

**ENCO**  
ENGINEERING  
CONSULTANTS

---

REGOLAMENTO GENERALE  
PER LA PROTEZIONE DEI DATI IN  
AZIENDA

V.01 –MAGGIO 2018

---

ENCO Engineering Consultants Srl

Via Feltre 183

32036 Sedico (BL) Italy

Tel +39 0437 852727 - Fax +39 0437 852717

IVA (VAT / TVA) 00607990256

<http://www.enco.energy>

## Sommario

<b>1. CLASSIFICAZIONE E CONTESTO DEL TRATTAMENTO DEI DATI PERSONALI</b> .....	<b>3</b>
1.1. PANORAMICA DEL TRATTAMENTO DATI PERSONALI.....	3
1.1.1. CONTESTO, SCOPO E FINALITA'.....	4
1.1.2. RUOLI E RESPONSABILITA' LEGATE AL TRATTAMENTO.....	5
1.1.3. STANDARD APPLICABILI AL TRATTAMENTO.....	7
1.1.3.1. Informativa e "Consenso Informato".....	7
1.1.3.2. Standard per le procedure informatizzate.....	8
1.2. DATI, PROCESSI E RISORSE.....	11
1.2.1. CATEGORIE INTERESSATE E TIPO DI DATI TRATTATI.....	11
1.2.1.1. Clienti.....	11
1.2.1.2. Fornitori.....	11
1.2.1.3. Collaboratori Esterni.....	12
1.2.1.4. Collaboratori Interni.....	16
1.2.1.5. Dipendenti e Titolari.....	17
1.2.1.6. Utenti del Sito Internet.....	19
1.2.2. PROCEDURA DI ARCHIVIAZIONE E CONSERVAZIONE DEI DATI.....	20
1.2.2.1. Formato Cartaceo.....	20
1.2.2.2. Formato Elettronico.....	21
1.2.3. CICLO DI VITA DEL TRATTAMENTO DEI DATI.....	24
1.2.3.1. Fase 1 – La raccolta del dato.....	24
1.2.3.2. Fase 2 – Archiviazione e protezione.....	24
1.2.3.3. Fase 3 – Accesso ed utilizzo.....	24
1.2.3.4. Fase 4 – Cancellazione e distruzione dei dati.....	25
1.2.4. RISORSE DI SUPPORTO AI DATI PERSONALI.....	26
<b>2. PRINCIPI FONDAMENTALI</b> .....	<b>27</b>
2.1. NECESSITA' E PROPORZIONALITA'.....	27
2.1.1. CARATTERISTICHE DEGLI SCOPI DEL TRATTAMENTO.....	27
2.2. ALTRI PRINCIPI E BASI LEGALI.....	28
2.2.1. PRINCIPI DI LICEITA', CORRETTEZZA E TRASPARENZA.....	28
2.2.2. PRINCIPI DI LIMITAZIONE E MINIMIZZAZIONE DEI DATI.....	29
2.2.3. PRINCIPI DI INTERGRITA' E RISERVATEZZA.....	29
2.2.4. PRINCIPI DI ACCURATEZZA, AGGIORNAMENTO E CONSERVAZIONE DEI DATI.....	29
2.3. DIRITTI PERSONALI DEI SOGGETTI INTERESSATI.....	30
2.3.1. INFORMAZIONE E CONSENSO DEI SOGGETTI INTERESSATI.....	30
2.3.2. DIRITTI DI ACCESSO E PORTABILITA'.....	31
2.3.3. DIRITTI DI RETTIFICA, CANCELLAZIONE ED OBLIO.....	33
2.3.4. DIRITTI DI RESTRIZIONE ED OBIEZIONE.....	34
2.3.5. TRASFERIMENTO DI DATI FUORI DALL'UNIONE EUROPEA.....	35

<b>3. RISCHI.....</b>	<b>36</b>
3.1. VALUTAZIONE DEL RISCHIO E DELL'IMPATTO .....	36
3.2. CONTROLLI GENERALI GIA' ESISTENTI O PIANIFICATI.....	37
3.2.1. STRATEGIE GENERALI APPLICATE PRIMA E DURANTE IL TRATTAMENTO.....	37
3.2.1.1. Minimizzazione quantità dei dati raccolti .....	37
3.2.2. PROTEZIONE DATI SU SUPPORTO INFORMATICO .....	37
3.2.2.1. Controllo degli accessi.....	37
3.2.2.2. Archiviazione su server e su database .....	39
3.2.2.3. Vulnerabilità del dato e lotta contro malware e virus .....	39
3.2.2.4. Sicurezza siti web, backup e manutenzione.....	40
3.2.2.5. Organizzazione.....	41
3.2.2.6. Politiche.....	41
3.3. MINACCE E RISCHIO NEL TRATTAMENTO DEI DATI PERSONALI.....	42
3.3.1. VALUTAZIONE DELLE PRINCIPALI MINACCE E DELLE FONTI DI RISCHIO.....	42
3.3.1.1. Definizione e tipi di minacce.....	42
3.3.1.2. Cause e fonti di rischio .....	42
3.3.2. STIMA DELLA GRAVITA' E DELLA PROBABILITA' DEL RISCHIO.....	43
3.3.2.1. Valutazione di probabilità e livello di rischio .....	43
3.3.2.2. Valutazione del rischio e dell'impatto.....	43
3.3.2.3. Classificazione delle minacce in base al rischio .....	43
3.3.3. DATA BREACH E NOTIFICA DELLA VIOLAZIONE.....	44
3.3.4. INFORMATIVE.....	45
3.3.4.1. Informativa clienti, fornitori e collaboratori.....	46
3.3.4.2. Informativa dipendenti .....	50

## Indice delle Figure

Figura 1 - Figure responsabili del trattamento .....	6
Figura 2 - Sistema di autorizzazione Incaricati.....	9
Figura 3 - Misure di sicurezza informatiche per Incaricati.....	10
Figura 4 - Autorizzazioni Sistema Informatico .....	21
Figura 5 - Fasi del ciclo di vita del trattamento.....	25
Figura 6 - Diagramma di valutazione del grado di rischio .....	36
Figura 7 - Tabella di classificazione minacce.....	44

# 1. CLASSIFICAZIONE E CONTESTO DEL TRATTAMENTO DEI DATI PERSONALI

Le tipologie di dato personale definite dalla normativa di riferimento, ed in particolare dall'art. 4, c. 1, lett. b e seguenti del del D.Lgs. 196/2003, sono le seguenti:

- **Dato personale (comune)**

Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- **Dati identificativi**

Dati personali che permettono l'identificazione diretta dell'interessato;

- **Dati sensibili**

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 personali idonei a rivelare lo stato di salute e la vita sessuale;

- **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 d 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.

## 1.1. PANORAMICA DEL TRATTAMENTO DATI PERSONALI

ENCO Engineering Consultants Srl, da qui in avanti identificata come "ENCO", è una società di ingegneria che si occupa di progettazione di opere civili, industriali e, principalmente negli ultimi anni, di centraline idroelettriche.

Opera sia nel territorio nazionale italiano che all'estero fin dalla sua fondazione, avvenuta nel 1983. L'azienda oltre a portare avanti la propria attività professionale secondo i canali tradizionali, è anche titolare di un sito internet, [www.enco.energy](http://www.enco.energy), dove è possibile contattare lo studio per richiedere informazioni sui servizi forniti.

ENCO esercita la propria attività nel rispetto dei principi e delle norme di comportamento indicati nel Codice Etico della società e nell'osservanza delle vigenti normative italiane e comunitarie.

Si avvale, al proprio interno, di un sistema di gestione della qualità certificato ISO 9001 e di un processo di controllo dell'impatto ambientale, anch'esso certificato secondo la normativa ISO 14001

ENCO, nell'esercizio della propria attività, considera di massima importanza l'assunzione di responsabilità etico-sociale e, a tal fine, si impegna affinché la gestione della società si muova nel rispetto degli interessi di tutti i soggetti coinvolti in modo diretto e/o indiretto: soci, amministratori, dipendenti, collaboratori interni ed esterni, clienti e fornitori e della società in cui opera.

Il trattamento dei dati personali che vengono raccolti ai fini dell'esercizio dell'attività di impresa o volontariamente trasmessi dall'utente nel caso del sito internet, avviene sempre secondo il rispetto delle linee guida aziendali sopra esposte.

ENCO

Le modalità, le finalità, gli standard ed i processi relativi al trattamento dei dati personali verranno analizzati maggiormente nel dettaglio nei capitoli successivi.

### 1.1.1. CONTESTO, SCOPO E FINALITA'

ENCO recepisce e mette in atto le prescrizioni del **Regolamento UE 2016/679 del 27 Aprile 2016** entrato in vigore il 25 maggio 2018, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati in tutti i rapporti interni ed esterni, con collaboratori, clienti, fornitori e dipendenti.

I dati personali saranno raccolti, conservati e trattati con **modalità elettroniche, informatiche e/o cartacee**, saranno **esclusivamente utilizzati per gli scopi previsti dai contratti che regolano il rapporto di ENCO con ciascun soggetto coinvolto** nella gestione dell'attività di impresa e trattati sempre con strumenti idonei a garantire un **adeguato livello di sicurezza** degli stessi.

Il Titolare del trattamento si impegna quindi ad acquisire solamente i dati necessari alla gestione dei suddetti rapporti, con particolare riferimento all'adempimento dei relativi obblighi di natura legale/contrattuale/professionale.

A questo proposito possiamo, a titolo esemplificativo, elencare alcune delle situazioni più frequenti in cui si presenti la necessità di un trattamento: esigenze preliminari alla stipula di contratti legati alla fornitura agli interessati di prodotti/servizi, per dare esecuzione agli stessi e per la tutela delle posizioni creditorie da essi derivanti; per le normali esigenze interne di tipo operativo, gestionale e contabile; per effettuare le necessarie comunicazioni; per adempiere a qualunque tipo di obbligo previsto da leggi o regolamenti vigenti, in particolare, in materia fiscale, per rispondere ad eventuali richieste di informazioni o candidature professionali.

Il trattamento dei dati avviene sempre presso la sede del Titolare:

ENCO Engineering Consultants Srl  
Via Feltre 183  
32032 Sedico (BL)  
Italia

## 1.1.2. RUOLI E RESPONSABILITA' LEGATE AL TRATTAMENTO

Nell'ambito di uno studio di ingegneria le figure soggettive fondamentali connesse alla protezione dei dati personali sono: il già menzionato Titolare del trattamento, il responsabile, l'incaricato e l'interessato.

Di seguito un breve riepilogo delle funzioni esercitate da ciascun soggetto ed una tabella riassuntiva di come questi ruoli sono stati assegnati nell'organizzazione aziendale di ENCO Engineering Consultants S.r.l.

- **TITOLARE DEL TRATTAMENTO**

È il soggetto che esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento, compreso il profilo della sicurezza (art. 28 del Codice).

L'Articolo 24 del Regolamento stabilisce la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare deve essere in grado di dimostrare la **conformità delle attività di trattamento** con il Regolamento stesso e deve mettere in atto misure adeguate ed efficaci a garanzia di ciò.

- **RESPONSABILE DEL TRATTAMENTO**

Si tratta di una persona fisica o giuridica che viene designata dal titolare del trattamento, predisposta a verificare i corretti adempimenti di legge (art.29 del Codice). ENCO non lo ha, per il momento nominato, ne fa le veci una figura interna all'azienda.

- **INCARICATO DEL TRATTAMENTO**

Chiunque compia operazioni di trattamento (art.30 del Codice). Può esclusivamente essere una persona fisica e nelle operazioni di trattamento è tenuto all'adozione di idonee misure di custodia e di controllo e qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita dei dati stessi, nonché i rischi di accesso non autorizzato o trattamento non consentito.

- **INTERESSATO AL TRATTAMENTO**

È la persona fisica cui si riferiscono i dati. In quanto proprietario dei dati personali esso gode di alcuni particolari diritti previsti dalla normativa ed esaminati nei successivi capitoli dedicati.

- **AMMINISTRATORE DI SISTEMA**

Non è una figura prevista dal codice ma l'abbiamo inserita in quanto, nel caso di ENCO, è esterna alla società che però, gestendo il sistema informatico dell'ufficio, può avere accesso a dati personali relativi a soggetti che interagiscono con l'azienda.

ENCO Engineering Consultants Srl <b>FIGURE RESPONSABILI DEL TRATTAMENTO DATI PERSONALI</b>	
TITOLARE DEL TRATTAMENTO	ENCO Engineering Consultants S.r.l. Rappresentante Legale: Ing. Michele Reolon Amministratore: Ing. Eugenio De Demo
RESPONSABILE DEL TRATTAMENTO	Non Nominato / Sig.ra Chiara Durante
INCARICATO/I DEL TRATTAMENTO	Sig.ra Chiara Durante Sig.ra Francesca Portolan
AMMINISTRATORE DI SISTEMA	Sig. Alessandro De Zorzi

Figura 1 - Figure responsabili del trattamento

## 1.1.3. STANDARD APPLICABILI AL TRATTAMENTO

ENCO si impegna a sviluppare nuovi standard e procedure di trattamento dei dati personali che siano conformi al Regolamento Europeo **Regolamento UE 2016/679 del 27 Aprile 2016** e, applicando il principio di “accountability” (o “responsabilizzazione”) introdotto dal suddetto documento vuole responsabilizzare, attraverso la diffusione delle informazioni e la formazione dei dipendenti, coloro i quali all’interno dell’azienda possono trovarsi nella condizione di dover effettuare un trattamento di dati personali.

### 1.1.3.1. Informativa e “Consenso Informato”

La procedura standard che coinvolge tutti gli interessati al trattamento dei dati, prevede la firma di una informativa scritta che è stata adeguata alla versione del regolamento entrata in vigore il 25 maggio 2018.

Lo scopo di questa informativa è dare la possibilità a tutti i soggetti interessati al trattamento di fornire un “consenso informato”.

La firma di questo documento non esclude comunque la possibilità di poter richiedere, in caso di dubbi di qualsiasi natura, maggiori informazioni ai responsabili del trattamento dati personali dell’azienda i quali potranno fornire ulteriori chiarificazioni anche oralmente e non necessariamente per iscritto.

L’informativa è indirizzata a qualsiasi soggetto interessato al trattamento, è dunque prevista per clienti, fornitori, collaboratori esterni e dipendenti.

Anche gli utenti che compilano il form presente sul sito [www.enco.energy](http://www.enco.energy) sono tenuti a confermare la lettura e la comprensione dell’informativa sul trattamento dei dati personali.

L’informativa è strutturata secondo le direttive imposte dal Codice e pertanto include le seguenti informazioni:

- le finalità del trattamento;
- le modalità del trattamento (strumenti elettronici o manuali, modalità di organizzazione o di raffronto ed elaborazione particolari, creazione di profili per età, professione o altro);
- se il conferimento dei dati richiesti è obbligatorio o facoltativo relativamente agli scopi dichiarati;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- se i dati possono essere ceduti a terzi, in tal caso identificandoli o quanto meno individuando le categorie dei soggetti destinatari;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l’ambito di diffusione dei dati medesimi;
- i diritti di cui all’articolo 7 del Codice;
- i dati identificativi del titolare del trattamento;
- i dati identificativi del responsabile del trattamento.



### **1.1.3.2. Standard per le procedure informatizzate**

I dati informatizzati riguardanti i dipendenti (password di accesso ai pc, password di accesso al database ENCO, etc...) sono private.

L'amministratore di sistema assegna una password di default al momento della creazione di ciascun account. Queste password, sia quelle delle email che quelle di accesso alle postazioni, possono venire poi modificate a piacimento dall'utente e rimangono private.

Esso ha la possibilità di utilizzarle previa autorizzazione del soggetto interessato e/o in sua presenza o in caso di necessità per risolvere problemi di natura tecnica.

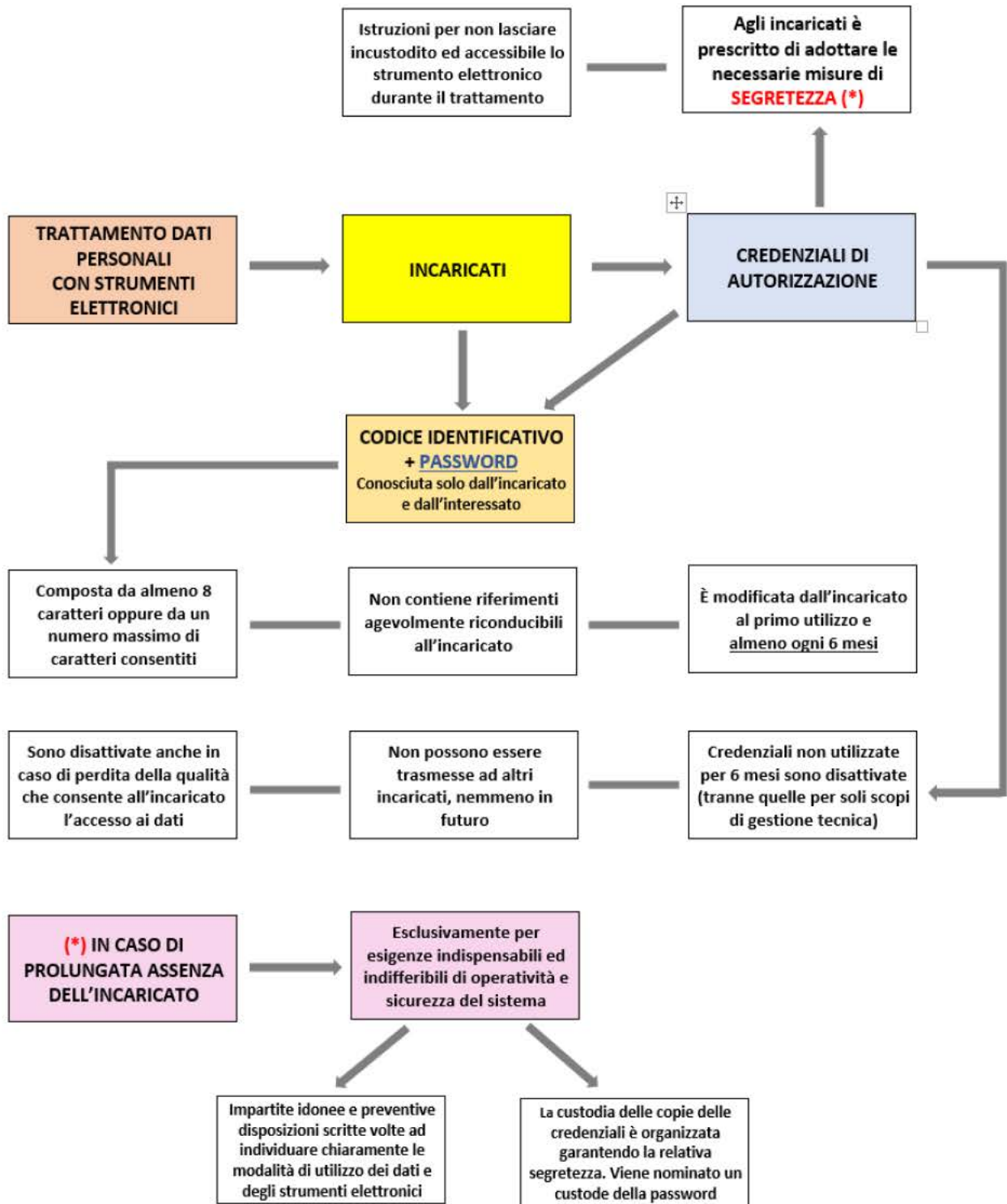


Figura 2 - Sistema di autorizzazione Incaricati

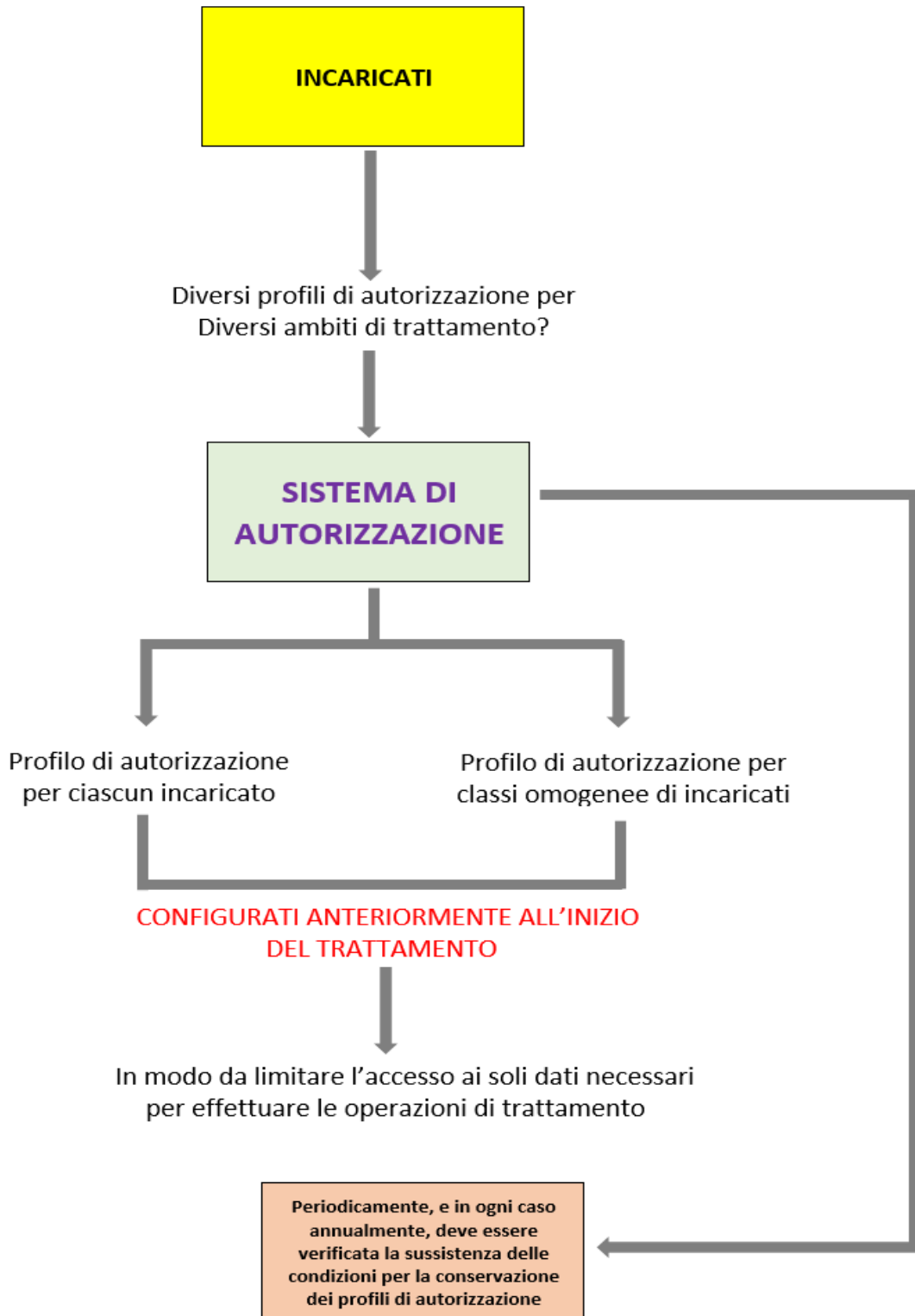


Figura 3 - Misure di sicurezza informatiche per Incaricati

## **1.2. DATI, PROCESSI E RISORSE**

### **1.2.1. CATEGORIE INTERESSATE E TIPO DI DATI TRATTATI**

#### **1.2.1.1. Clienti**

##### **a) TIPOLOGIA DI DATI TRATTATI**

Tutti i dati necessari nell'ambito del rapporto con il cliente (recapiti telefonici, email etc.) e per adempiere ai fini amministrativi nell'esercizio dell'attività di impresa.

Dati personali ed identificativi relativi alla persona fisica o giuridica (nome e cognome/ ragione sociale, indirizzo) e indispensabili a fini fiscali per la procedura di fatturazione (partita iva).

Questi dati si ritrovano anche nel contratto che regola la prestazione di servizi, nella documentazione prodotta durante lo svolgimento dell'incarico e nella corrispondenza.

Si tratta di dati indispensabili per poter effettuare una fornitura di servizi, per tanto il consenso al trattamento nelle finalità limitate allo svolgimento dell'incarico è una condizione sine qua non per effettuare la prestazione. Alcuni dati anagrafici e relativi alle commesse (ragione sociale etc.) sono registrati e conservati anche nel database online.

##### **b) AMBITO E FINALITÀ DEL TRATTAMENTO**

I dati sono utilizzati limitatamente ai termini del contratto stipulato e al fine di portare a termine la prestazione dei servizi. Essi non possono essere trasmessi a terzi senza consenso e al di fuori delle finalità previste.

##### **c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI**

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo.

I documenti rilevanti ai fini fiscali, come le fatture, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del cliente, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta.

La corrispondenza online viene conservata per tutto il periodo della durata della collaborazione. La casella email è personale del singolo dipendente pertanto l'accesso ai dati contenuti nella corrispondenza è limitato all'operatore interessato.

Per comunicazione di carattere riservato si predilige l'utilizzo della posta certificata PEC.

#### **1.2.1.2. Fornitori**

##### **a) TIPOLOGIA DI DATI TRATTATI**

Il trattamento dei dati nell'ambito dell'attività d'impresa e dei rapporti con i fornitori interessa dati personali ed identificativi necessari per adempiere ai fini amministrativi indispensabili per l'esercizio dell'attività di impresa.

Anche qui sono inclusi i riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica/giuridica (nome e cognome/ ragione sociale, indirizzo), indispensabili a fini fiscali per la procedura di fatturazione (partita iva), dati bancari per l'effettuazione dei pagamenti.

Questi dati sono presenti nei documenti amministrativi (fatture ricevute), nel contratto che regola i rapporti di fornitura e nella corrispondenza.

#### b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati sono utilizzati limitatamente ai termini del contratto stipulato e al fine di ricevere la prestazione dei servizi o la fornitura come da accordi. Essi non possono essere trasmessi a terzi senza consenso e al di fuori delle finalità previste, siano esse amministrative o relative all'incarico.

#### c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo. Alcuni dati anagrafici e relativi alle commesse (ragione sociale etc.) sono registrati e conservati anche nel database online.

I documenti rilevanti ai fini fiscali, come le fatture, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del fornitore, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta.

I contratti di fornitura in essere (forniture cancelleria, macchine da ufficio, energia elettrica etc.) sono conservati per tutta la durata del contratto, anch'essi sia in forma cartacea che elettronica.

La corrispondenza online viene conservata per tutto il periodo della durata della collaborazione. La casella email è personale del singolo dipendente pertanto l'accesso ai dati contenuti nella corrispondenza è limitato all'operatore interessato.

Per comunicazione di carattere riservato si predilige l'utilizzo della posta certificata PEC.

### **1.2.1.3. Collaboratori Esterni**

ENCO si avvale frequentemente della collaborazione di professionisti esterni, sia italiani che internazionali. Tale collaborazione avviene secondo diverse modalità: si può trattare di un'esternalizzazione da parte dell'azienda di alcuni servizi (come, ad esempio, l'affidamento ad un ingegnere esterno dei calcoli strutturali per un progetto), di una collaborazione per la partecipazione ad una gara d'appalto (spesso nelle gare internazionali viene richiesta la disponibilità di un team di esperti, da cui la necessità di collaborare con figure professionali esterne), di una vera e propria partecipazione continuativa nell'ambito di una singola commessa (ad esempio quando si presenti la necessità di assumere un ingegnere esterno per seguire la direzione lavori in cantiere).

È evidente che in tutti i casi elencati si presenta la necessità di regolamentare il trattamento dei dati personali, identificarne la finalità e le modalità di conservazione.

- **ESTERNALIZZAZIONE DI UN SERVIZIO**

- a) TIPOLOGIA DI DATI TRATTATI

Si tratta di un tipo di collaborazione regolata da un contratto che prevede l'emissione di una fattura per i servizi prestati, di conseguenza i dati trattati, come per clienti e fornitori, rientreranno nelle categorie dei dati personali ed identificativi.

Sono inclusi i riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica/giuridica (nome e cognome/ ragione sociale, indirizzo), indispensabili a fini fiscali per la procedura di fatturazione (partita iva), dati bancari per l'effettuazione dei pagamenti.

Questi dati sono presenti nei documenti amministrativi (fatture ricevute), e nel contratto che regola i rapporti di collaborazione e nella corrispondenza.

In questo caso tra i dati rilevanti ai fini fiscali è bene elencare anche quanto contenuto nella certificazione unica annuale. Quest'ultima non viene compilata da ENCO, ma da un'azienda esterna che cura la consulenza per il lavoro; ciò nonostante ENCO viene a contatto con questi dati nel momento della consultazione del documento e della consegna dello stesso all'interessato.

- b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati sono utilizzati limitatamente ai termini del contratto stipulato, al fine di portare a termine la prestazione di servizi ed espletare le necessarie pratiche amministrative. Essi non possono essere trasmessi a terzi senza consenso e al di fuori delle finalità previste.

- c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo.

I documenti rilevanti ai fini fiscali, come le fatture, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del collaboratore, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta.

Alcuni dati anagrafici sono registrati e conservati anche nel database online.

La corrispondenza online viene conservata per tutto il periodo della durata della collaborazione. La casella email è personale del singolo dipendente pertanto l'accesso ai dati contenuti nella corrispondenza è limitato all'operatore interessato.

Per comunicazione di carattere riservato si predilige l'utilizzo della posta certificata PEC.

- **COLLABORAZIONE NELL'AMBITO DI UNA GARA D'APPALTO**

- a) TIPOLOGIA DI DATI TRATTATI

Al momento della partecipazione ad una gara d'appalto viene spesso richiesto di proporre un team di esperti che si renderà disponibile alla realizzazione dell'incarico oggetto di gara. In questa fase preliminare non viene stipulato nessun contratto ma è necessario che il collaboratore fornisca il proprio Curriculum Vitae e ne autorizzi la trasmissione a terzi (in questo caso la commissione giudicante che ha indetto la gara).

Il CV contiene dati identificativi e personali, include riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica/giuridica (nome e cognome etc.) e ulteriori informazioni su passate esperienze scolastiche e lavorative.

Questi dati sono presenti non solo nel CV, ma, alcuni, anche nella corrispondenza ed in altre sezioni dei documenti di gara.

Per far sì che l'autorizzazione al trattamento e al trasferimento a terzi di questi dati sia trasparente al massimo il soggetto titolare del CV è tenuto a firmare una liberatoria al trattamento ed al trasferimento dei dati che è posta in calce al documento stesso.

In aggiunta alla presentazione del CV può essere necessario dover allegare ulteriori documenti contenenti dati personali, come copie del diploma di laurea o certificati di appartenenza ad ordini professionali (sempre a seguito di autorizzazione da parte dell'interessato).

- b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati sono utilizzati limitatamente alla finalità di partecipazione alla gara. Nel caso di possibilità di ulteriori collaborazioni o richiesta dell'interessato il CV nello specifico può essere trasmesso a terzi non collegati alla specifica partecipazione, previa autorizzazione.

Non è possibile fare lo stesso con copie di documenti quali i sopra citati documenti di laurea o certificati di iscrizione agli ordini professionali la cui trasmissione ed utilizzo al di fuori delle finalità esplicitate nel bando di gara non è ammessa.

Le gare d'appalto spesso si svolgono all'estero, oltre i confini dell'Unione Europea. Le modalità del trasferimento dati verso stati extra UE e le problematiche che questo comporta saranno meglio esaminate nel capitolo 2.2.6.

- c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo. Essendo la partecipazione di una gara equiparabile, dal punto di vista dell'archiviazione di ENCO, all'apertura di una commessa, tutti i dati relativi ai collaboratori vengono conservati fino all'esito della gara medesima.

I Curriculum Vitae, anch'essi conservati in forma elettronica o cartacea, sono archiviati in vista di possibili future collaborazioni finché non risultino superati.

Alcuni dati anagrafici sono registrati e conservati anche nel database online.

La corrispondenza online viene conservata per il periodo necessario alla partecipazione alla gara. La casella email è personale del singolo dipendente pertanto l'accesso ai dati contenuti nella corrispondenza è limitato all'operatore interessato.

Se necessario perché richiesto dai termini di gara, si ricorre all'utilizzo della posta certificata PEC.

- **PARTECIPAZIONE CONTINUATIVA NELL'AMBITO DI UNA COMMESSA**

- a) TIPOLOGIA DI DATI TRATTATI

Si tratta di un tipo di collaborazione regolata da un contratto che prevede l'emissione di una fattura per i servizi prestati, di conseguenza i dati trattati, come per clienti e fornitori, rientreranno nelle categorie dei dati personali ed identificativi.

Sono inclusi i riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica/giuridica (nome e cognome/ ragione sociale, indirizzo), indispensabili a fini fiscali per la procedura di fatturazione (partita iva), dati bancari per l'effettuazione dei pagamenti.

Questi dati sono presenti nei documenti amministrativi (fatture ricevute), nel contratto che regola i rapporti di collaborazione, nella corrispondenza e in alcuni documenti prodotti durante lo svolgimento dei servizi, come la In questo caso tra i dati rilevanti ai fini fiscali è bene elencare anche quanto contenuto nella certificazione unica annuale. Quest'ultima non viene compilata da ENCO, ma da un'azienda esterna che cura la consulenza per il lavoro; ciò nonostante ENCO viene a contatto con questi dati nel momento della consultazione del documento e della consegna dello stesso all'interessato.

Spesso questo tipo di collaborazione viene messa in atto anche con professionisti stranieri per i quali viene meno la necessità della CU ma per i quali si devono tenere in considerazione le modalità del trasferimento dati verso stati fuori dall'Unione Europea. Per quanto invece riguarda i collaboratori italiani che rientrano in questa categoria e per i quali viene emessa la certificazione unica, si rimanda a quanto già specificato al primo punto di questo elenco (esternalizzazione di un servizio).

- b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati sono utilizzati limitatamente ai termini del contratto stipulato, al fine di portare a termine la prestazione di servizi e espletare le necessarie pratiche amministrative. Essi non possono essere trasmessi a terzi senza consenso e al di fuori delle finalità previste.

- c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo. Alcuni dati anagrafici sono registrati e conservati anche nel database online.

I documenti rilevanti ai fini fiscali, come le fatture, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del collaboratore, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta.

La corrispondenza online viene conservata per tutto il periodo della durata della collaborazione. La casella email è personale del singolo dipendente pertanto l'accesso ai dati contenuti nella corrispondenza è limitato all'operatore interessato.

Per comunicazione di carattere riservato si predilige l'utilizzo della posta certificata PEC.



## 1.2.1.4. Collaboratori Interni

### a) TIPOLOGIA DI DATI TRATTATI

Il rapporto con questa categoria è solitamente regolato da un contratto che prevede l'emissione di una fattura mensile per le prestazioni effettuate.

I collaboratori interni hanno con ENCO una collaborazione continuativa e svolgono la professione all'interno dei locali dello studio utilizzando strumenti informatici forniti da ENCO.

Per questa ragione essi dispongono di una personale password di accesso alla rete informatica ed internet dell'ufficio, di accesso al server e dispongono di autorizzazioni specifiche.

I dati interessati al trattamento per questa categoria sono quelli personali ed identificativi, inclusi i riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica/giuridica (nome e cognome/ ragione sociale, indirizzo), indispensabili a fini fiscali per la procedura di fatturazione (partita iva), dati bancari per l'effettuazione dei pagamenti.

Tra i dati necessari ai fini fiscali, anche in questo caso annoveriamo quanto contenuto nella certificazione unica annuale. Quest'ultima non viene compilata da ENCO, ma da un'azienda esterna che cura la consulenza per il lavoro; ciò nonostante ENCO viene a contatto con questi dati nel momento della consultazione del documento e della consegna dello stesso all'interessato.

In aggiunta avremo poi tutti i dati informatizzati per l'accesso ai sistemi informatici, che verranno gestiti come da Figura 3.

Altri dati possono essere contenuti nella corrispondenza, considerato che i collaboratori interni utilizzano caselle email sul dominio di ENCO e utilizzano strumenti informatici dell'azienda.

### b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati sono utilizzati limitatamente ai termini del contratto stipulato e, di volta in volta, alla singola commessa. Vengono trattati per le finalità amministrative indispensabili e non possono essere trasmessi a terzi senza consenso. Nello specifico le CU vengono consegnate personalmente al diretto interessato per mano dell'incarico, in modo che venga rispettato il vincolo di riservatezza.

I dati di accesso al sistema informatico sono strettamente personali ed utilizzati solo negli ambiti previsti dall'attività di ufficio e trattati come da Figura 3.

La corrispondenza rimane privata e non consultabile senza autorizzazione. Viene cancellata al termine del contratto di collaborazione.

La password di accesso alla mail viene assegnata dall'amministratore di sistema al momento di creazione della casella di posta ma può venire modificata dal singolo utente e mantenuta riservata.

Una copia della password può essere conservata per casi di emergenza come descritto in Figura 2.

La gestione della casella PEC, obbligatoria per molte figure professionali, è totalmente in capo all'interessato in quanto personale. Egli si curerà di rispettare i vincoli di riservatezza e mettere in atto le misure necessarie per non causare dispersione di dati.

## c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo.

I documenti rilevanti ai fini fiscali, come le fatture, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del collaboratore, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta. Alcuni dati, tra cui le ore di lavoro di ciascun collaboratore per ciascuna commessa e quelli anagrafici sono registrati e conservati anche nel database online.

I dati di accesso al sistema informatico sono invece conservati, per garantirne la segretezza, dall'interessato. In caso di sua assenza vengono seguite le procedure come da Figura 3.

### 1.2.1.5. Dipendenti e Titolari

#### a) TIPOLOGIA DI DATI TRATTATI

Per il trattamento dei dati relativi ai dipendenti diventa fondamentale la figura dell'incaricato, il/la quale ha la possibilità di garantire che il vincolo di riservatezza sia sempre rispettato e che non vi sia una diffusione impropria di informazioni.

All'interno della gestione dei dipendenti nell'ufficio i dati con cui si viene a contatto sono molteplici: personali, identificativi ma, in questo caso anche sensibili e giudiziari.

I dati sensibili, come quelli relativi alle visite mediche obbligatorie che possono fornire informazioni sullo stato di salute degli interessati, sono trattati da un ente esterno (nel caso di ENCO trattasi di Confartigianato, con sede a Belluno in Piazza della Resistenza, 8 ) ma vengono comunque trasmessi all'incaricato dell'ufficio per l'archiviazione e la gestione delle comunicazioni/consegne ai dipendenti interessati e che quindi entra in contatto con questa categoria di informazioni.

Nel caso della presentazione di certificato medico per malattia, il dipendente è tenuto a comunicare al datore di lavoro esclusivamente il codice di controllo INPS, in modo da limitare il trattamento di un dato che, potendo rilevare condizioni di salute dell'interessato, rientrerebbe nella categoria dei dati sensibili.

Rientrano nella stessa categoria anche alcuni dati contenuti nelle buste paga. Anche in questo caso il trattamento è primariamente affidato ad una azienda esterna, Feinar Srl (con sede in Via Rossa, 101 – Belluno), che si occupa per ENCO della consulenza sul lavoro. Come già accade per i documenti relativi alla medicina del lavoro anche questi vengono trasmessi all'incaricato dell'ufficio che si fa carico della trasmissione dei documenti e delle informazioni ai diretti interessati garantendo il rispetto dei vincoli di riservatezza. Questo tipo di dati sono oggetto di trattamento solo quando riguardano i dipendenti. Feinar si farà inoltre cura di non riportare in busta paga diciture particolari che possono essere rivelatrici di aspetti relativi a peculiari rapporti familiari o sigle sindacali, utilizzando diciture meno esplicite.

I dati giudiziari non sono oggetto di trattamento frequente, ma occasionalmente l'incaricato può entrare in contatto con questo tipo di informazioni, in particolar modo se riferite ai titolari. Un esempio in cui questa situazione si può verificare è la partecipazione ad una gara d'appalto che richieda la presentazione di un certificato del casellario giudiziale o dei carichi pendenti relativo ad uno o entrambi i dirigenti aziendali.

Rimangono oggetto di trattamento i dati personali ed identificativi: riferimenti anagrafici (recapiti telefonici, email etc.), tutti i dati relativi alla persona fisica (nome e cognome/indirizzo), tutti i dati necessari per fini amministrativi (codice fiscale etc.), dati relativi a contratti ed orari di lavoro. Questo tipo di dati sono oggetto di trattamento sia quando riguardano i dipendenti che quando riguardano i titolari.

Sia dipendenti che titolari hanno a disposizione password di accesso alla rete internet ed alla rete informatica aziendale, seppur con diversi livelli di autorizzazione. Username e password per l'accesso al server, alle email o ai pc sono personali e conservate secondo le direttive di Figura 3.

Altri dati relativi ai titolari che sono necessari per l'adempimento di pratiche amministrative possono essere trattati, previo consenso, dall'incaricato.

Altri dati possono essere contenuti nella corrispondenza, considerato che i dipendenti utilizzano caselle email sul dominio di ENCO e utilizzano strumenti informatici dell'azienda.

Le caselle PEC dei titolari sono gestite personalmente dagli interessati che ne conservano le credenziali d'accesso e ne gestiscono l'archiviazione.

## b) AMBITO E FINALITA' DEL TRATTAMENTO

I dati relativi ai dipendenti ed ai titolari sono utilizzati limitatamente ai termini del contratto, al fine garantire lo svolgimento del lavoro e l'adempimento di tutti i tipi di pratiche. Essi non possono essere trasmessi a terzi senza consenso e al di fuori delle finalità previste.

La corrispondenza rimane privata e non consultabile senza autorizzazione. Viene cancellata al termine del contratto. La password di accesso alla mail viene assegnata dall'amministratore di sistema al momento di creazione della casella di posta ma può venire modificata dal singolo utente e mantenuta riservata. Una copia della password può essere conservata per casi di emergenza come descritto in Figura 2.

## c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

I dati vengono archiviati sia in forma cartacea che informatica, secondo gli schemi al capitolo successivo. Alcuni dati, tra cui le ore di lavoro di ciascun dipendente per ciascuna commessa e quelli anagrafici sono registrati e conservati anche nel database online.

I documenti rilevanti ai fini fiscali, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973 sia nell'archivio elettronico che in quello cartaceo. Quelli relativi ai dipendenti (CU, copie delle buste paga etc.) sono conservati per la durata del contratto.

Le pratiche relative alla singola commessa, le quali spesso contengono a propria volta informazioni su dati identificativi e personali del dipendente o del titolare, vengono conservate per un periodo intorno ai 15 anni sia su supporto informatico che su carta.

I dati di accesso al sistema informatico sono conservati dall'interessato. In caso di sua assenza vengono seguite le procedure come da Figura 3.

I documenti relativi ai dati sensibili e giudiziari vengono conservati per il tempo necessario (durata del contratto oppure scadenza della validità del documento, nel caso delle certificazioni) sia su supporto informatico che cartaceo.

La consultazione dell'archivio cartaceo è limitata all'incaricato, la consultazione dell'archivio informatico è regolata alle autorizzazioni stabilite dall'amministratore di sistema ed è limitata all'incaricato ed ai titolari.

#### **1.2.1.6. Utenti del Sito Internet**

La normativa di riferimento per quanto concerne la gestione della privacy di un sito internet è il Decreto Legislativo n° 196 – 30/06/2003, con particolare attenzione all'art. 13 (informativa), art.17 (trattamento che presenta rischi specifici), art.130 (comunicazioni indesiderate).

L'informativa privacy e la policy per l'utilizzo dei cookie sono pubblicate integralmente sul sito web aziendale [ww.enco.org](http://ww.enco.org), come stabilito per legge.

##### **a) TIPOLOGIA DI DATI TRATTATI**

Per contattare l'azienda è necessario compilare un form in cui si rendono noti alcuni dati personali (nome, cognome, indirizzo mail e stato di provenienza) previo rilascio dell'autorizzazione al trattamento.

##### **b) AMBITO E FINALITA' DEL TRATTAMENTO**

I dati raccolti nel sito internet vengono trattati esclusivamente per le finalità limitate alla risposta della richiesta di contatto inviata. Non è consentito un trattamento al di fuori di questo ambito almeno che il rapporto non si trasformi in quello tra cliente/fornitore; in questo caso le regole da seguire per il trattamento diventeranno quelle previste per la categoria, vedi paragrafo 1.2.1.1.

##### **c) ARCHIVIAZIONE E CONSERVAZIONE DEI DATI**

I dati raccolti vengono trasmessi tramite posta elettronica e con essa vanno conservati, come spiegato nei paragrafi precedenti.

La casella di posta cui vengono trasmessi è quella aziendale generica ([info@enco.energy](mailto:info@enco.energy)) il cui accesso è comunque consentito solamente ai titolari ed agli incaricati.

## 1.2.2. PROCEDURA DI ARCHIVIAZIONE E CONSERVAZIONE DEI DATI

### 1.2.2.1. Formato Cartaceo

- ANAGRAFICHE E CONTRATTI CLIENTI/FORNITORI

I documenti vengono conservati in archivio, ordinato in ordine alfabetico per fornitore o cliente. L'accesso all'archivio necessita di autorizzazione dell'incaricato, in possesso della chiave dell'armadietto dove sono raccolti i documenti.

La tempistica di conservazione è limitata alla durata dei contratti di fornitura/servizio, oppure intorno ai 15 anni se il periodo di collaborazione perdura.

- COMMESSE ED INCARICHI

Le pratiche di ciascuna commessa sono raccolte in un singolo raccoglitore/cartellina, identificata con il numero di riferimento della commessa (quest'ultimo viene stabilito secondo le procedure illustrate nel manuale Qualità ISO 9001). Vengono conservate in armadio per circa 15 anni, in modo da essere disponibili in caso di qualsiasi tipo di richiesta informazioni dovesse pervenire.

I dati contenuti in queste pratiche sono stati forniti previa autorizzazione al trattamento e l'accesso è permesso a tutti i dipendenti dell'ufficio.

- DOCUMENTI AMMINISTRATIVI

I documenti amministrativi sono conservati separatamente; l'accesso a questi documenti è limitato all'incaricato e ai titolari. Come già menzionato, sono conservati per dieci anni secondo quanto stabilito dall'art. 22 del DPR n. 600/1973.

Considerato che la tenuta della contabilità dello studio è esternamente appaltata allo Studio Commercialista Sara De Toffol e tutta la documentazione inerente, durante l'anno contabile, viene mensilmente consegnata a tale studio per la contabilità mensile e la redazione del bilancio a fine anno è pratica comune che i documenti contabili dell'anno in corso siano conservati in maniera provvisoria presso la sede di tale studio commercialista, che è situato a Sedico, Via Feltre 82. Allo stesso modo la documentazione relativa alla denuncia dei redditi annuale degli ingegneri titolari di ENCO viene affidata allo Studio De Toffol nel periodo della dichiarazione e riconsegnata a ENCO dopo che la presentazione è stata effettuata.

- CORRISPONDENZA

La corrispondenza viene archiviata a seconda della categoria di appartenenza dei documenti consegnati. Se si tratta, ad esempio, di fatture, queste verranno archiviate con i documenti amministrativi ed il trattamento dei dati avverrà di conseguenza.

## 1.2.2.2. Formato Elettronico

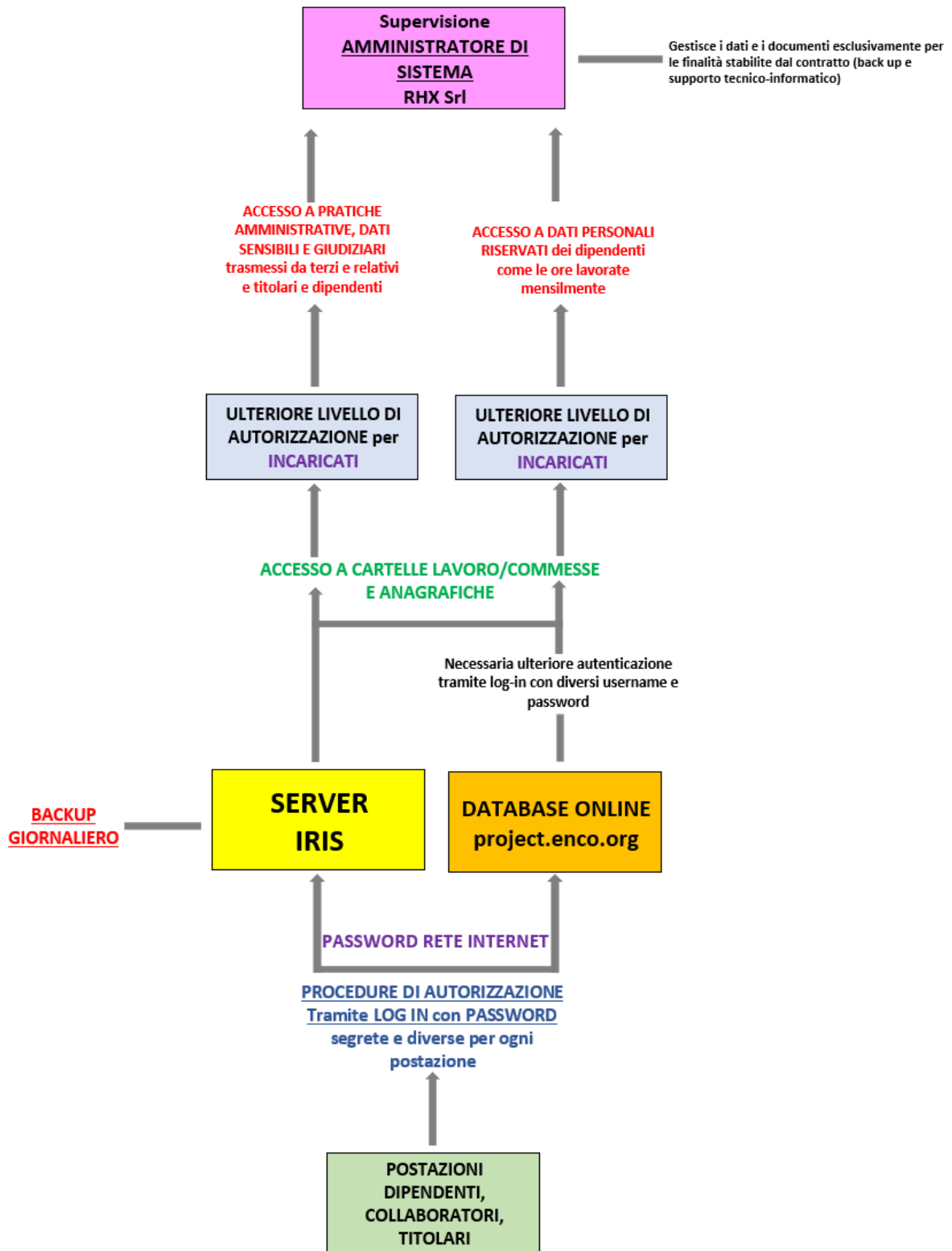


Figura 4 - Autorizzazioni Sistema Informatico

Come illustrato nella figura 4, la gestione del sistema informatico di ENCO è affidata ad un'azienda esterna: RHX S.r.l. con sede legale in piazza Resistenza, 5/1 31053 Pieve di Soligo (Treviso).

L'amministratore di sistema (nella persona di Alessandro De Zorzi, titolare di RHX Srl) ha accesso tramite proprio user e password a tutti i file a tutti i dati contenuti nel server IRIS e nel database project.enco.org ma non è autorizzato in alcun modo a consultare i dati in essi contenuti e tutte le operazioni che svolge devono essere limitate alle finalità del rapporto di fornitura e supporto informatico e back up che svolge per ENCO S.r.l.

I documenti e i dati di ogni genere e natura sono conservati all'interno del server IRIS, nelle cartelle predisposte. L'accesso a suddette cartelle è regolamentato dalle autorizzazioni predisposte dall'amministratore di sistema su indicazione dei titolari del trattamento (come illustrato in figura 3).

Per ottenere l'accesso sia al database che al server IRIS è necessario autenticarsi con nome utente e password. È possibile richiedere l'accesso all'archivio, limitatamente alle finalità stabilite, anche per utenti esterni. Per effettuare questo tipo di accesso è necessario comunque avere a disposizione delle credenziali ed essere a conoscenza della password della rete aziendale.

- ANAGRAFICHE E CONTRATTI CLIENTI/FORNITORI

All'interno del database online è archiviata una anagrafica, cui ogni utente ha accesso, contenente tutti i dati anagrafici di clienti, fornitori, dipendenti e collaboratori.

Allo stesso modo dati necessari per la gestione quotidiana dei rapporti con clienti e fornitori sono archiviati all'interno del server o nelle cartelle delle commesse di riferimento oppure nelle cartelle di segreteria ed amministrazione.

L'accesso a questo tipo di documenti è aperto a tutti coloro che operano nella rete aziendale.

- COMMESSE ED INCARICHI

Nel database i dati relativi alle commesse sono registrati all'interno della pagina di riferimento della commessa specifica. Dalla pagina principale ciascun utente può effettuare una ricerca inserendo il codice della commessa, ma solo i dati identificativi come nome del cliente sono consultabili.

Le commesse sono archiviate secondo il codice attribuitogli nella cartella LAVORO all'interno del server IRIS. Per la gestione quotidiana dell'attività di impresa ogni utente in possesso di autenticazione alla rete aziendale ha accesso a questa cartella, ma alcuni file confidenziali possono essere a loro volta protetti da password.

- DOCUMENTI AMMINISTRATIVI

I documenti amministrativi non sono in alcuna maniera presenti online sul database. Gli unici dati confidenziali presenti sono quelli relativi al conto mensile delle ore lavorate; l'accesso a questa sezione è comunque regolamentato da autorizzazioni più restrittive che ne limitano l'accessibilità ai soli incaricati, predisposte dall'amministratore di sistema su indicazione dei titolari.

Nel server IRIS i documenti amministrativi vengono archiviati nella cartella AMMINISTRAZIONE, la cui accessibilità è limitata agli incaricati ed ai titolari.

- CORRISPONDENZA - EMAIL

Essendo l'accesso alla posta elettronica personale, tutti i dati in essa contenuti sono archiviati nel computer dell'interessato e mantenuti in essere per tutta la durata del contratto.

È possibile per l'amministratore di sistema accedere ad una casella di posta, ma solamente per le finalità stabilite nel contratto di fornitura ad ENCO.

La gestione delle caselle di posta PEC di titolari e collaboratori è gestita dai singoli interessati che si occupano di mantenere i vincoli di sicurezza e di gestire l'archiviazione dei dati.

La gestione della casella PEC di ENCO è invece limitata ai titolari ed agli incaricati che ne gestiscono vincoli di sicurezza e archiviazione dei dati. E' necessario notare che spesso i documenti trasmessi via posta elettronica certificata sono importanti e contengono dati "più sensibili", per tanto è necessario porre un'attenzione extra al momento della consultazione e dell'archiviazione assicurandosi sempre di avere ottenuto il consenso al trattamento.



## 1.2.3. CICLO DI VITA DEL TRATTAMENTO DEI DATI

Il regolamento EU 16/679 mette al centro del sistema di trattamento dei dati il concetto di **privacy by design**. Con questo approccio si andrà a regolamentare meglio ogni fase del trattamento dei dati personali cercando di mettere primo piano alcune domande fondamentali come: quali dati è necessario raccogliere? Con quale metodo? A cosa servono? In modo da creare un procedimento logico di raccolta, trattamento e protezione che sia efficiente.

È importante che si arrivi a garantire un ciclo di vita sicuro in ogni fase, ma particolarmente in quella finale che prevede la cancellazione sicura.

### 1.2.3.1. Fase 1 – La raccolta del dato

L'aspetto più importante ed innovativo di questa prima fase introdotto dal regolamento EU 16/679 è quello della valutazione della qualità del dato.

È quindi fondamentale limitare la quantità di dati raccolti, tenendo anche in considerazione la necessità di alleggerire le pratiche di trattamento dati personali ed i relativi costi che esse comportano, in favore di una ricerca della qualità e della utilità del dato.

Questa scrematura, che deve essere effettuata a monte del procedimento di trattamento dati, avviene definendo lo scopo della raccolta dati e la valutazione della loro strategicità rispetto all'esercizio dell'attività di impresa.

L'acquisizione del dato passa sempre attraverso il rilascio del consenso da parte dell'interessato, il quale dovrà essere informato sulle finalità e lo scopo del trattamento.

### 1.2.3.2. Fase 2 – Archiviazione e protezione

Questa fase è stata presa in considerazione, in relazione alle tipologie di dati e categorie di soggetti interessati, nel capitolo precedente. L'archiviazione avviene sia nel sistema informatico aziendale che a livello di archivio cartaceo.

La descrizione delle protezioni dati è ben descritta in figura 4.

È necessario precisare che anche quando l'archiviazione è delegata a soggetti terzi, non viene mai meno la responsabilità sui dati personali gestiti e sulla loro sicurezza, per tanto è necessario stabilire con attenzione il dove e per quanto tempo conservare i dati raccolti ed organizzare la gestione e l'archiviazione in modo da garantire il massimo livello di sicurezza.

### 1.2.3.3. Fase 3 – Accesso ed utilizzo

È scontato precisare che l'azienda utilizza i dati raccolti. È però necessario stabilire le procedure di utilizzo, specificando quale settore aziendale tratta un certo tipo di dati e a quali finalità. È per tanto opportuno stabilire i diritti di accesso per ciascun settore o per ciascun dipendente, come nel caso di ENCO che è un'azienda di dimensioni molto limitate.

La definizione dei diritti di accesso aiuta ciascun dipendente ad individuare i propri processi di responsabilità in base alla possibilità di accedere ai dati ed utilizzarli. La figura 4 illustra brevemente lo schema dei diritti di accesso messi in pratica.

## 1.2.3.4. Fase 4 – Cancellazione e distruzione dei dati

La cancellazione dei dati è un diritto fondamentale dell'interessato previsto anche dal GDPR. È sempre importante tenere presente che non sempre azioni come cancellare un dato elettronico o buttare un foglio di carte equivalgono alla completa eliminazione di un dato. Le informazioni possono essere memorizzate ovunque per cui il grado di controllo in questa fase deve essere sempre molto alto. Per i documenti cartacei si deve procedere con la distruzione mentre per quelli elettronici è necessario ricorrere alla cancellazione sicura. L'importanza di questa procedura sarà meglio esposta nel capitolo dedicato al diritto dell'interessato alla cancellazione dei dati che lo riguardano.

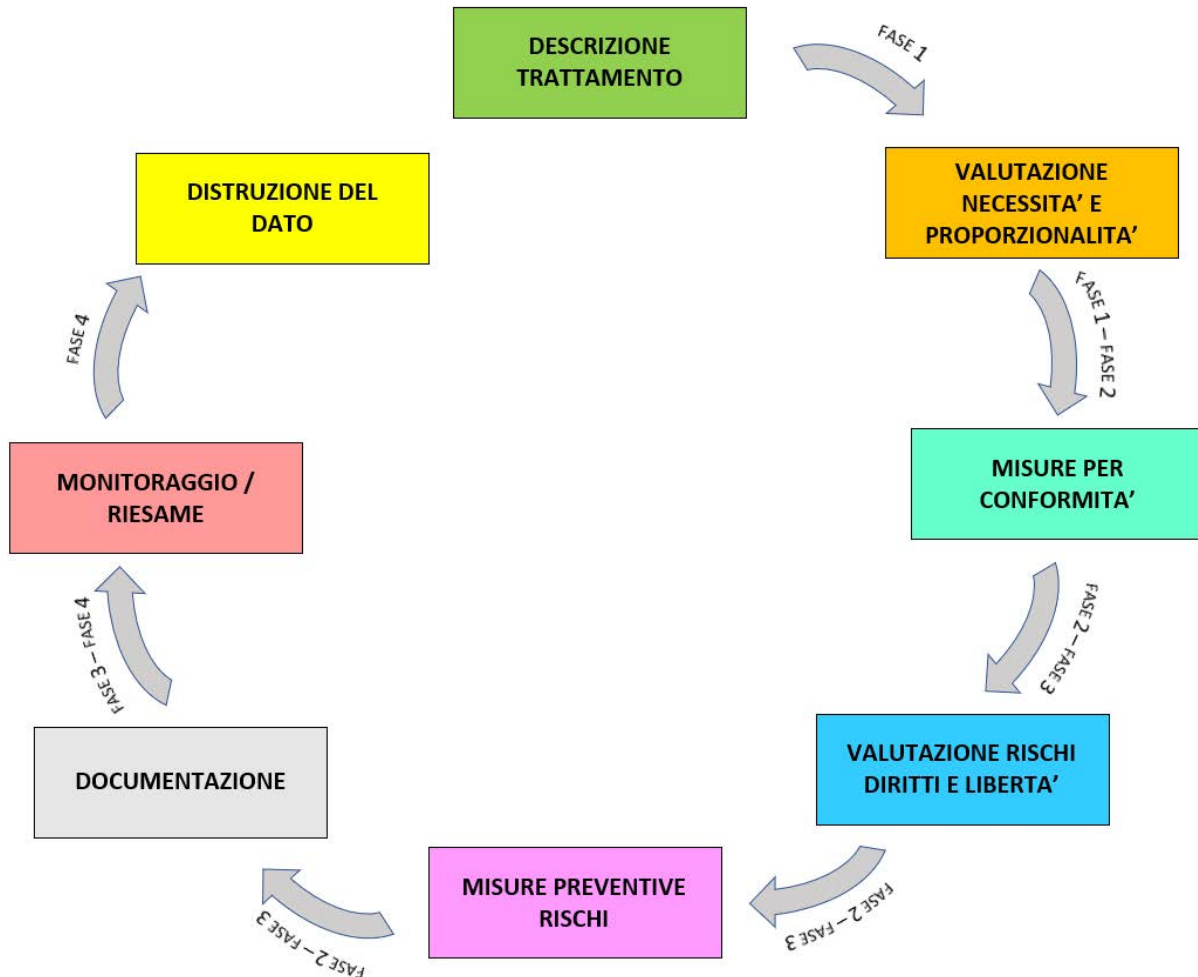


Figura 5 - Fasi del ciclo di vita del trattamento

## 1.2.4. RISORSE DI SUPPORTO AI DATI PERSONALI

- ARCHIVIO CARTACEO

I documenti relativi alle commesse sono archiviati in ordine cronologico (assegnazione numero di riferimento della commessa) in 4 armadi dell'ufficio (commesse più recenti) e nella stanza adibita esclusivamente ad archivio (commesse più vecchie) presso la sede di ENCO, in Via Feltre 183 a Sedico (BL).

I documenti amministrativi sono archiviati in altri 4 armadi, sempre situati presso la sede di ENCO, con accesso limitato agli incaricati.

La contabilità dell'anno corrente viene invece conservata presso lo studio della commercialista Sara De Toffol, che se ne occupa. Lo studio è situato in Via Feltre, 82 a Sedico (BL).

- ARCHIVIO INFORMATICO

Le postazioni lavorative che hanno accesso al **SERVER IRIS**, dove sono archiviate tutte le pratiche relative all'attività d'impresa di ENCO sono 8.

Gli accessi alle diverse cartelle del server sono regolati dalle autorizzazioni predisposte dai titolari e dall'amministratore di sistema, come già illustrato precedentemente.

Il backup viene effettuato giornalmente su cassetine esterne che vengono conservate nell'apposito archivio situato nella sala server. Gli utenti semplici non hanno accesso ai file di backup che sono recuperabili esclusivamente dall'amministratore di sistema.

## 2. PRINCIPI FONDAMENTALI

La figura 5 nel capitolo precedente anticipa alcuni dei principi fondamentali da tenere presenti durante il trattamento dei dati personali.

Questi principi sono messi in evidenza nel **Regolamento UE 2016/679 del 27 Aprile 2016**, la loro messa in atto è importante per garantire una gestione corretta dei dati e conforme alla corrente legislazione.

### 2.1. NECESSITA' E PROPORZIONALITA'

I principi di necessità e proporzionalità sono fondamentali fin dalle fasi precedenti l'inizio del trattamento e devono essere tenuti in considerazione in ogni sua fase.

- PRINCIPIO DI NECESSITA'

Il principio impone a ciascuna amministrazione titolare del trattamento di accertare se la finalità perseguita possa essere realizzata rilevando solamente i dati necessari (ad esempio non raccogliendo dati biometrici o altri dati sensibili se non strettamente utili) ed evitando in ogni caso un eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato.

- PRINCIPIO DI PROPORZIONALITA'

Il principio di proporzionalità impone una gestione del rischio e una predisposizione di misure per la protezione dati personali che siano proporzionali alla quantità ed al tipo ("livello di sensibilità") dei dati raccolti.

#### 2.1.1. CARATTERISTICHE DEGLI SCOPI DEL TRATTAMENTO

- CLIENTI E FORNITORI

Per quel che riguarda clienti e fornitori ENCO Engineering Consultants S.r.l. raccoglie ed utilizza i dati personali **specificatamente** per dare esecuzione al rapporto commerciale in essere tra le parti e dare attuazione agli obblighi previsti dalla normativa italiana e comunitaria.

Il trattamento è **necessario** per l'esecuzione di un contratto di forniture e per adempiere alle pratiche ad esso correlate.

Il trattamento è **legittimo** in quanto l'interessato ha acconsentito al trattamento dei propri dati personali per gli scopi specifici indicati nell'informativa messa a disposizione.

- COLLABORATORI ESTERNI ED INTERNI

ENCO Engineering Consultants S.r.l. raccoglie ed utilizza i dati personali dei collaboratori per lo scopo **specifico** di gestione del rapporto di collaborazione all'interno dell'attività di impresa ovvero, ad esempio, per la stesura del contratto e la gestione delle pratiche amministrative come la fatturazione.

Il trattamento è **necessario** per adempiere agli obblighi amministrativi e legati al contratto, come da legge italiana e comunitaria.

Il trattamento è **legittimo** in quanto l'interessato ha acconsentito al trattamento dei propri dati personali per gli scopi specifici indicati nell'informativa messa a disposizione.

- DIPENDENTI

ENCO Engineering Consultants S.r.l. raccoglie ed utilizza i dati personali dei dipendenti per lo scopo **specifico** di gestione del rapporto di lavoro come previsto dalla normativa italiana e comunitaria. I dati considerati "sensibili" che possono essere contenuti nelle buste paga o nelle cartelle sanitarie dei dipendenti sono soggetti a vincoli di riservatezza maggiormente restrittivi e trattati esclusivamente dagli incaricati solo per **specifici fini di archiviazione**, sempre in maniera conforme alla normativa.

Il trattamento è **necessario** per l'instaurazione di un contratto di lavoro e per adempiere alle pratiche ad esso correlate.

Il trattamento è **legittimo** in quanto l'interessato ha acconsentito al trattamento dei propri dati personali per gli scopi specifici indicati nell'informativa messa a disposizione.

## 2.2. ALTRI PRINCIPI E BASI LEGALI

Il **Regolamento Europeo 2016/679 del 27 Aprile 2016** stabilisce che un trattamento di dati personali deve trovare fondamento in una base giuridica.

L'**articolo 6** del regolamento europeo enuncia le condizioni in base alle quali il trattamento può dirsi lecito, queste voci sono elencate nel principio di liceità del trattamento.

Nei processi per il trattamento illustrati nei capitoli precedenti si possono trovare i riferimenti e le conformità con i principi legalmente previsti per il trattamento dei dati personali che sono di seguito elencati ed illustrati per una più chiara comprensione.

### 2.2.1. PRINCIPI DI LICEITA', CORRETTEZZA E TRASPARENZA

- PRINCIPIO DI LICEITA' E CORRETTEZZA

Per quanto riguarda l'ambito di attività di ENCO, il trattamento è lecito solo alle condizioni previste espressamente dall'art. 6 del Regolamento ovvero quando l'interessato ha espresso il proprio consenso ("consenso informato") al trattamento dei propri dati per una o più specifiche finalità, o quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o ancora quando il trattamento è necessario per adempiere ad un obbligo legale a cui è soggetto il titolare del trattamento.

Infine il trattamento è lecito quando lo stesso è necessario per il perseguimento del legittimo interesse del titolare; quest'ultima circostanza deve essere interpretata alla luce di un bilanciamento tra gli interessi del titolare del trattamento e gli interessi, i diritti e le libertà fondamentali dell'interessato.

- PRINCIPIO DI TRASPARENZA

Il principio di trasparenza è fondamentale e rientra anche tra i diritti dell'interessato.

Dovranno essere trasparenti le modalità con cui sono raccolti ed utilizzati i dati personali e devono essere facilmente accessibili e comprensibili le informazioni e comunicazioni relative al trattamento (identità del titolare del trattamento, finalità del trattamento, diritti degli interessati etc.)

## 2.2.2. PRINCIPI DI LIMITAZIONE E MINIMIZZAZIONE DEI DATI

- PRINCIPIO DI LIMITAZIONE

I dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente devono essere trattati in una modalità che sia compatibile con tali finalità. Il trattamento dei dati per finalità diverse da quelle per le quali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con tali iniziali finalità-

- PRINCIPIO DI MINIMIZZAZIONE

I dati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati. Questo principio si rifà anche a quanto già esposto nel capitolo dedicato alle fasi del ciclo di vita dei dati.

## 2.2.3. PRINCIPI DI INTERGRITA' E RISERVATEZZA

- PRINCIPI DI INTEGRITA' E RISERVATEZZA

I dati devono sempre essere trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate a proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale (vedere capitoli precedenti).

## 2.2.4. PRINCIPI DI ACCURATEZZA, AGGIORNAMENTO E CONSERVAZIONE DEI DATI

- PRINCIPIO DI ESATTEZZA E AGGIORNAMENTO

I dati devono essere sempre esatti ed aggiornati. Eventuali inesattezze devono essere tempestivamente rettificare ovvero i dati inesatti devono essere cancellati.

- PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

I dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati (nello specifico vedere i capitoli precedenti).

## 2.3. DIRITTI PERSONALI DEI SOGGETTI INTERESSATI

Il regolamento generale sulla protezione dei dati riserva particolare attenzione alla definizione dei diritti dell'interessato al trattamento.

Diventa importante per i titolari di trattamento adottare le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto previsto precedentemente – dovrà avere per impostazione predefinita forma scritta (anche elettronica).

La guida del Garante all'applicazione di questa porzione del Regolamento evidenzia alcuni aspetti fondamentali:

**Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese**, estendibili fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.**

**Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) (*art. 12.5*), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso (*art. 15, paragrafo 3*); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso (*art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3*).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.

Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici.

### 2.3.1. INFORMAZIONE E CONSENSO DEI SOGGETTI INTERESSATI

Come già specificato nel paragrafo dedicato al principio di liceità del trattamento, quest'ultimo deve avvenire **sempre dopo l'ottenimento del consenso informato da parte dell'interessato.**

L'ottenimento del consenso avviene, di norma, attraverso la firma dell'informativa scritta. Nulla vieta che per il trattamento di dati non sensibili alcune informazioni o variazioni possano anche venire trasmesse per via orale.

Come già più volte sottolineato, l'ottenimento del consenso è indispensabile per effettuare il trattamento dei dati che a sua volta è condizione necessaria affinché ENCO possa fornire i propri servizi o gestire rapporti di dipendenza e collaborazione.

## 2.3.2. DIRITTI DI ACCESSO E PORTABILITA'

### 2.3.2.1.1. Diritto d'accesso: descrizione

Il **diritto di accesso** è disciplinato dall'art. 15 del Regolamento. Sancisce che l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, e, se in corso tale trattamento l'accesso ai dati ed alle seguenti informazioni:

- Finalità del trattamento
- Categorie di dati personali oggetto del trattamento
- Destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali
- Quando possibile il periodo di conservazione dei dati personali previsto, oppure, se non è possibile, i criteri utilizzati per determinare questo periodo.
- L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento
- Il diritto di proporre reclamo ad un'autorità di controllo
- Qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine
- L'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il titolare del trattamento deve fornire all'interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta di accesso, ai sensi degli articoli da 15 a 20, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa.

Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste.

Qualora si applichi la proroga, l'interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico, salvo indicazione diversa dell'interessato.

Se non si ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo ad un'autorità di controllo e di proporre ricorso giurisdizionale.



## 2.3.2.1.2. Diritto d'accesso: come viene esercitato

- CLIENTI / FORNITORI / COLLABORATORI ESTERNI

Le informazioni essenziali sono contenute nell'informativa per il consenso al trattamento dei dati personali. Nel particolare in questo documento sono esplicitate in modo chiaro e facilmente comprensibile le informazioni sopra elencate.

L'accesso a informazioni più dettagliate è sempre possibile su richiesta cartacea, elettronica o anche orale dell'interessato.

Sarà cura del titolare del trattamento rispondere alla suddetta richiesta secondo tempi e modalità definiti precedentemente.

- COLLABORATORI INTERNI / DIPENDENTI

Anche queste categorie ricevono le informazioni essenziali tramite l'informativa per l'espressione del consenso al trattamento. Essi hanno comunque accesso ad alcune categorie di dati archiviati in forma cartacea o elettronica presso la sede dell'azienda e sono liberi di richiedere l'assistenza dell'incaricato per garantirsi l'accesso ad altri dati personali protetti da maggiori livelli di sicurezza.

La richiesta può essere fatta in forma cartacea, elettronica o anche orale dell'interessato.

Sarà cura del titolare del trattamento rispondere alla suddetta richiesta secondo tempi e modalità definiti precedentemente.

## 2.3.2.1.3. Diritto di portabilità: descrizione

L'interessato ha sempre il diritto di ricevere una copia dei dati personali oggetto di trattamento. Secondo il **diritto alla portabilità**, l'articolo 20 del Regolamento stabilisce che copia dei dati debba essere consegnata in formato strutturato, di uso comune e leggibile da dispositivo automatico da parte del titolare del trattamento.

L'interessato ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti nel caso in cui:

- Il trattamento si basi sul consenso ai sensi dell'articolo 6 o dell'articolo 9
- Il trattamento sia effettuato con mezzi automatizzati

Nell'esercitare i propri diritti relativamente alla portabilità dei dati l'interessato ha il diritto di ottenere la trasmissione diretta dei dati da un titolare del trattamento all'altro, se tecnicamente fattibile.

Il diritto alla portabilità si può considerare come una sorta di estensione del diritto di accesso.

## 2.3.2.1.4. Diritto di portabilità: come viene esercitato

- CLIENTI / FORNITORI / COLLABORATORI ESTERNI ed INTERNI/DIPENDENTI

Per tutte queste categorie i documenti contenenti dati personali e le informazioni relative al trattamento vengono forniti in copia elettronica, in formati leggibili e strutturati di uso comune.

In caso di richiesta da parte degli interessati ENCO si rende disponibile a fornire copia della documentazione in forma cartacea.

## 2.3.3. DIRITTI DI RETTIFICA, CANCELLAZIONE ED OBLIO

### 2.3.3.1.1. Diritto di rettifica: descrizione

Il **diritto di rettifica**, già previsto dall'ordinamento italiano, prevede per l'interessato l'ottenimento da parte del titolare del trattamento della rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

### 2.3.3.1.2. Diritto di rettifica: come viene esercitato

- CLIENTI / FORNITORI / COLLABORATORI ESTERNI ed INTERNI/DIPENDENTI

Qualsiasi persona fisica o giuridica parte delle categorie interessate al trattamento può in qualsiasi momento richiedere per via cartacea o elettronica la rettifica o l'integrazione dei dati personali soggetti al trattamento.

ENCO si riserva il diritto di verificare la legittimità della richiesta in base alla finalità del trattamento comunicata in fase di richiesta di consenso ed eventualmente procedere con la rettifica o l'integrazione dei dati.

### 2.3.3.1.3. Diritto alla cancellazione ed oblio: descrizione

Con il **diritto alla cancellazione** ed all'oblio, l'interessato acquisisce il diritto a chiedere che siano cancellati e non più sottoposti al trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati che lo riguardano o quando il trattamento dei suoi dati personali non sia conforme con il Regolamento.

Questo diritto appare particolarmente rilevante quando i dati trattati sono presenti sul web.

Dovrebbe comunque rimanere lecita l'ulteriore conservazione dei dati qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per finalità di archiviazione di pubblico interesse, finalità statistiche o difendere un diritto in sede giudiziaria.

### 2.3.3.1.4. Diritto alla cancellazione ed oblio: come viene esercitato

- CLIENTI / FORNITORI / COLLABORATORI ESTERNI ed INTERNI/DIPENDENTI

Qualsiasi persona fisica o giuridica parte delle categorie interessate al trattamento può in qualsiasi momento richiedere per via cartacea o elettronica la cancellazione e la distruzione dei dati personali soggetti al trattamento.

ENCO si riserva il diritto di verificare la legittimità della richiesta in base alla finalità del trattamento ed alle necessità della conservazione dei dati oggetto di richiesta di eliminazione ed eventualmente comunicare l'accoglimento della richiesta e la conferma di avvenuta cancellazione dei dati su tutte le piattaforme di archiviazione.

Nel caso di un ritiro del consenso da parte dell'interessato, ENCO, nel caso in cui il trattamento sia necessario e indispensabile per l'esercizio dell'attività di impresa, il rapporto di fornitura, di

collaborazione o rapporto lavorativo si riserva il diritto di interrompere il rapporto in corso per l'impossibilità di gestirlo ed adempiere agli obblighi amministrativi venendo a mancare l'accesso ai dati.

## 2.3.4. DIRITTI DI RESTRIZIONE ED OBIEZIONE

### 2.3.4.1.1. Diritto di obiezione o opposizione: descrizione

Il **diritto di obiezione o opposizione** dell'interessato, in aggiunta a quanto già espresso nella vecchia legislazione, è inteso, nel nuovo Regolamento, come strumento per limitare il potere informatico controllandone mezzi e fini. Consente inoltre di arginare le intrusioni nei propri dati personali consentendo di opporsi e rifiutare il consenso al trattamento.

L'art.21 sancisce che l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1 (lettere e) ed f)), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento non tratta più i dati personali salvo che egli dimostri l'esistenza di motivi legittimi preminenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'art 22 regola il trattamento automatizzato dei dati personali, circostanza che però non interessa l'attività di ENCO Engineering Consultants Srl.

### 2.3.4.1.2. Diritto di obiezione o opposizione: come viene esercitato

Qualsiasi persona fisica o giuridica parte delle categorie interessate al trattamento può in qualsiasi momento opporsi, per via cartacea o elettronica, al trattamento dei propri dati personali.

ENCO si riserva il diritto di verificare la legittimità della richiesta in base alla finalità del trattamento e di eventualmente rivendicare l'esistenza di motivi legittimi preminenti che consentirebbero la prosecuzione del trattamento, e solo eventualmente comunicare l'accoglimento della richiesta e l'interruzione del trattamento.

### 2.3.4.1.3. Diritto di restrizione o limitazione: descrizione

Il **diritto di restrizione o limitazione** del trattamento dei dati personali può venire richiesto dall'interessato in alcuni casi specifici:

- L'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati
- Il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece ne sia limitato l'utilizzo
- Benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
- L'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Quando il trattamento è limitato i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

#### 2.3.4.1.4. Diritto di restrizione o limitazione: come viene esercitato

Qualsiasi persona fisica o giuridica parte delle categorie interessate al trattamento può in qualsiasi momento esercitare il diritto di restrizione o limitazione al trattamento per i propri dati, per via cartacea o elettronica, al trattamento dei propri dati personali.

ENCO si riserva il diritto di verificare la presenza di una delle condizioni in elenco e di valutare la legittimità della richiesta in base alla finalità del trattamento ed eventualmente comunicare l'accoglimento della richiesta e l'interruzione del trattamento.

### **2.3.5. TRASFERIMENTO DI DATI FUORI DALL'UNIONE EUROPEA**

In un'ottica di compliance con la regolamentazione sul trasferimento di dati extra UE, le organizzazioni devono dotarsi di adeguate procedure organizzative che consentano di valutare preventivamente le casistiche di trasferimento ed essere in grado di dimostrare il rispetto dei requisiti normativi disciplinati dal GDPR (accountability).

La politica messa in campo da ENCO in questo ambito si basa su una considerazione molto semplice: il dato personale trasferito in un paese esterno all'Unione Europea deve godere del medesimo livello di protezione di cui beneficerebbe se rimanesse nei confini dell'Unione.

Di conseguenza, considerando che i dati soggetti a trasferimento sono "non sensibili" ed il trasferimento avviene sempre in un contesto di collaborazione regolato da contratto, ENCO si riserva di includere nei punti chiave del contratto i principi base del trattamento dei dati: consenso informato, informativa sulle finalità e diritti degli interessati e tratta i dati inclusi nel contratto utilizzando le strategie già illustrate nei capitoli precedenti.

### 3. RISCHI

L'analisi del rischio privacy ha un ruolo fondamentale: diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati.

#### 3.1. VALUTAZIONE DEL RISCHIO E DELL'IMPATTO

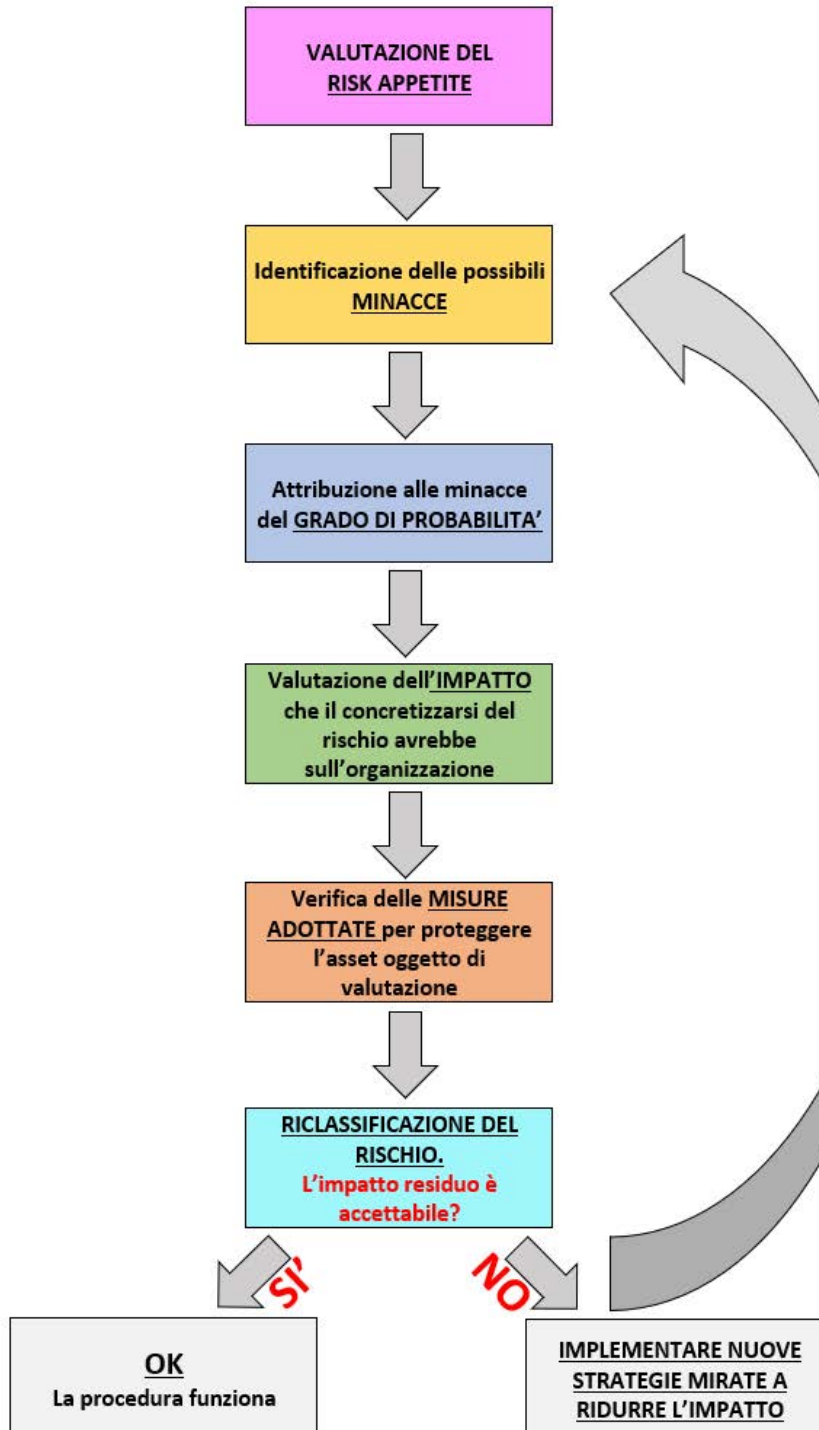


Figura 6 - Diagramma di valutazione del grado di rischio

Nel valutare l'adeguato 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.

Lo schema a pagina precedente illustra una strategia di stima delle minacce e del rischio volta ad ottenere una valutazione dell'efficacia delle misure adottate per la protezione dei dati.

## 3.2. CONTROLLI GENERALI GIÀ ESISTENTI O PIANIFICATI

Per aumentare il livello di sicurezza e protezione dei dati personali esistono una serie di controlli, accorgimenti e politiche già esistenti e/o già pianificate.

Di seguito una carrellata delle strategie messe in atto da ENCO già allo stato attuale, per garantire la sicurezza dei dati personali in sede di trattamento e di archiviazione.

### 3.2.1. STRATEGIE GENERALI APPLICATE PRIMA E DURANTE IL TRATTAMENTO

#### 3.2.1.1. Minimizzazione quantità dei dati raccolti

ENCO si impegna fin dal momento della raccolta dei dati a minimizzare la quantità di informazioni soggette a trattamento, richiedendo esclusivamente quanto previsto dalle finalità ed indispensabile per l'esercizio dell'attività di impresa.

Si assicura inoltre che la stessa cura sia adottata dalle aziende terze che gestiscono alcuni dati, anche sensibili, per conto della società.

### 3.2.2. PROTEZIONE DATI SU SUPPORTO INFORMATICO

Quando si parla di protezione dei dati, è importante distinguere tra i dati statici e quelli in movimento. I dati statici sono quelli a cui non si può accedere – tra cui per esempio quelli masterizzati su un DVD e archiviati su uno scaffale o quelli contenuti nell'hard disk di un PC spento. I dati in movimento solo quelli a cui si può accedere o che possono essere inviati.

Il primo obiettivo è proteggere i dati in movimento da chiunque non sia legittimato ad utilizzarli. Ma sarà necessario anche proteggere i dati statici che potrebbero successivamente diventare dati in movimento.

#### 3.2.2.1. Controllo degli accessi

##### 3.2.2.1.1. Indicazioni Generali

ENCO da sempre ha adottato un sistema di gestione dei processi legati alla creazione, registrazione e gestione delle identità degli utenti ed i loro relativi permessi ed autorizzazioni. Questa policy se applicata in modo corretto garantisce una maggiore efficacia del programma di valutazione e limitazione del rischio, impedendo l'implementazione delle richieste d'accesso in appropriate e monitorando le altre.

I vantaggi sono:

- ottimizzazione della gestione degli account dei dipendenti
- la possibilità di tenere traccia delle autorizzazioni rilasciate agli utenti ed avere così uno storico dei permessi degli account informatici aziendali

- contribuire alla protezione delle applicazioni e dei dati critici dell'azienda garantendo al tempo stesso una comodità di accesso e di utilizzo agli utenti e all'amministratore di sistema
- grazie alla migliore visibilità ed al più ampio contesto delle informazioni utente centralizzate, la capacità di analizzare varie metriche in tempo reale ed intraprendere le azioni appropriate per mitigare le minacce, generando un sistema sicuro per consentire agli utenti di collegarsi ovunque ed in qualsiasi momento rispettando sempre le regole e le normative.

I profili degli utenti vengono definiti in base alle necessità di accesso per lo svolgimento delle proprie mansioni.

#### 3.2.2.1.2. Password e mezzi di autenticazione

La password di accesso alla rete aziendale viene impostata dall'amministratore di sistema, ne sono a conoscenza esclusivamente dipendenti e collaboratori che operano nelle postazioni dell'ufficio. Deve essere composta da una sequenza di lettere maiuscole e minuscole e numeri. Non è stabilito un numero di tentativi minimi per effettuare l'accesso.

La rete wifi che garantisce anche l'accesso al server, oltre che quello ad internet, è dotata di una password diversa, sempre impostata dall'amministratore di sistema e composta da una sequenza di lettere maiuscole e minuscole. Non è stabilito un numero di tentativi minimi per effettuare l'accesso.

Le password di accesso alle postazioni di lavoro vengono inizialmente assegnate dall'amministratore di sistema ma possono venire modificate dal singolo utente.

La composizione di queste password è libera, ma si sconsiglia di utilizzare riferimenti che possano ricondurre all'utente titolare della postazione. Il numero di tentativi minimi per effettuare l'accesso è di tre.

Le credenziali d'accesso per ottenere le autorizzazioni necessarie all'accesso alle aree del server sono impostate dall'amministratore di sistema al momento dell'assegnazione dei permessi ai singoli utenti. I dipendenti ed i collaboratori non ne sono a conoscenza. Vengono utilizzare password alfanumeriche. Il numero di tentativi minimi per effettuare l'accesso è di tre.

Le password di accesso alle email vengono assegnate dall'amministratore di sistema e possono venire modificate dall'interessato intestatario della casella. La password assegnata deve essere alfanumerica e composta da almeno 8 caratteri comprendenti maiuscole/minuscole e segni di punteggiatura. Il numero di tentativi minimi per effettuare l'accesso è di tre.

La password di accesso al database project.enco.org è assegnata dall'amministratore di sistema al momento di creazione dell'account e dell'assegnazione dei privilegi. Si tratta di una password alfanumerica che può venire modificata dall'utente in un singolo momento. Sono invece non modificabili, se non tramite le credenziali di amministratore, i privilegi assegnati che garantiscono l'accesso a diverse aree del database. Il numero di tentativi minimi per effettuare l'accesso è di tre.

L'eventuale sblocco degli account è possibile solamente con un intervento dell'amministratore di sistema.

### **3.2.2.2. Archiviazione su server e su database**

#### **3.2.2.2.1. Indicazioni generali**

L'archiviazione dei documenti amministrativi (tra i quali includiamo non solo le fatture ma anche i documenti bancari, assicurativi, documenti di identità, documenti relativi alla retribuzione etc.) avviene esclusivamente su server, nelle cartelle predisposte il cui accesso è limitato ai soli dipendenti le cui mansioni ne necessitano la consultazione.

L'archiviazione dei documenti relativi alle commesse avviene su server ma alcuni dati sono registrati anche nel database project.enco.org. Questo perché la creazione della cartella relativa alla commessa avviene innanzitutto sulla piattaforma online tramite l'inserimento di alcuni dati basilari (nome della commessa, cliente, tipologia di incarico etc.) che consentirà la generazione di un codice e la contemporanea creazione di una cartella corrispondente sul server IRIS:

L'accesso a queste cartelle è aperto a tutti i dipendenti e collaboratori interni in quanto fondamentale per lo svolgimento di qualsiasi mansione all'interno dello studio.

#### **3.2.2.2.2. Ulteriori strumenti di protezione**

L'accesso ad alcuni file confidenziali sia tra i documenti amministrativi che tra quelli relativi alle commesse può essere ulteriormente protetto da password impostate per l'apertura del file o da limitazioni relative alla modifica da parte di alcuni utenti.

Queste impostazioni possono essere applicate a discrezione dai titolari qualora il file in questione sia considerato particolarmente "sensibile".

### **3.2.2.3. Vulnerabilità del dato e lotta contro malware e virus**

Tra le politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività e procedure operative documentali al momento attuiamo:

- Costante aggiornamento dei sistemi operativi di tutte le postazioni di lavoro.  
L'aggiornamento avviene in maniera automatica, previo avviso all'utente il quale è responsabile della sua installazione.
- Costante aggiornamento dei software installati presso le postazioni per ridurre al minimo falle sulla sicurezza
- Procedura di backup giornaliera su cassette esterne per consentire il recupero di dati danneggiati
- Blocco di possibili installazioni di software non sicuri e necessità di accesso come amministratore per eventuali nuove installazioni
- Antivirus attivo e sempre aggiornato su ciascuna postazione. Per garantire che questa attività sia svolta con puntualità e precisione, essa è compito dell'amministratore di sistema.
- Sistema di firewall online che impedisce l'accesso a siti non sicuri ed impedisce connessioni non sicure con possibilità di fughe di dati, anch'esso gestito dall'amministratore di sistema
- Tracciamento degli accessi per evitare l'accesso di utenti estranei
- Protezione della rete internet con la creazione di diverse reti wifi e impedimento per gli ospiti di accedere tramite wifi al server aziendale
- Servizio di avviso via mail in caso di rilevamento di minacce da parte dell'amministratore di sistema.



### **3.2.2.4. Sicurezza siti web, backup e manutenzione**

#### **3.2.2.4.1. Backup**

Il sistema di protezione firewall è esclusivamente gestito dall'amministratore di sistema; nel caso in cui un utente connesso alla rete tenti di accedere ad un sito internet considerato pericoloso, questo accesso sarà bloccato; se si stabilirà che si tratta di un sito che non crea una minaccia per la sicurezza si renderà necessario richiedere all'amministratore di sistema che sia inserito nelle eccezioni del firewall.

#### **3.2.2.4.2. Backup**

La procedura di backup di tutti i file del server IRIS avviene giornalmente.

E' supportata dall'amministratore di sistema che quotidianamente controlla che il processo avvenga correttamente e senza errori. Al termine della procedura viene inviata una mail di conferma alla casella di posta [info@enco.energy](mailto:info@enco.energy), con un log dei file oggetto di backup.

Viene effettuato su supporti esterni, cassetine numerate, secondo un calendario stabilito ad inizio anno solare.

È compito del dipendente, in questo caso anche incaricato privacy, inserire giornalmente la cassetta prevista nel server ed estrarre quella del giorno precedente.

Le cassette con i backup effettuati vengono conservate nella sala server in armadio chiuso a chiave cui hanno accesso solamente i dipendenti incaricati.

I dipendenti non possiedono le autorizzazioni necessarie per ripristinare un file (corrotto, accidentalmente eliminato o errato – ricordiamo che i file archiviati su server IRIS, se eliminati, non si spostano momentaneamente nel cestino ma sono direttamente cancellati) dall'archivio di backup ed è necessario l'intervento dell'amministratore di sistema per poter effettuare questa operazione.

#### **3.2.2.4.3. Manutenzione**

Ciascun utente è in parte responsabile della manutenzione della propria postazione, non solo prestando cura nell'utilizzo dell'attrezzatura e a non mettere a rischio la sicurezza dei dati tramite accessi non consentiti, ma anche procedendo con regolarità all'aggiornamento del sistema operativo, hardware e software quando richiesto.

Per qualsiasi altra operazione necessaria è tenuto ad intervenire l'amministratore di sistema il quale si occupa anche di alcune altre operazioni di manutenzione periodica che sono però importantissime, prime tra tutte l'aggiornamento degli antivirus, i controlli di sicurezza della rete (necessità di cambiare chiavi d'accesso), la verifica di eventuali errori nel processo di backup che possano costituire falle nella sicurezza, la gestione dei domini.

Una nota a parte merita la manutenzione del sito internet e degli eventuali accessi indesiderati all'area riservata.

Il sito internet è gestito dall'azienda TLO di Enzo Tassan che si occupa della sua gestione tecnica e manutenzione, basandosi sulle direttive dei titolari.

Gli accessi all'area riservata vengono comunicati sulla mail [info@enco.energy](mailto:info@enco.energy), così come gli eventuali messaggi di richiesta di informazioni.

ENCO ha anche un altro piccolo sito internet su dominio minihydro.com.

Anche gli accessi all'area amministratore di questo sito (la gestione di questo dominio è affidata alla società Iarin srl, così come quella del resto dei domini) vengono comunicati su [info@enco.energy](mailto:info@enco.energy) in modo da prevenire e segnalare eventuali tentativi di accesso indesiderati.

### **3.2.2.5. Organizzazione**

L'organizzazione delle mansioni e delle postazioni è descritta nel documento di valutazione dei rischi per la sicurezza.

L'accesso alle postazioni è personale, necessita di password ed è sempre tracciabile (dall'amministratore di sistema), di conseguenza è anche riconducibile ad un singolo utente l'accesso ai dati e la loro modifica. È consentito per l'amministratore di sistema effettuare questo tipo di verifiche solo in caso di dubbio di violazioni o pratiche scorrette.

L'accesso ai dati, come già più volte specificato, è regolato da permessi stabiliti dall'amministratore di sistema in accordo con i titolari.

Gli accessi fisici sono anch'essi monitorati, così come gli accessi alla rete aziendale.

### **3.2.2.6. Politiche**

Queste le strategie che ENCO mette in atto per migliorare la protezione dei dati e gestire i rischi del trattamento. Stabilire:

- 1) I dati a cui avrà accesso o che gli saranno trasmessi.
- 2) Le operazioni che deve eseguire sui dati.
- 3) La durata per la quale può memorizzare i dati.
- 4) Tutti i destinatari a cui il responsabile del trattamento potrà trasmettere i dati.
- 5) Le operazioni da eseguire al termine del servizio (cancellazione permanente dei dati o restituzione dei dati nel contesto della reversibilità quindi distruzione di dati).
- 6) Gli obiettivi di sicurezza stabiliti dal titolare del trattamento.
- 7) Determinare la ripartizione delle responsabilità.

A queste si aggiungono le già citate procedure di minimizzazione dei dati e riduzione della loro natura identificativa.

### **3.3. MINACCE E RISCHIO NEL TRATTAMENTO DEI DATI PERSONALI**

#### **3.3.1. VALUTAZIONE DELLE PRINCIPALI MINACCE E DELLE FONTI DI RISCHIO**

##### **3.3.1.1. Definizione e tipi di minacce**

Intendiamo per minaccia, un qualsiasi incidente potenziale che mette in pericolo le informazioni ed i dati in possesso dell'Azienda. Ciò avviene quando, per cause intenzionali o accidentali, una minaccia è in grado di sfruttare una carenza dei sistemi, dell'organizzazione, delle applicazioni e dei servizi.

L'individuazione preventiva delle minacce consente di meglio tarare il sistema di sicurezza dell'Azienda in relazione ai rischi che potrebbe incontrare.

Le minacce possono essere distinte in base alla loro origine:

- **INTERNA:** dovuta al comportamento dei membri dell'Azienda
- **ESTERNA:** dovuta al comportamento degli utenti o di terzi;
- **AMBIENTALE:** dovuta ad eventi accidentali, sia tecnici sia disastrosi, che possono danneggiare il sistema informativo nel suo complesso o qualcuno dei suoi componenti chiave; o danneggiare l'archivio dati cartaceo

##### **3.3.1.2. Cause e fonti di rischio**

Tra le fonti di rischio che possono contribuire al concretizzarsi delle minacce possiamo rilevare:

- carenze organizzative
- responsabilità non bene individuate o assegnate,
- carenze procedurali o di controllo;
- colpa, incuria, ignoranza o imperizia nei comportamenti degli addetti o degli utenti;
- dolo: volontà di impossessarsi indebitamente delle informazioni o di recare danno

Le più importanti minacce prese in considerazione sono:

- accesso non autorizzato alle informazioni da parte di terzi interni o esterni non autorizzati;
- alterazione, modificazione non autorizzata da parte di persone non autorizzate delle informazioni o dei software di gestione dati;
- perdita, distruzione, danneggiamento o impedimento all'uso dei dati, apparecchi o dei supporti informatici;
- divulgazione: accesso da parte di soggetti non autorizzati per legge a informazioni personali e/o dati sensibili non divulgabili;
- trattamento illecito o non conforme alle finalità della raccolta: consiste nella realizzazione di situazioni di fatto non conformi alla finalità della raccolta e comunque alle prescrizioni di legge.

## 3.3.2. STIMA DELLA GRAVITA' E DELLA PROBABILITA' DEL RISCHIO

### 3.3.2.1. Valutazione di probabilità e livello di rischio

Ogni minaccia è soggetta ad una valutazione di probabilità all'interno del contesto aziendale.

La valutazione della probabilità è effettuata in base alle considerazioni relative all'organizzazione ed alle strategie aziendali già in atto, esposte nei capitoli precedenti e al tipo di attività di impresa esercitata da ENCO, in che misura e maniera.

### 3.3.2.2. Valutazione del rischio e dell'impatto

Per effettuare una stima della gravità e della probabilità del rischio è necessario chiarire i concetti di vulnerabilità e danno.

Per VULNERABILITA' si intende la capacità del sistema di sicurezza dell'Azienda di contrastare le minacce valutate.

Per DANNO invece intendiamo l'insieme delle conseguenze derivanti dal verificarsi dell'evento negativo.

Il rischio viene valutato applicando la seguente formula:

$$\text{RISCHIO} = \text{PROBABILITA' MINACCIA} \times \text{DANNO}$$

Il livello di rischio è calcolando tenendo conto delle seguenti informazioni:

- livelli di vulnerabilità;
- minacce ipotizzabili;
- probabilità di accadimento;
- qualità delle informazioni

La valutazione dell'impatto della possibile concretizzazione di un rischio viene effettuata tenendo in considerazione tutte le informazioni raccolte.

### 3.3.2.3. Classificazione delle minacce in base al rischio

Nella tabella a pagina seguente, la gravità dell'impatto e la probabilità della minaccia sono espressi da un valore compreso tra 1 (insignificante / estremamente improbabile) e 5 (estremamente grave / certo).

DESCRIZIONE MINACCIA	VALUTAZIONE D'IMPATTO (V)	PROBABILITA' DELLA MINACCIA (P)	MISURA DEL RISCHIO (=V*P)	CLASSIFICA DELLA MINACCIA
Accesso non autorizzato ad aree riservate da parte di <b>utenti interni</b>	3	3	9	7
Accesso non autorizzato da parte di <b>utenti esterni non autorizzati</b>	4	2	8	10
Alterazione o modifica non autorizzata da parte di <b>utenti interni</b> delle informazioni	3	2	6	15
Alterazione o modifica non autorizzata da parte di <b>utenti esterni</b> delle informazioni	4	2	8	14
Alterazione o modifica non autorizzata da parte di <b>amministratore di sistema</b> delle informazioni	5	2	10	6
Alterazione o modifica non autorizzata da parte di <b>utenti interni di software/hardware</b>	3	3	9	9
Alterazione o modifica non autorizzata da parte di <b>utenti esterni di software/hardware</b>	4	2	8	11
Alterazione o modifica non autorizzata da parte di <b>amministratore di sistema di software/hardware</b>	5	3	15	2
Alterazione, <b>perdita, danneggiamento</b> all'uso dei dati per <b>cause ambientali</b>	5	4	20	1
<b>Perdita, danneggiamento</b> o impedimento all'uso dei dati a causa di <b>utenti interni</b>	3	3	9	8
<b>Perdita, danneggiamento</b> o impedimento all'uso dei dati a causa di <b>utenti esterni</b>	4	2	8	12
<b>Perdita, danneggiamento</b> o impedimento all'uso dei dati a causa dell' <b>amministratore di sistema</b>	5	2	10	5
<b>Divulgazione</b> dei dati da parte di <b>utenti non autorizzati</b> al trattamento	5	2	10	4
<b>Divulgazione</b> dei dati da parte di utenti autorizzati ma <b>senza ottenimento del consenso</b>	4	2	8	13
<b>Trattamento illecito</b> o non conforme alle finalità della raccolta	4	3	12	3

Figura 7 - Tabella di classificazione minacce

### 3.3.3. DATA BREACH E NOTIFICA DELLA VIOLAZIONE

L'articolo 3 del Regolamento obbliga il titolare del trattamento a notificare la violazione dei dati personali all'Autorità Garante entro 72 ore dal momento in cui si è venuti a conoscenza del fatto, ovvero nel momento in cui il titolare se ne è reso consapevole.

Se la violazione è suscettibile di comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.

ENCO si impegna al rispetto di tali normative e si impegna ad effettuare la comunicazione di eventuali violazioni dei dati tramite i mezzi di comunicazione predisposti, posta elettronica certificata o raccomandata R1.

### 3.3.4. INFORMATIVE

Agli articoli 13, comma 1, e 14, comma 1, il Regolamento indica in modo tassativo i contenuti dell'informativa da prestare all'interessato.

In particolare, il titolare deve sempre specificare:

- la base giuridica del trattamento;
- l'interesse legittimo sotteso al trattamento, ove presente;
- l'eventuale trasferimento di dati a Paesi terzi e, in tal caso, gli strumenti impiegati per il trasferimento;
- il periodo di conservazione dei dati o il criterio impiegato per la definizione del periodo di conservazione;
- il diritto di presentare reclamo all'autorità di controllo;
- in caso di impiego di processi decisionali automatizzati, la logica di tali processi e le conseguenze previste per l'interessato.

L'informativa dovrà, dunque, essere resa in forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile.

Dovrà, inoltre, essere fornita entro un termine ragionevole che non potrà superare un mese dalla raccolta oppure al momento della comunicazione dei dati.

Seguono i due modelli di informativa utilizzati: uno per i clienti, fornitori e collaboratori ed uno per i dipendenti.

### 3.3.4.1. Informativa clienti, fornitori e collaboratori

**Informativa resa ai sensi dell'art.13 del Decreto Legislativo 196/2003 del 30 giugno 2003 (codice in materia di protezione dei dati personali) e alla luce del Regolamento UE 2016/679, entrato in vigore il 25/05/2018.**

Gentile Signore/Signora,

La direzione della Enco Engineering Consultants S.r.l., titolare del trattamento dati, con sede in via Feltre 183 – 32036 Bribano (BL), con la presente desidera informarLa che la normativa sulla privacy è stata aggiornata in seguito all'introduzione del Regolamento UE 2016/679 del 27 aprile 2016, entrato in vigore il 25 maggio 2018.

In relazione alle informazioni di cui si entrerà in possesso, ai fini della tutela delle persone e altri soggetti in materia di trattamento di dati personali si informa quanto segue:

#### **a) TITOLARE DEL TRATTAMENTO**

Il titolare del trattamento è identificato nella persona giuridica ENCO Engineering Consultants S.r.l., rappresentata dagli Ingegneri Michele Reolon (legale rappresentante) ed Eugenio De Demo (Socio).

I dati di contatto del titolare del trattamento e del rappresentante legale della società sono i seguenti:

<b>TITOLARE DEL TRATTAMENTO</b>	<b>RAPPRESENTANTE LEGALE</b>
ENCO Engineering Consultants S.r.l. Via Feltre, 183 32036 Sedico (BL)- Italy Email info@enco.energy Telefono 0437 852727	Ing. Michele Reolon Via Cavassico Superiore, 89/A 32028 Trichiana (BL) – Italy Email office@enco.energy Telefono 0437 852727

#### **b) DATI TRATTATI**

Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.); Dati relativi all'attività economica e commerciale (partita iva, etc); Dati bancari per effettuazione pagamenti; Dati personali contenuti nei Curriculum Vitae. Gli stessi sono forniti direttamente dall'Interessato

#### **c) FINALITA' BASE GIURIDICA DEL TRATTAMENTO**

I dati raccolti saranno utilizzati esclusivamente per le finalità stabilite dal contratto sottoscritto da ENCO, titolare del trattamento, con il soggetto interessato.

Gli scopi sono limitati all'esercizio dell'attività di impresa e all'adempimento degli obblighi amministrativi, civilistici e fiscali previsti dalla legislazione italiana.

Queste, sinteticamente, le finalità del trattamento per cui ENCO richiede i dati:

- Stipulazione contratto cliente/fornitore
- Contratto di collaborazione temporanea o continuativa con professionisti
- Collaborazione con professionisti nell'ambito di gare d'appalto

Qualora si presentasse la necessità di trattare i dati per finalità diverse da quelle qui espresse, il consenso già fornito sarà nullo ed il Titolare dovrà provvedere ad informare nuovamente l'interessato in conformità all'effettivo trattamento.

#### **d) CONFERIMENTO**

La comunicazione di alcuni dati è considerata requisito necessario ed obbligatorio per adempiere alle finalità elencate e, di conseguenza, l'eventuale mancata comunicazione dei dati o il non conferimento del consenso rendono impossibile l'attuazione del contratto o delle finalità rispetto al soggetto interessato.

#### **e) MODALITA' DEL TRATTAMENTO**

Le modalità con le quali verranno trattati i dati personali contemplano la modalità cartacea e quella informatizzata.

L'accesso ai dati è consentito esclusivamente agli incaricati designati dal Titolare che potranno effettuare operazioni di archiviazione, utilizzo nei limiti della finalità ed ogni altra opportuna operazione che si svolga nel rispetto delle disposizioni di legge, garantendo non solo la sicurezza e la riservatezza dei dati ma anche l'esattezza, l'aggiornamento e la pertinenza delle informazioni raccolte.

#### **f) COMUNICAZIONE E DIFFUSIONE**

I dati raccolti non vengono trasmessi a terzi tranne nel caso dei Curricula Vitae. Questi ultimi sono trasmessi a terzi per la partecipazione di gare d'appalto, previa autorizzazione dell'interessato. La trasmissione può avvenire anche in paesi terzi, extra UE.

#### **g) DURATA DEL TRATTAMENTO**

I dati raccolti con la finalità di adempimento degli obblighi amministrativi, civilisti e fiscali vengono conservati (su supporto informatico e cartaceo) per dieci anni, come previsto dall'art. 22 del DPR n.600/1973. Le stesse direttive vengono seguite anche per dati di altro genere, trattandosi in genere di dati dello stesso tipo.

#### **h) DIRITTI DEGLI INTERESSATI**

In relazione ai predetti trattamenti potranno essere da Lei esercitati i diritti di cui all'art. 7 d.lgs. 196/2003 quali:

- ottenere la conferma circa l'esistenza o meno di dati che La riguardano;
- conoscere l'origine dei dati, la logica e la finalità su cui si basa il trattamento;



- ottenere la cancellazione, la trasformazione in forma anonima o il blocco di dati trattati in violazione di Legge, l'aggiornamento, la rettifica e l'integrazione dei dati stessi;
- opporsi, per motivi legittimi, al trattamento dei dati stessi;
- Revocare il consenso al trattamento

nei limiti ed alle condizioni previste degli articoli 8, 9 e 10 del citato decreto legislativo rivolgendosi a ENCO Engineering Consultants S.r.l. – Via Feltre 183, 32036 – Sedico (BL), mandando una mail all'indirizzo [info@enco.energy](mailto:info@enco.energy), o inviando un fax al numero 0437 852717.

## **i) ULTERIORI INFORMAZIONI**

Ulteriori informazioni in ordine al trattamento ed alla comunicazione di dati previsti direttamente o altrimenti acquisiti potranno essere richieste al responsabile incaricato per il trattamento dei dati presso la sede della Società. Il presente avviso naturalmente non esclude che altre informazioni siano date anche oralmente agli interessati al momento della raccolta dei dati.

Rimane fermo che tale consenso è comunque condizionato al rispetto delle disposizioni della vigente normativa. Ulteriori informazioni circa il trattamento dei dati potranno essere comunicate anche verbalmente.

Restano saldi tutti gli altri punti del contratto in materia di tipologia di incarico, obblighi reciproci di riservatezza, accettazione del codice etico e le indicazioni riguardanti il tacito rinnovo del contratto.

Sedico, 23/05/2018

## DICHIARAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI D.LGS. 196/2003 del 30 giugno 2003

Presa visione dell'informativa, il/la Sottoscritto/a,

nato/a,            il

Dichiaro di avere ricevuto l'informativa di cui all'art. 13 del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" in relazione ai trattamenti dei dati richiesti ed alle informazioni fornite, conforme anche al Regolamento UE 2016/679

Autorizzo e dà il consenso al trattamento dei propri dati per le finalità elencate al punto c) dell'informativa (obbligatorio)

Autorizzo il trasferimento dei propri dati a paesi terzi per le finalità al punto f) dell'informativa

, il

Firma dell'interessato

Il Titolare del Trattamento

**ENCO**  
**ENGINEERING CONSULTANTS S.r.l.**  
Via Feltre, 183 - 32036 SEDICO (BL)  
C.F. e P.IVA 00607990258

**3.3.4.2. Informativa dipendenti**

**Informativa resa ai sensi dell'art.13 del Decreto Legislativo 196/2003 del 30 giugno 2003 (codice in materia di protezione dei dati personali) e alla luce del Regolamento UE 2016/679, entrato in vigore il 25/05/2018.**

Gentile Signore/Signora,

La direzione della Enco Engineering Consultants S.r.l., titolare del trattamento dati, con sede in via Feltre 183 – 32036 Bribano (BL), con la presente desidera informarLa che la normativa sulla privacy è stata aggiornata in seguito all'introduzione del Regolamento UE 2016/679 del 27 aprile 2016, entrato in vigore il 25 maggio 2018.

In relazione alle informazioni di cui si entrerà in possesso, ai fini della tutela delle persone e altri soggetti in materia di trattamento di dati personali si informa quanto segue:

**j) TITOLARE DEL TRATTAMENTO**

Il titolare del trattamento è identificato nella persona giuridica ENCO Engineering Consultants S.r.l., rappresentata dagli Ingegneri Michele Reolon (legale rappresentante) ed Eugenio De Demo (Socio).

I dati di contatto del titolare del trattamento e del rappresentante legale della società sono i seguenti:

<b>TITOLARE DEL TRATTAMENTO</b>	<b>RAPPRESENTANTE LEGALE</b>
ENCO Engineering Consultants S.r.l. Via Feltre, 183 32036 Sedico (BL)- Italy Email info@enco.energy Telefono 0437 852727	Ing. Michele Reolon Via Cavassico Superiore, 89/A 32028 Trichiana (BL) – Italy Email office@enco.energy Telefono 0437 852727

**k) DATI TRATTATI**

Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo, telefono, fax, e-mail, dati fiscali, ecc.); Dati bancari per effettuazione pagamenti; Dati personali contenuti nei Curriculum Vitae; tutti questi dati sono forniti direttamente dall'interessato.

Dati personali contenuti nelle buste paga e nella documentazione relativa alla medicina del lavoro, entrambi trattati da aziende esterne: rispettivamente Feinar S.r.l. e Confartigianato, la cui responsabilità rimane comunque del Titolare del trattamento. Questi ultimi sono esclusivamente oggetto di archiviazione e vengono trattati esclusivamente dagli incaricati.

## **l) FINALITA' BASE GIURIDICA DEL TRATTAMENTO**

I dati raccolti saranno utilizzati esclusivamente per le finalità stabilite dal contratto sottoscritto da ENCO, titolare del trattamento, con il soggetto interessato.

Gli scopi sono limitati a quanto previsto dal contratto di lavoro dipendente (CCNL Studi Professionali) e all'adempimento degli obblighi fiscali e civilistici imposti dalla legislazione italiana.

Queste, sinteticamente, le finalità del trattamento per cui ENCO richiede i dati:

- Stipulazione e adempimenti relativi al contratto dipendente/datore di lavoro
- Trasmissione/Archiviazione documenti la cui principale gestione è affidata al Consulente del lavoro
- Trasmissione/Archiviazione documenti la cui principale gestione è affidata al Consulente per la medicina del lavoro.

Qualora si presentasse la necessità di trattare i dati per finalità diverse da quelle qui espresse, il consenso già fornito sarà nullo ed il Titolare dovrà provvedere ad informare nuovamente l'interessato in conformità all'effettivo trattamento.

## **m) CONFERIMENTO**

La comunicazione di alcuni dati è considerata requisito necessario ed obbligatorio per adempiere alle finalità elencate e, di conseguenza, l'eventuale mancata comunicazione dei dati o il non conferimento del consenso rendono impossibile l'attuazione del contratto o delle finalità rispetto al soggetto interessato.

## **n) MODALITA' DEL TRATTAMENTO**

Le modalità con le quali verranno trattati i dati personali contemplano la modalità cartacea e quella informatizzata.

L'accesso ai dati è consentito esclusivamente agli incaricati designati dal Titolare che potranno effettuare operazioni di archiviazione, utilizzo nei limiti della finalità ed ogni altra opportuna operazione che si svolga nel rispetto delle disposizioni di legge, garantendo non solo la sicurezza e la riservatezza dei dati ma anche l'esattezza, l'aggiornamento e la pertinenza delle informazioni raccolte.

## **o) COMUNICAZIONE E DIFFUSIONE**

I dati raccolti non vengono trasmessi a terzi tranne nel caso dei Curricula Vitae. Questi ultimi sono trasmessi a terzi per la partecipazione di gare d'appalto, previa autorizzazione dell'interessato. La trasmissione può avvenire anche in paesi terzi, extra UE.

## **p) DURATA DEL TRATTAMENTO**

I dati raccolti con la finalità di adempimento degli obblighi amministrativi, civilistici e fiscali vengono conservati (su supporto informatico e cartaceo) per dieci anni, come previsto dall'art. 22 del DPR n.600/1973. Le stesse direttive vengono seguite anche per dati di altro genere, trattandosi in genere di dati dello stesso tipo.

## q) DIRITTI DEGLI INTERESSATI

In relazione ai predetti trattamenti potranno essere da Lei esercitati i diritti di cui all'art. 7 d.lgs. 196/2003 quali:

- ottenere la conferma circa l'esistenza o meno di dati che La riguardano;
- conoscere l'origine dei dati, la logica e la finalità su cui si basa il trattamento;
- ottenere la cancellazione, la trasformazione in forma anonima o il blocco di dati trattati in violazione di Legge, l'aggiornamento, la rettifica e l'integrazione dei dati stessi;
- opporsi, per motivi legittimi, al trattamento dei dati stessi;
- Revocare il consenso al trattamento

nei limiti ed alle condizioni previste degli articoli 8, 9 e 10 del citato decreto legislativo rivolgendosi a ENCO Engineering Consultants S.r.l. – Via Feltre 183, 32036 – Sedico (BL), mandando una mail all'indirizzo [info@enco.energy](mailto:info@enco.energy), o inviando un fax al numero 0437 852717.

## r) ULTERIORI INFORMAZIONI

Ulteriori informazioni in ordine al trattamento ed alla comunicazione di dati previsti direttamente o altrimenti acquisiti potranno essere richieste al responsabile incaricato per il trattamento dei dati presso la sede della Società. Il presente avviso naturalmente non esclude che altre informazioni siano date anche oralmente agli interessati al momento della raccolta dei dati.

Rimane fermo che tale consenso è comunque condizionato al rispetto delle disposizioni della vigente normativa. Ulteriori informazioni circa il trattamento dei dati potranno essere comunicate anche verbalmente.

Restano saldi tutti gli altri punti del contratto in materia di tipologia di incarico, obblighi reciproci di riservatezza, accettazione del codice etico e le indicazioni riguardanti il tacito rinnovo del contratto.

Sedico, 23/05/2018

**DICHIARAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI D.LGS. 196/2003 del 30 giugno 2003**

Presa visione dell'informativa, il/la Sottoscritto/a,

nato/a,            il

Dichiaro di avere ricevuto l'informativa di cui all'art. 13 del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" in relazione ai trattamenti dei dati richiesti ed alle informazioni fornite, conforme anche al Regolamento UE 2016/679

Autorizza e dà il consenso al trattamento dei propri dati per le finalità elencate al punto c) dell'informativa (obbligatorio)

Autorizza il trasferimento dei propri dati a paesi terzi per le finalità al punto f) dell'informativa

, il

Firma dell'interessato

Il Titolare del Trattamento

**ENCO**  
**ENGINEERING CONSULTANTS S.r.l.**  
Via Feltre, 183 - 32036 SEDICO (BL)  
C.F. e P.IVA 00607990258