvedimenti disciplinari

PROVVEDIMENTI DISCIPLINARI

Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme della presente Policy potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

1. Il biasimo inflitto verbalmente;
2. Lettera di richiamo inflitto per iscritto;
3. Multa
4. La sospensione dalla retribuzione e dal servizio:
5. Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'ente potrà procedere al licenziamento del dirigente autore dell'infrazione.

VALIDITA' AGGIORNAMENTO AFFISSIONE

Validità

Il presente Disciplinare ha validità a partire da: 18/12/2018.

Aggiornamento

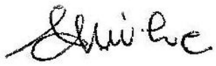
La presente Policy sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative.

Ogni variazione della presente Policy sarà comunicata ai Designati ed al Referente.

Affissione

Il presente Disciplinare verrà affisso nella bacheca aziendale ai sensi della legge 300/70 e del CCNL.

Castiglione del Lago, 18/12/2018 **Firma del Titolare**



In data odierna il presente documento è stato consegnato a Daniele Giammetti, Marco Chionne, Yuri Bosetti, Emanuele Paolucci, che dichiarano di averlo ricevuto e di averne preso visione.

Firme